Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

LDI, Postfach 20 04 44, 40102 Düsseldorf

Herrn
Landtagspräsident
Ulrich Schmidt, MdL
Platz des Landtags 1

40221 Düsseldorf

Reichsstraße 43, 40217 Düsseldorf
E-Mail: poststelle@ldi.nrw.de
Bearbeitung: **Frau Siekmann**
Durchwahl: (0211) 38 424 - **93**

Aktenzeichen:
L 5.4.2

- Aktenzeichen bitte unbedingt angeben -

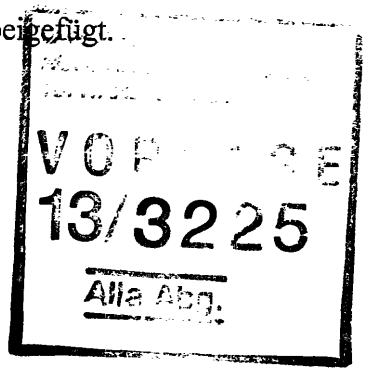
16. Februar 2005

17. Datenschutz- und Informationsfreiheitsbericht 2005 der Landesbeauftragten für Datenschutz und Informationsfreiheit

Sehr geehrter Herr Landtagspräsident,

nach § 27 Datenschutzgesetz für das Land Nordrhein-Westfalen (DSG NRW) lege ich dem Landtag den 17. Datenschutz- und Informationsfreiheitsbericht für die Zeit vom 01.01.2003 bis zum 31.12.2004 vor.

Die für die Mitglieder des Landtags bestimmten Exemplare sind beigefügt.



Mit freundlichen Grüßen

Ihre B. Sokol

(Sokol)

Datenschutz und Informationsfreiheit

Bericht 2005

Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Nordrhein-Westfalen

Siebzehnter Datenschutz- und Informationsfreiheitsbericht

der

Landesbeauftragten für Datenschutz

und Informationsfreiheit

Nordrhein-Westfalen

Bettina Sokol

für die Zeit vom 1. Januar 2003
bis zum 31. Dezember 2004

Herausgeberin:

Landesbeauftragte für Datenschutz
und Informationsfreiheit
Nordrhein-Westfalen
Bettina Sokol
Reichsstraße 43

40217 Düsseldorf

Tel: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

Düsseldorf 2005

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorbemerkung		1
1	**Zur Situation von Datenschutz und Informationsfreiheit**	2
2	**Technik**	7
2.1	RFID – gläserner Konsum	7
2.2	Telefonieren via Internet	9
2.3	Vertrauenswürdige, transparente IT-Produkte und Systeme	12
2.3.1	Sichere Informationsflüsse	13
2.3.2	Trusted Computing Platform (TCP)	14
2.3.3	Online-Update	15
2.4	Risiken offener Schnittstellen am PC	16
2.5	Erstellen von Sicherheitskonzepten	19
2.6	Datensicherheit in mittelständischen Unternehmen	21
2.7	Einzelfragen zur Datensicherheit	23
2.7.1	Löschen von personenbezogenen Daten auf Speichermedien	23
2.7.2	Unerkannte Datenübermittlung beim Homebanking	26
2.7.3	Nachlässiger Umgang mit Prüfungsunterlagen und Patientenakten	27
3	**Medien**	28
3.1	Die GEZ und der Adresshandel	28
3.2	Weniger Datenschutz bei den Neuregelungen zur Telekommunikation	28
3.2.1	Geltendes Recht? Das lässt sich doch ändern...	28
3.2.2	Die Adresse zur Nummer	29
3.2.3	Lückenlose Telekommunikationsüberwachung	30
3.2.4	Kommt die Vorratsdatenspeicherung durch die Hintertür?	31
3.3	Melderegisterauskunft online	32
3.4	Einzelfragen zu Telekommunikation, Internet und E-Mail	33

3.4.1	Etwas mehr Schutz gegen unerwünschte Werbung per Telekommunikation erreicht	33
3.4.2	Die private Homepage	35
3.4.3	Mobbing im Internet	36
3.4.4	Personenbezogene Internet-Umfrage einer Initiative	36
3.4.5	Mitteilungen aus Zwangsversteigerungs- und Insolvenzverfahren im Internet durch private Stellen	38
4	**Videoüberwachung**	40
4.1	Videoüberwachung an Schulen	40
4.2	Sonnenbad auf dem Balkon – live im Internet	41
4.3	Wer ein Taxi benutzt, wird videoüberwacht!	43
4.4	Videoüberwachung am Arbeitsplatz	44
4.5	Videoüberwachung in Umkleidekabinen eines Fitness-Studios	46
5	**Handel und Wirtschaft**	49
5.1	Radio Frequency Identification im Handel	49
5.2	Dubiose Datenverarbeitung im Call-Center	51
5.3	Weitergabe von Abonnentendaten durch insolvente Zeitungsverlage	52
5.4	Adressen machen Leute? - Statistische Daten zu Kaufkraft und Zahlungsmoral	55
5.5	Auskunfteien: Bonitätsauskünfte an Versicherungen	57
5.6	Heiße Luft statt harter Fakten: Schätzdaten in Bonitätsauskünften	59
5.7	Living by numbers – Bonitätsbewertungen durch Scoring	60
5.8	Kreditfabriken	63
5.9	Kleine Gefälligkeiten – kein Kavaliersdelikt!	67
6	**Verkehr**	70
6.1	Passagierdatenübermittlung an U.S.-Zollbehörden	70

6.2	Fluggepäck wird schon vor der Landung elektronisch durchgecheckt	73
7	**Verfassungsschutz**	75
8	**Polizei**	76
8.1	Änderungen des Polizeigesetzes	76
8.2	Nachlese Rasterfahndung	80
8.3	Von der Demo in die Datei	82
8.4	Verbesserter Datenschutz bei der Führung von Kriminalakten	83
8.5	Zweifelhafter Fernsehruhm	84
9	**Justiz**	86
9.1	Bundesverfassungsgericht stärkt das Allgemeine Persönlichkeitsrecht	86
9.2	Keine Erweiterung der DNA-Analyse zulassen	87
9.3	Telefonverbindungsdaten ohne richterliche Anordnung – die Spitze eines Eisbergs?	88
9.4	Auswertung von Patientenakten durch geschädigte Krankenkassen bei Betrugsvorwurf	91
9.5	Mitteilungen aus Zwangsversteigerungs- und Insolvenzverfahren im Internet durch Justizbehörden – ungewollte Publizitätswirkung?	93
9.6	Offene Kontodaten und Namenslisten von Gefangenen	94
10	**Soziales**	97
10.1	Das Sozialgeheimnis wahren	97
10.2	Die Grundsicherung im Alter und bei Erwerbsminderung	98
10.3	Datenverarbeitung durch den Medizinischen Dienst der Krankenversicherung	101
10.4	Gutachten für die gesetzliche Unfallversicherung	103
10.5	Seniorenheime	107
10.6	Beobachtungsbogen in Kindertagesstätten	107

10.7	„Hartz IV“ und der Datenschutz	108
11	**Gesundheit**	112
11.1	Datenverarbeitung im Gesundheitswesen	112
11.2	Einrichtung eines neuen Krebsregisters	114
11.3	Mammografie-Screening	115
11.4	Elektronische Patientenakte – das Problem der Verantwortlichkeit	116
11.5	Gesundheitskarte	117
12	**Beschäftigtendatenschutz**	120
13	**Wissenschaft**	121
13.1	Studieren über Gebühr	121
13.2	Evaluation der Lehre	122
13.3	Auskunftei für juristische Staatsprüfungen	124
14	**Forschung**	127
14.1	Das Kompetenznetz HIV/AIDS	127
14.2	Forschungsregister	128
15	**Schule**	130
15.1	Die SMS gegen das Schuleschwänzen	130
15.2	Einsicht in Abiturunterlagen	131
16	**Kultur**	133
16.1	Abgabe von Reproduktionen personenbezogenen Archivguts an Gedenkeinrichtungen	133
16.2	Stadtarchiv statt Archiv-GmbH	134
16.3	Archivarische Findmittel im Internet	136
17	**Kommunales**	138
17.1	Immer gleich der ganze Kaufvertrag?	138

17.2	Missbrauch des Fahrzeugregisters	138
17.3	Veröffentlichung von Daten der Ratsmitglieder im Internet	139
18	**Ausländerinnen und Ausländer**	141
18.1	Besucherkontrollen in Asylbewerberunterkünften	141
18.2	Bedenkliche Ausschreibungspraxis im Schengener Informationssystem	141
19	**Finanzen**	143
19.1	Gläserne Steuerpflichtige durch das Steueränderungsgesetz	143
19.2	Das Recht der Steuerpflichtigen auf Akteneinsicht – nur im Ermessen der Finanzbehörden?	146
20	**Statistik**	148
20.1	Mikrozensus	148
20.2	Forschungsdatenzentrum der Statistischen Landesämter	149
21	**Internationaler Datenverkehr**	151
22	**Behördliche und betriebliche Datenschutzbeauftragte**	153
22.1	Datenschutzbeauftragte bei öffentlichen Stellen	153
22.2	Betriebliche Datenschutzbeauftragte	155
23	**Informationsfreiheit**	157
23.1	Keine Flucht aus der Informationspflicht ins Privatrecht ermöglichen	157
23.2	Bereichsspezifische Zugangsregelungen	159
23.2.1	Wann ist eine Zugangsregelung eine Zugangsregelung?	159
23.2.2	Die Gemeindeordnung geht dem IFG NRW nicht vor	160
23.2.3	Vorrang des Verwaltungsverfahrensgesetzes, aber ohne Sperrwirkung	162
23.3	Ungeahnter Zuwachs an vermeintlichen Geschäftsgeheimnissen	164
23.3.1	Wer hat die Amtskette gespendet?	164

23.3.2	Und noch einmal: angebliche Geschäftsgeheimnisse	165
23.3.3	Grundstückskaufverträge sind keine Geschäftsgeheimnisse	166
23.3.4	Cross-Border-Leasing-Geschäfte – top secret?	168
23.4	Mehr Licht! Beispiele aus verschiedenen Verwaltungsbereichen	170
23.4.1	Starke Nachfrage nach Bauangelegenheiten	170
23.4.2	Umfangreiche Aktenbestände sind kein Ablehnungsgrund	171
23.4.3	Was steht eigentlich in den Berechnungsgrundlagen für Abfall- und Straßengebühren?	172
23.5	Aktive Informationspolitik im Rat leider vorerst gescheitert	173
23.6	Gebührenvorauszahlung: Informationen gegen Vorkasse ist nicht im Sinne des IFG NRW	173
23.7	Neuerungen im Recht auf Zugang zu Umweltinformationen	175
Anhang		177
Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder		177
Entschließungen der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)		213
Stichwortverzeichnis		219
Bestellformular Infomaterial		

Vorbemerkung

Immer wieder freuen wir alle in der Dienststelle uns über den bestärkenden Zuspruch, den wir auch von vielen Bürgerinnen und Bürgern erhalten. Gerade in schwierigen Zeiten ist das Aufmunterung und Unterstützung. Haben Sie herzlichen Dank dafür! Herzlich danken möchte ich an dieser Stelle aber natürlich auch meinen Mitarbeiterinnen und Mitarbeitern, die mit ihrer kompetenten Arbeit und mit ihrem großen Engagement den Grund für solche freundlichen Schreiben schaffen.

Die Zuständigkeit für die Informationsfreiheit hat nicht nur unser Aufgabenfeld bereichert, sondern auch erstmals den Berichtstitel erweitert. Um die Bedeutung der Informationsfreiheit neben dem Datenschutz angemessen auf der Titelseite zum Ausdruck bringen zu können, wurde die unschöne Länge der Bezeichnung „Datenschutz und Informationsfreiheit – Bericht 2005" zähneknirschend in Kauf genommen.

Fortgeführt werden konnte in diesem Berichtszeitraum ebenfalls die Kooperation mit dem Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster. Mit dem Sommersymposium Informationsfreiheit 2003 und der Tagung „Living by Numbers – Ein Leben zwischen Statistik und Wirklichkeit", die 2004 die Adressbewertung und das Scoring in der Privatwirtschaft zum Gegenstand hatte, wurden wieder zwei sehr gut besuchte gemeinsame Veranstaltungen durchgeführt.

Erwähnt sei nicht zuletzt auch, dass ich zum Ende meiner ersten Amtszeit als Landesbeauftragte für Datenschutz und Informationsfreiheit im März 2004 für eine zweite Amtszeit, also für weitere acht Jahre, in meinem Amt bestätigt worden bin. Besonders gefreut hat es mich, dass alle im Landtag vertretenen Fraktionen mich ohne Gegenstimme und ohne Enthaltung gewählt haben. Für dieses Vertrauen in meine Arbeit möchte ich mich sehr herzlich bedanken.

1 Zur Situation von Datenschutz und Informationsfreiheit

Ein Klima des Misstrauens greift bedauerlicherweise immer weiter um sich. Dies gilt sowohl im öffentlichen Bereich als auch in der Privatwirtschaft und sogar für höchstpersönliche Beziehungen. Die immer leichtere und kostengünstigere Verfügbarkeit neuer technischer Möglichkeiten führt zudem dazu, dass die Technik breit gefächert zur Förderung dieses Misstrauens instrumentalisiert werden kann. Kaum ein Mensch dürfte noch einen **Überblick** darüber besitzen, wer, was, wann und wie lange über wen in welchem Verwendungszusammenhang weiß. Datenverarbeitungen ohne bewusste Mitwirkung oder Kenntnis der davon betroffenen Personen haben in einem erschreckenden Ausmaß zugenommen. Intransparenz stellt Selbstbestimmung jedoch in Frage.

Die These vom Klima des Misstrauens sei an einigen Beispielen erläutert: Pressemeldungen zufolge boomt das Geschäft der Labore, die DNA-Analysen durchführen. Väter scheinen in großer Zahl nachprüfen zu wollen, ob sie auch wirklich der jeweils leibliche Vater des Kindes sind, für das sie Unterhalt zahlen. Eine Speichelprobe von Vater und Kind genügt, um die Abstammung feststellen zu können. Ohne die Einwilligung des Kindes oder der sorgeberechtigten Mutter verletzt diese heimliche Handlung schwerwiegend das Persönlichkeitsrecht. Zu diesen **heimlichen Vaterschaftstests** hat jetzt auch der Bundesgerichtshof entschieden, dass die Untersuchung des genetischen Materials eines anderen Menschen ohne dessen ausdrückliche Zustimmung rechtswidrig ist. DNA-Analysen hinter dem Rücken der Betroffenen sind auch im Arbeitsleben nicht erlaubt. So darf etwa das Ergebnis eines unzulässigen Tests nicht zur Stützung einer Verdachtskündigung herangezogen werden. Die Datenschutzbeauftragten des Bundes und der Länder fordern schon seit Jahren zur Klarstellung der Rechtslage ein Verbot heimlicher DNA-Analysen. Oder sollen sogar beliebige Dritte straflos Zwietracht in funktionierenden Familien säen können? Sehr zu begrüßen ist daher die kürzlich angekündigte Initiative aus dem Bundesjustiz- und dem Bundesgesundheitsministerium, ein gesetzliches Verbot heimlicher DNA-Tests auf den Weg bringen zu wollen.

Andere Beispiele für das Klima des Misstrauens sind die Geschäftsideen, mit denen Menschen zum Teil **ohne ihr Wissen kategorisiert** und bewertet werden. „Wollen Sie wissen, was Ihr Nachbar verdient?“ Mit diesem und ähnlichen Slogans wurde eine CD-ROM beworben, die adressenbezogen

Aussagen über Kaufkraft und Zahlungsmoral versprach. Es handelte sich dabei zwar überwiegend um statistisch aufbereitetes und angereichertes Datenmaterial, mit dem Wahrscheinlichkeitsaussagen getroffen werden sollten. Allerdings konnte der Eindruck entstehen, es ginge um Tatsachenangaben. Für etliche Adressgebiete bestanden dann allerdings auch die ausgeworfenen Informationen in so eindeutig personenbeziehbaren Daten, dass wegen des darin liegenden Datenschutzverstoßes ein Bußgeld zu verhängen war. Automatische Bewertungen von Personen durch ihre Zuordnung zu einer Vergleichsgruppe finden auch mit anderen mathematisch-statistischen Verfahren statt. Diese so genannten Scoring-Verfahren werden etwa bei der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA), bei Geldinstituten, im Versandhandel und im Versicherungsbereich eingesetzt.

Die rasche technische Entwicklung ermöglicht es dem Misstrauen, sich in ständig verfeinerten **Überwachungs- und Kontrollmöglichkeiten** Bahn zu brechen. Was für die Warenverwaltung von Vorteil sein mag, ist für das Persönlichkeitsrecht häufig nachteilig – beispielsweise Funkchips (RFID) mit ihren Potenzialen, die leicht missbrauchbar sind. Chips unter der Haut, Ortung via Internet – fast täglich kommen neue Ideen hinzu, die technisch Bewegungs- und Verhaltensprofile ermöglichen. Wenn die Pässe und Personalausweise künftig mit Funkchips ausgestattet sind, auf denen unter anderem die Fingerabdrücke abgespeichert sind, könnte es nicht nur bei Grenzkontrollen einige Überraschungen geben. Die Massentauglichkeit biometrischer Verfahren ist nach wie vor ungewiss und die Fehlerrate nicht unbeträchtlich. Hinzu kommt bei einer unverschlüsselten Speicherung der Merkmale auf den Funkchips noch ein weiteres Sicherheitsrisiko: Das unbefugte und unbemerkbare Auslesen der Chips und womöglich der Hightech-Identitätsdiebstahl.

Auch im öffentlichen Bereich mehren sich die Zeichen wachsenden Misstrauens des Staates gegenüber seinen Bürgerinnen und Bürgern. Beispielsweise ist seit Jahren in immer kürzeren zeitlichen Abständen die verdachtslose, routinemäßige Speicherung aller Verkehrsdaten im Bereich der Telekommunikation und der Internetnutzung auf Vorrat für unterschiedliche Zeiträume in der Diskussion. Dieses gewaltige Datenreservoir soll bei möglichen Anlässen in der Zukunft von Strafverfolgungsbehörden und möglicherweise auch von Geheimdiensten genutzt werden können. Zum Glück fand die **Vorratsdatenspeicherung** bei der Novelle des Telekommunikationsgesetzes im Sommer 2004 nicht

genügend befürwortende Stimmen. Sie wäre wohl auch kaum mit dem Grundgesetz vereinbar. Denn aus der Aufbewahrung der hinterlassenen Spuren ergeben sich die Bewegungs- und Verhaltensprofile aller Nutzerinnen und Nutzer von Telekommunikation und Internet. Auf europäischer Ebene ist die Forderung nach einer Vorratsdatenspeicherung allerdings gerade wieder einmal erneut erhoben worden.

Zu welchen Ergebnissen ein ausuferndes staatliches Misstrauen gegenüber allen Menschen führen kann, ist in den Vereinigten Staaten von Amerika zu beobachten. Die Durchleuchtung aller Flugpassagiere beispielsweise ist hier ebenso zu nennen wie die restriktive Einreisepraxis, die im Falle eines früheren Popstars sogar zu Protesten des britischen Außenministers geführt haben soll. Solche Verhältnisse sind hierzulande zwar nicht gegeben, aber die Tendenz zu immer mehr staatlichen Eingriffen in das Recht auf informationelle Selbstbestimmung ist unübersehbar. Die **ausgeweiteten Befugnisse** – nicht nur der Sicherheitsbehörden – für immer mehr heimliche Maßnahmen beschränken sich auch nicht auf das behauptete Ziel der Terrorismusbekämpfung. Zum Zweck der Förderung der Steuerehrlichkeit ist es ab April 2005 nicht nur Finanzbehörden, sondern auch einer unbestimmten Vielzahl weiterer Behörden möglich, Zugriff auf Bankdaten zu erhalten. Vom Abruf ihrer Kontenstammdaten erfahren die Bankkundinnen und Bankkunden zunächst nicht in jedem Fall etwas. Diese Art des Kontenzugriffs war ursprünglich allein zur Terrorismusbekämpfung eingeführt worden.

Was Zweckänderungen und Erweiterungen von Zweckbindungen angeht, stimmt auch die künftige Vergabe eines einheitlichen und dauerhaften Identifizierungsmerkmals im Steuerrecht bedenklich. Diese Nummer, die künftig jeder Person von Geburt an zugeteilt und lebenslang erhalten bleiben soll, wird parallel in den Meldebehörden und im Bundesamt für Finanzen gespeichert. Da neben der Nummer natürlich weitere Daten wie Namen, Vornamen, Geburtsdatum und -ort sowie Anschriften gespeichert werden, wird alsbald erstmals in der Geschichte der Bundesrepublik Deutschland mit dem Bundesamt für Finanzen eine zentrale Stelle über die Grunddaten der kompletten Bevölkerung verfügen. Bislang bestand in Politik und Gesellschaft weitgehend Konsens darüber, dass weder eine Zentraldatei der Meldedaten noch ein einheitliches, fachübergreifendes **Personenkennzeichen** gewollt ist. Auch wenn die Daten aus der **Zentraldatei** gesetzlich festgelegt nur für steuerliche Zwecke genutzt werden dürfen, lehrt doch die Vergangenheit, dass das Entstehen von weiteren

Nutzungsbegehrlichkeiten zu anderen Zwecken zu befürchten ist. Gesetze lassen sich ja ändern.

Häufigere Änderungen haben auch die Bestimmungen über **DNA-Analysen** im strafprozessualen Verwendungszusammenhang schon erfahren. Bei der letzten Novelle im April 2004 wurden zusätzliche Straftaten aufgenommen, die Anlass für die Durchführung einer DNA-Analyse sein können. Außerdem wurden die mit der Analyse erlaubten Zwecke um die Bestimmung des Geschlechts erweitert. Das ist einigen leider nicht genug. Sie fordern genauso **geringe Voraussetzungen für eine DNA-Analyse** wie für eine erkennungsdienstliche Behandlung. Dies verkennt, dass wegen der Aussagekraft der gewinnbaren Überschussinformationen die DNA-Analyse eine wesentlich intensivere Eingriffsqualität in das Recht auf informationelle Selbstbestimmung besitzt als ein herkömmlicher Fingerabdruck. Nach den verfassungsrechtlichen Anforderungen dürfte es zudem mehr als zweifelhaft sein, ob bereits jede beliebige Straftat für die Durchführung einer DNA-Analyse herhalten kann. Und nicht zuletzt muss es bei der Prognoseentscheidung, ob von der betroffenen Person auch künftig die Begehung von erheblichen Straftaten zu erwarten ist, durch eine neutrale und unabhängige Instanz bleiben. Der **Vorbehalt einer richterlichen Anordnung** von DNA-Analysen ist eine unverzichtbare grundrechtssichernde Verfahrensvorkehrung.

Zur Grundrechtsaushöhlung gibt es aber auch gegenläufige Tendenzen. So hat das Bundesverfassungsgericht im März 2004 die strafprozessualen Vorschriften über den so genannten **großen Lauschangriff**, also über die akustische Überwachung von Wohnraum, in weiten Teilen für **verfassungswidrig** erklärt. Aus der grundrechtlich geschützten Menschenwürde hat das Gericht einen unantastbaren Kernbereich privater Lebensgestaltung abgeleitet. Dieser Kernbereich ist absolut geschützt und damit jedem staatlichen Zugriff unter allen Umständen entzogen. Auch den besonderen Stellenwert einer unbelauschten Telekommunikation hat das Gericht in einer anderen Entscheidung vom gleichen Tag noch einmal bestärkt. Die Rechtsprechung des Bundesverfassungsgerichts hat Auswirkungen auch auf das Landesrecht. Die Befugnisse von Polizei und Verfassungsschutz zur akustischen Überwachung von Wohnraum und Telekommunikation müssen ebenso auf den Prüfstand wie die sie begleitenden Maßnahmen. Es sind Benachrichtigungs- und Kennzeichnungspflichten festzulegen, die den verfassungsrechtlichen Anforderungen entsprechen. Auch andere verdeckte Datenerhebungen müssen so ausgestaltet werden,

dass sie nicht in den absolut geschützten Kernbereich privater Lebensgestaltung eingreifen.

So wenig ermutigend wie manche Entwicklungen im Bereich des Schutzes der Privatheit und der informationellen Selbstbestimmung sind, so erfreulich ist andererseits die Grundtendenz im Bereich der **Informationsfreiheit**. Die Bürgerinnen und Bürger machen regen Gebrauch von ihrem guten Recht auf Information. Vielen Anträgen wird reibungslos stattgegeben. Die Streitfälle, die die Dienststelle erreichen, zeigen allerdings auch einige Problempunkte auf, in denen dem Gesetz klarstellende Änderungen gut täten. Dies gilt beispielsweise für den – manchmal umstrittenen – Anwendungsbereich des Gesetzes, aber auch für die Frage der Vorrangigkeit vermeintlich konkurrierender Regelungen. Insbesondere für die Betriebs- und Geschäftsgeheimnisse bedürfte es einer detaillierteren Bestimmung mit flankierenden Verfahrensvorgaben. Allzu oft berufen sich die öffentlichen Stellen nämlich auf diesen Informationsverweigerungsgrund, ohne dass er tatsächlich vorläge. Welche Unternehmen einem Bürgermeister eine Amtskette schenken, kann zum Beispiel gerade kein Geschäftsgeheimnis sein.

2 Technik

2.1 RFID – gläserner Konsum

Mit großer Aufmerksamkeit und Skepsis wurden die Entwicklungen und Projekte beim Einsatz von funkfähigen elektronischen Etiketten (RFID = Radio Frequency Identification Device) in der Warenlogistik und im Verkauf begleitet. Die grundlegende Technik ist zwar schon einige Jahre alt, durch die rasant fortschreitende Miniaturisierung, den Einsatz von Computer- und Speicherchips und die immer geringeren Stückkosten ergeben sich jedoch eine Vielzahl von Einsatzmöglichkeiten, aber auch Risiken für das informationelle Selbstbestimmungsrecht.

RFID-Systeme bestehen aus Transpondern (kontaktlosen Datenträgern), die an den zu identifizierenden Gegenständen angebracht sind, den mobilen oder stationären Lesegeräten sowie den damit verbundenen Applikationen (Hintergrundsystemen) zur Auswertung der Informationen.

Die Transponder können Funksignale empfangen und abgeben. Die Funkübertragung reicht für die verschiedenen Bautypen nach den ISO-Normen von wenigen Millimetern bis zu etwa einem Meter für die aktive Kommunikation zwischen RFID und Lesegerät. Messungen und Versuche haben jedoch ergeben, dass die tatsächlichen Reichweiten insbesondere für passives Abhören weit über diese Werte hinausgehen. RFIDs können sehr geringe Ausmaße (kleiner als 1 qmm) besitzen und nach derzeitigem Stand bis zu mehreren 100 Bit speichern. Die hierfür erforderliche elektrische Energie kann sowohl über eine eigene Stromversorgung (aktiver RFID-Tag) als auch über das Funksignal des RFID-Lesegerätes (passiver RFID Tag) bereitgestellt werden, so dass RFIDs auch ohne eigene Batterie funktionieren. RFIDs haben eine sehr lange Lebensdauer. Aufgrund ihrer verschiedenen technischen Ausprägung besitzen RFIDs eine **große Einsatzbreite**. Sie reicht von einfachen Diebstahletiketten ohne eigene Speichermöglichkeit, die lediglich ein Signal auslösen können, bis hin zu komplexen Chipkartensystemen mit derzeit noch nicht abschätzbaren Speicher- und Verarbeitungsmöglichkeiten beispielsweise für kontaktlose Geldkarten oder Fahrausweise.

RFID-Systeme werden für eine Reihe unterschiedlicher Zwecke eingesetzt, beispielsweise zur Kennzeichnung von Containern in der Logistik, von Büchern in Bibliotheken oder bei Tieren zur Feststellung der Identität. In fast allen Branchen gibt es Bestrebungen, mittels RFID Produkte zu

kennzeichnen und Warenströme zu automatisieren. Auch als Sicherheitsmerkmal für die Erkennung der Echtheit von Unterlagen sind sie verstärkt ins Blickfeld gerückt. So sollen möglicherweise Visa, Personalpapiere, Geldscheine oder die Eintrittskarten zur Fußball-WM 2006 mit RFID-Technologie ausgestattet werden.

Anhand der dargestellten Produkteigenschaften und Einsatzfelder erscheint eine Vielzahl von **Missbrauchsszenarien** denkbar: Personen könnten beispielsweise anhand ihrer Kleidungsstücke oder auch anhand mitgeführter Gegenstände erkannt werden, ohne dass sie dies bemerken. Darüber hinaus könnten RFID-Lesegeräte auch mit Videosystemen zur Beobachtung der Kundschaft gekoppelt werden oder auch eine Personenidentifizierung erfolgen, wenn in den Ausweispapieren RFID-Chips eingebaut werden.

In einer Entschließung vom 25./26. März 2004 (Abdruck im Anhang, Nr. 20) haben die Datenschutzbeauftragten des Bundes und der Länder zu den Risiken der RFIDs Stellung genommen. Sie wenden sich insbesondere dagegen, dass

- RFIDs versteckt angebracht und verdeckt ausgelesen werden, und damit die Anonymität verringern,
- Daten der RFID-Transponder aus den verschiedenen Anwendungsfällen mit personenbezogenen Daten zusammengeführt werden,
- über Hintergrundsysteme Profile erzeugt und gespeichert werden.

Sie fordern deshalb Hersteller von RFID-Systemen, die Produzenten von RFID gekennzeichneten Waren und den Handel auf,

- die Betroffenen umfassend über Einsatz und Verwendungszweck von RFID-Systemen zu informieren und ursprüngliche Verwendungszwecke nicht zu erweitern oder zu verändern,
- RFID-Tags (Etiketten) so zu gestalten, dass eine Löschung der Daten auf den RFID-Chips einschließlich der in der Fertigung aufgebrachten eindeutigen Seriennummer oder ihre problemlose Entfernung von den Produkten möglich ist,
- in RFID-Chips wirksame Blockierungsmechanismen vorzuhalten, so dass kein Nutzungszwang gegeben ist und anonymes Kaufen weiterhin möglich ist,

- die Systeme so zu gestalten, dass es nicht möglich ist, über Hintergrundsysteme unbemerkt und ungewollt Profile von Kundinnen und Kunden zu erstellen.

Sollen RFIDs in Identifikationssystemen wie Ausweisen oder Geldkarten oder als Echtheitsmerkmal beispielsweise in Geldscheinen eingesetzt werden, sollte dies nur erfolgen, wenn zuvor **Technikfolgenabschätzungen** vorgenommen werden, in denen Risiken und Nutzen gegeneinander abgewogen worden sind. In der Folge sollte insbesondere nur die Technik eingesetzt werden, die durch ihre Merkmale die Anonymität oder Nichtverfolgbarkeit der Personen am meisten schützt und damit die Furcht vor permanenter Überwachung und Kontrolle nimmt.

Ein besonderes Augenmerk ist auf die **Hintergrundapplikationen** zur Auswertung der von den RFIDs gelieferten Informationen zu legen. Denkbar und möglich sind hier umfassende Speicherungen und Auswertungen in Data Warehouse- und Data Mining-Systemen (siehe hierzu 15. Datenschutzbericht 2001 unter 2.2). Da beispielsweise bei Einkäufen ein Personenbezug leicht über Einkaufs- oder Kreditkarteninformationen herstellbar ist, könnte über derartige Systeme das Szenario vom gläsernen Konsum schnell Realität werden. Hier gilt es mit Augenmaß auf Massendatenspeicherung zu verzichten.

Nur durch einen transparenten Umgang mit der RFID-Technologie können auch künftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit bei personenbezogenen Daten sichergestellt werden. Auch beim Einsatz von miniaturisierten und in Produkte oder Identifikationssysteme eingebetteten IT-Systemen muss das Recht auf informationelle Selbstbestimmung gewährleistet bleiben.

2.2 Telefonieren via Internet

Große Zukunftsaussichten werden der Internet-Telefonie (VoIP = Voice over IP) vorausgesagt. Hierbei sollen die breitbandigen Datennetze auch zur Sprachübertragung genutzt werden und eine weitere Konvergenz der Medien Sprache, Bild und Ton erfolgen. Zu berücksichtigen ist allerdings, dass bei einem nachhaltigen Angebot von VoIP für Dritte die betroffenen Systeme und Netze unter das Informations- und Kommunikationsrecht fallen. Insbesondere im Hinblick auf die Wahrung des Telekommunikationsgeheimnisses ist hier einer Reihe von Risiken zu begegnen.

Sprache und Daten wurden in der Vergangenheit überwiegend über getrennte Netze geführt. Hauptgründe hierfür waren das mangelnde Echtzeitverhalten und die schlechtere Verfügbarkeit der Datennetze verbunden mit Komforteinbußen und fehlenden Endgeräten. Auf dem Markt sind mittlerweile jedoch eine Reihe von Komponenten und Produkten vorhanden, die es erlauben, über ein einheitliches IP-Netz auch die Sprachkommunikation abzuwickeln. Hierdurch erschließen sich nicht nur Einsparungen auf der Netzebene, sondern es können auch Verknüpfungen zu vorhandenen Datenbanken gebildet oder genutzt werden, und damit Informationen zusammenhängend gespeichert und ausgewertet werden. Realisierbar sind zentrale **Anrufmanagementsysteme**, die über ihre Software beliebige Steuerungen und Auswertungen zulassen. So ist es nicht verwunderlich, dass sowohl öffentliche Stellen und Firmen ihre internen Netze auf diese Technik umstellen als auch Access-Provider diese Dienstleistung für die Öffentlichkeit anbieten.

VoIP ist das Aussenden, Übermitteln und Empfangen digitalisierter Sprache und damit der Telekommunikation zuzurechnen. Werden geschäftsmäßig Telekommunikationsdienste angeboten, ist somit das **Fernmeldegeheimnis** zu wahren. Um diese Forderung zu erfüllen, sind für alle beteiligten IT-Systeme und Übertragungswege hinreichende Maßnahmen zum Schutz der Telekommunikationsdaten und damit in erster Linie Schutz der Daten vor unerlaubtem Zugriff zu treffen. Hierbei ist zuerst zu berücksichtigen, dass die Internet-Telefonie sich eines anderen Übertragungsweges bedient als die herkömmliche Telekommunikation. Die Sprache wird paketvermittelt über das Internet oder über firmeninterne Intranets geschickt. In Abhängigkeit von der eingesetzten Technik können an unterschiedlichen Stellen für verschiedene Zwecke in einstellbaren Zeiträumen und Umfängen Sprachdaten oder Verkehrsdaten gespeichert werden. Für eine Risikobetrachtung ist also die technische Ausprägung eines angebotenen VoIP-Dienstes sehr genau zu hinterfragen.

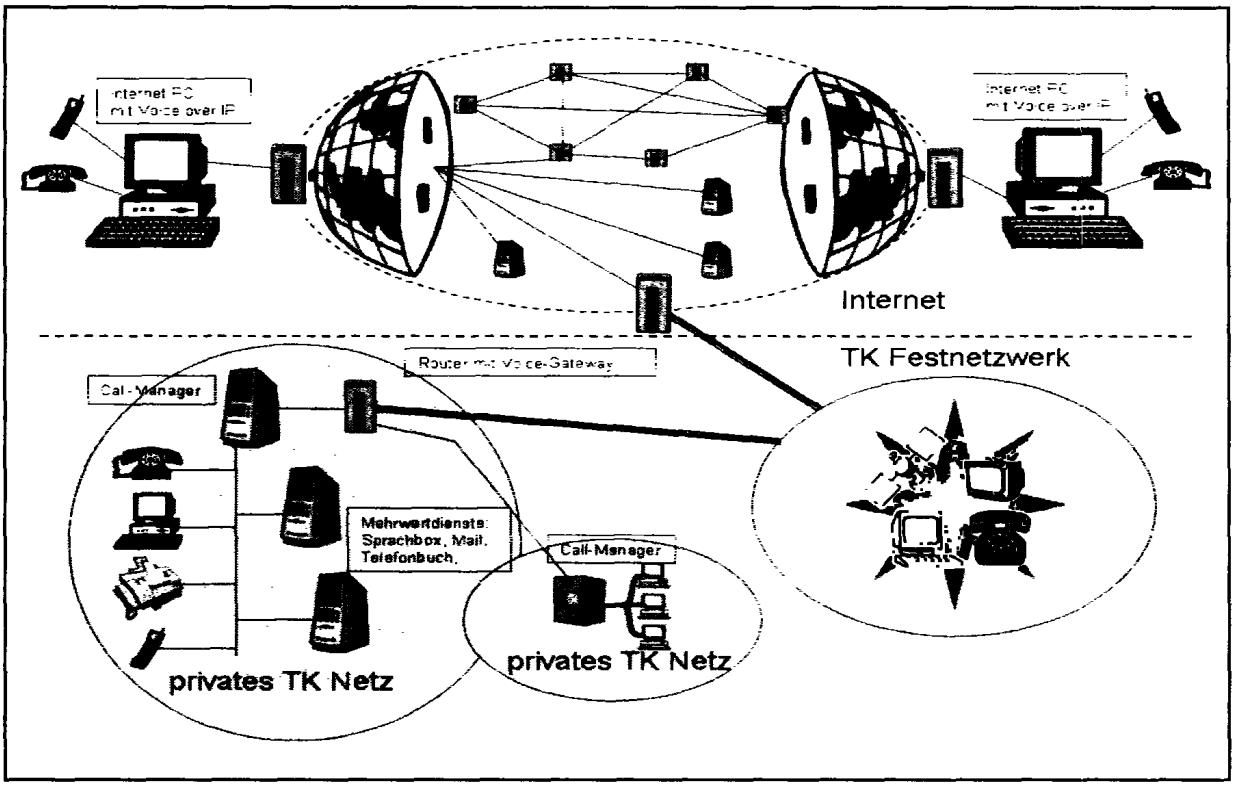


Bild 1: Möglichkeiten technischer Ausprägung privater VoIP-Nebenstellenanlagen und VoIP- Direktanbieterinnen

Wird ein Sprachdienst mittels VoIP angeboten, bei dem Vermittlungspunkte genutzt werden, die im Internet liegen, so können Datenspeicherungen oder sogar Datenübermittlungen (eventuell sogar ins Ausland) stattfinden, die nicht mehr allein in der Hand der Anbieterin liegen. Sie kann dann keine Gewähr dafür übernehmen, dass während der gesamten Kommunikation das Fernmeldegeheimnis gewahrt ist, da die beteiligten IP-Netze dieses nicht zwangsläufig gewähren müssen. Die derzeitigen Telekommunikations-Sprachnetze sind demgegenüber sicherer, weil sie vollständig in der Hand oder unter Kontrolle der Anbieterinnen liegen und nur Partnerunternehmen und -netze beteiligt sind, die ebenfalls diesen Regeln unterliegen. Soll eine Kommunikation mittels VoIP datenschutzgerecht erfolgen, sind somit weitere technische und organisatorische Maßnahmen zum Schutz der Kommunikation erforderlich. Zu denken ist hierbei beispielsweise daran, die Daten, die über das Internet verschickt werden, zu verschlüsseln. Erfolgt eine **Zwischenspeicherung** der Daten auf Netzservern oder PCs der Teilnehmerinnen und Teilnehmer, sind gegebenenfalls weitere Maßnahmen zur Löschung der Nachrichteninhalte nach Ende der Kommunikation und

zum Umgang mit den vorhandenen Verkehrsdaten zu treffen. So dürfen nach dem Telekommunikationsrecht Verkehrsdaten nur erhoben und über das Ende der Verbindung hinaus verwendet werden, soweit sie zum Aufbau weiterer Verbindungen, für Zwecke der Abrechnung oder zur Störungs- und Missbrauchsbekämpfung erforderlich sind.

Wird ein VoIP-Dienst innerhalb einer **geschlossenen Benutzungsruppe,** also beispielsweise im Sinne von privaten Nebenstellenanlagen in Firmennetzen, angeboten, ist die Firma ebenfalls zur Wahrung des Fernmeldegeheimnisses und zur Einhaltung der Datenschutzbestimmungen verpflichtet. Ihre Netze und die Sprachkommunikation sind so zu gestalten, dass die Vertraulichkeit des gesprochenen Wortes im gesamten Netz gewährleistet ist und die Erhebung und Speicherung von Verkehrs- und Inhaltsdaten ausschließlich im erlaubten Umfang erfolgt. Hierzu ist es sinnvoll, für das Verfahren eine Risikoanalyse durchzuführen und ein Sicherheitskonzept zu erstellen.

Soll ein VoIP-Dienst angeboten werden, so ist die Netzstruktur so zu gestalten, dass das Fernmeldegeheimnis gewahrt wird.

2.3 Vertrauenswürdige, transparente IT-Produkte und Systeme

IT-Systeme besitzen heute überwiegend einen leistungsfähigen Internetzugang, über den eine umfangreiche Kommunikation sowie der Bezug elektronischer Produkte der verschiedensten Art möglich sind. Gleichzeitig setzt dieser Zugang die Systeme aber erhöhten Risiken durch Hackerangriffe und Computerviren aus und macht sie potentiell unsicher.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit der Initiierung der Entwicklung von Schutzprofilen, der Begleitung internationaler Bestrebungen zur Schaffung vertrauenswürdiger IT-Systeme aber auch durch kritische Betrachtung der Praxis der Softwareindustrie bei Online-Updates im Berichtszeitraum mehrfach der Verbesserung des Datenschutzes und der Datensicherheit von **IT-Systemen** gewidmet. Auch die EU-Datenschutzrichtlinie für elektronische Kommunikation vom 12.07.2002 enthält die grundlegende Verpflichtung, die Sicherheit und Vertraulichkeit der Kommunikation über elektronische Netze zu gewährleisten.

Sollen die auf vielen Ebenen eingeleiteten Initiativen zu eGovernment und eCommerce erfolgreich sein, ist ein grundlegendes Vertrauen in die Beherrschbarkeit der genutzten IT-Systeme und in einen **angemessenen Schutz** der personenbezogenen Daten unabdingbar. Anwenderinnen und Anwender müssen sich darauf verlassen können, dass die an den Kommunikationen beteiligten Systeme überprüfbar korrekt arbeiten und Informationen nur auf ihre Initiative hin und im gewollten Umfang ausgetauscht werden. In jedem Fall ist die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten zu gewährleisten.

2.3.1 Sichere Informationsflüsse

Eine Möglichkeit der Vertrauensbildung ist die Definition von **Schutzprofilen** mit Sicherheitsanforderungen für zu erstellende Produkte nach den internationalen Regelungen der Common Criteria (siehe hierzu 15. Datenschutzbericht unter 2.4, S. 43 ff). Der Bundesbeauftragte für den Datenschutz bietet seit November 2002 ein mit dem Bundesamt für Sicherheit in der Informationstechnik entwickeltes Schutzprofil (Protection Profile) zur sicheren Kontrolle von Informationsflüssen in IT-Systemen an. Entsprechend diesen Vorgaben erstellte Produkte können dann nach Abschluss der Entwicklung durch unabhängige Institutionen nach international gültigen Kriterien geprüft werden.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren an die Hersteller, entsprechende vertrauenswürdige und datenschutzfreundliche Produkte zu entwickeln oder vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt (Abdruck der Entschließung vom 27./28. März 2003 im Anhang, Nr. 7). Anwenderinnen und Anwendern moderner Technik ist zu empfehlen, nur solche Produkte einzusetzen, die von Ihnen oder von unabhängigen Dritten jederzeit auf die Wirksamkeit von Sicherheitsvorkehrungen überprüft werden können und die insbesondere eine **Transparenz der Verfahrensabläufe** gewährleisten sowie die Forderung nach Datensparsamkeit erfüllen.

2.3.2 Trusted Computing Platform (TCP)

Unter dem Stichwort „Trusted Computing Platform (TCP)"„ haben führende Hard- und Softwarehersteller eine Spezifikation erarbeitet, welche die Sicherheit und **Vertrauenswürdigkeit von Rechnersystemen** erhöhen soll. Ziel ist es, durch Systemerweiterungen, die im Kern in einem TPM = Trusted Platform Modul integriert sind, eine Hard-/Software zu schaffen, die sich in einem festgeschriebenen Zustand befindet, sich immer in der erwarteten Art und Weise verhält und dies ihren Besitzerinnen und Besitzern sowie ihren Kommunikationspartnerinnen und -partnern beweisen kann. Ein weiterer wichtiger Aspekt ist es, digitale Rechte besser schützen und durchsetzen zu können. Hierzu erfüllt das TPM im Wesentlichen die drei Aufgaben:

- Einstellung eines an das TPM gebundenen einzigartigen Schlüsselpaares (Endorsement Key), dessen privater Schlüssel im TPM gespeichert wird, über das die Echtheit des TPM bescheinigt und die Erzeugung von Identitäten ermöglicht wird,
- Bereitstellen kryptografischer Funktionen für andere Systemkomponenten über Schlüsselhierarchien und
- Überwachung des Systemzustands und Erteilung von Auskünften hierüber.

Die Datenschutzbeauftragten des Bundes und der Länder erkennen diese Entwicklungsziele an. Sie begrüßen insbesondere alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen, erkennen aber auch die berechtigten Forderungen der Softwarehersteller nach Bezahlung kostenpflichtiger Software an. Allerdings betrachten sie die Entwicklungsziele dann skeptisch, wenn damit die Einführung zentraler, für die Nutzenden **intransparenter Kontrollinstanzen** verbunden ist. Die Hersteller von Informations- und Kommunikationstechnik werden deshalb aufgefordert, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und
- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden (Abdruck der Entschließung vom 27./28. März 2003 im Anhang, Nr. 1).

2.3.3 Online-Update

Zur Gewährleistung der Sicherheit und Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Softwarehersteller bieten deshalb in zunehmendem Maße an, **Online-Updates** für komplette Softwarepakete oder einzelne Aktualisierungen auf die Rechner ihrer Kundinnen und Kunden zu laden und automatisch zu installieren. Dieses Verfahren ist für alle Seiten zunächst bequem, verbunden mit diesen Online-Services sind aber auch Datenschutzrisiken.

Immer öfter werden bei Online-Updates – oftmals für die Nutzenden unbemerkbar oder zumindest nicht transparent – Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner **ausgelesen** und an die Hersteller **übermittelt**, ohne dass dies im derzeit praktizierten Umfang erforderlich wäre. Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software, die dann in der Regel genutzt werden, ohne genau die Erweiterungen sowie die Auswirkungen auf andere Anwendungen zu kennen.

Es ist darauf hinzuweisen, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen im datenschutzrechtlichen Sinn **Wartungstätigkeiten** sind. Sie dürfen nur von dazu ausdrücklich ermächtigten Personen durchgeführt werden. Insbesondere der Zugriff auf personenbezogene Daten ist im Zusammenhang mit Wartungstätigkeiten nur im unvermeidbaren Maß zu gestatten. Daneben sind neue Softwarekomponenten vor dem Einsatz auf Produktionssystemen zu testen und von autorisierter Stelle freizugeben. Die

meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht.

Für private Nutzerinnen und Nutzer kann das unbemerkte Übersenden von Daten an Softwarehersteller mit erheblichen Risiken für den Schutz der Privatsphäre verbunden sein und anonyme Nutzungsmöglichkeiten der Produkte ausschließen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Funktionen zur Verfügung stehen.

In ihrer Entschließung vom 7. August 2003 (Abdruck im Anhang, Nr. 11) wenden sich die Datenschutzbeauftragten des Bundes und der Länder deshalb entschieden gegen Software-Updates, die einen unkontrollierbaren Zugriff auf die IT-Systeme erfordern. Update-Verfahren müssen **benutzerinitiiert**, **transparent** und **revisionssicher** sein. Sie sollten nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit zu berücksichtigen. Weiterhin sollten auch datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden.

2.4 Risiken offener Schnittstellen am PC

Ein Computer ist immer nur so gut geschützt wie der schwächste Baustein in seinem Sicherheitskonzept. Hierzu zählen besonders auch die zur Verfügung stehenden offenen Schnittstellen. In Zeiten der „Plug and Play"-Konfigurationen der Betriebssysteme und der riesigen Speichermöglichkeiten schnell wechselbarer Speichermedien werden die hierdurch entstehenden Risiken immer größer.

Mobile Geräte mit großer Speicherkapazität stellen ein hohes Sicherheitsrisiko für Rechner und Unternehmensnetzwerke dar, wenn ihre Verwendung durch Mitarbeiterinnen und Mitarbeiter unkontrolliert erfolgen kann. Potenzielle Sicherheitsrisiken beinhalten dabei neben Laptops, PDAs und externen Festplatten zunehmend auch Musik-Player, Handies sowie

Digitalkameras mit Speicherchips. Die Geräte können Einfallstore für Trojaner und Viren sein, weil sie Firewall und Anti-Virensoftware leicht umgehen können. Sie ermöglichen es aber auch, rasch Unternehmensdaten über leistungsfähige Schnittstellen wie **USB** oder **Firewire** zu entwenden.

Um Datenmissbrauch vorzubeugen, sind in vielen Behörden und Betrieben schon seit langem Floppy- und CD-Laufwerke aus den PCs verbannt worden. Nun aber gilt es auch den neuen Risiken zu begegnen. Ein Beispiel sind USB-Memory-Sticks, die in die USB-Schnittstelle gesteckt und automatisch erkannt werden. Durch solche **virtuellen Laufwerke** und **externen Datenspeicher** ergeben sich folgende potentielle Sicherheitsprobleme:

- Der PC könnte von diesen Laufwerken unkontrolliert gebootet werden.
- Es könnte unkontrolliert Software von diesen Laufwerken eingespielt werden.
- Daten könnten unberechtigt auf die Wechselmedien kopiert werden.
- Beim Booten von Wechselmedien oder beim Installieren von Fremdsoftware können nicht nur Sicherheitseinstellungen außer Kraft gesetzt werden, sondern die Rechner können auch mit Computer-Viren und anderen Schadensprogrammen infiziert werden.

In Vorgaben für **Sicherheitskonzepte** wird daher empfohlen, mit geeigneten technischen und organisatorischen Sicherheitsmaßnahmen den Gefährdungen entgegen zu wirken. Hierzu gehören:

- Ausbau oder Verschluss von Schnittstellen,
- Deaktivierung im BIOS oder Betriebssystem,
- Kontrolle der Schnittstellennutzung sowie
- Richtlinien für die Nutzung.

Für die Umsetzung dieser Maßnahmen werden **Software-Tools** angeboten, die eine Administration der erforderlichen Sperr- und Kontrollfunktionen in den Computersystemen durchführen. Alle nicht erforderlichen Software- und Hardwarekomponenten, die Schnittstellen unterstützen, sollten entfernt oder gesperrt werden. Zusätzlich sollte der Anschluss von externen Datenspeichern durch das Sperren der nicht benötigten Schnittstellen im BIOS erschwert werden. Diese Sicherheitseinstellung verdient besondere Beachtung, da die Nutzung oder Sperrung der Schnittstellen an dieser Stelle unabhängig vom Betriebssystem erfolgt. Je nach Alter und Versionsstand unter-

stützen die BIOS-Einstellungen verschiedene Administrationsmöglichkeiten. Es kann bestimmt werden, welche Schnittstellen aktiviert oder deaktiviert werden, welche Protokolle unterstützt werden und ob es erlaubt ist, über eine Schnittstelle zu booten.

In einer Sicherheitsbetrachtung sind die verschiedenen **Import- und Exportwege** bei der Speicherung und Verarbeitung von Daten zu beschreiben. Auch ist zu ermitteln, welche Möglichkeiten für das Eindringen von Hackern vorhanden sind. Weiter ist der Umgang mit den verfügbaren Diskettenlaufwerken, CD-ROM-Laufwerken, seriellen und parallelen Schnittstellen für die Systemadministration und Nutzenden festzulegen. Grundsätzlich sollten sie nur einen für die jeweilige Aufgabe unbedingt erforderlichen Zugriff auf Systemressourcen erhalten, die eine Verwendung von externen Speichermedien ermöglichen.

Doch nicht nur die drahtgebundenen Anschlüsse der Computersysteme mit mobilen Speichergeräten sind eine Gefährdung für die Systeme und die darauf gespeicherten Daten. In die neuen Generationen der Rechner werden auch **Funk-Schnittstellen** implementiert. Übertragungstechniken wie Bluetooth und W-LAN bieten weitere Möglichkeiten auf Daten zuzugreifen und Manipulationen vorzunehmen (siehe hierzu auch 16. Datenschutzbericht 2003 unter 3.4). Funkübertragungen bringen ein hohes Risiko mit sich, da Angriffe nicht an Geschäftsgebäude gebunden sind. Hier sind ein restriktiver Umgang und die kontrollierte Nutzung zu fordern. Alle Möglichkeiten der Zugangs- und Nutzungsreglementierung sollten schon bei der Installation dieser Techniken eingerichtet werden. Leider sind die Standardeinstellungen der meisten Schnittstellen auf eine offene transparente Übertragung ausgerichtet. Zur Erreichung der größtmöglichen Sicherheit ist jedoch der umgekehrte Ansatz erforderlich „Alles was nicht erlaubt ist, wird gesperrt". Um eine höhere Sicherheit zu erreichen, ist immer wieder eine Überprüfung des Funktionsumfangs und der Schutzmechanismen erforderlich.

Insgesamt ist festzuhalten, dass sich die Gefahren von offenen Schnittstellen und mobilen Speichermedien nur bei bewusstem, kontrolliertem Einsatz beherrschen lassen. Hierzu sind genaue Regeln und Sicherheitsprofile, welche die erlaubten Funktionen beschreiben, festzulegen. Nicht erforderliche Komponenten sind zu deaktivieren. Bei Veränderung einzelner Komponenten und Schnittstellen ist auch an die Überarbeitung der Sicherheitsanforderungen und die Überprüfung der getroffenen Schutzmechanismen zu denken.

2.5 Erstellen von Sicherheitskonzepten

Nach Ablauf der Übergangsfrist des in 2000 novellierten Datenschutzgesetzes NRW sind alle dem Anwendungsbereich unterworfenen datenverarbeitenden Stellen verpflichtet, auch für Altverfahren ein Sicherheitskonzept zu erstellen. Stichproben bei einigen Behörden im Lande ergaben jedoch, dass Konzepte im Sinne des Gesetzes bisher kaum existieren.

Häufig wird im Zusammenhang mit der Erstellung von Sicherheitskonzepten auf die Komplexität des Themas hingewiesen. Die danach aufkommende Frage nach dem Vorhandensein einer Art Kochrezept zur Erstellung eines solchen Konzeptes kann an dieser Stelle mit einem klaren „Jein" beantwortet werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt einen sehr umfassenden Maßnahmenkatalog zur Verfügung, mit dessen Hilfe ein mittlerer Schutzbedarf abgedeckt werden kann. Das **Grundschutzhandbuch** genannte Werk steht auf der Web-Seite des BSI (www.bsi.de) kostenlos zum Download bereit. Auch eine gedruckte Version sowie ein datenbankgestütztes Tool kann gegen geringes Entgeld erworben werden. Es beinhaltet circa 780 standardisierte Sollmaßnahmen, aus denen die firmen- oder behördenspezifischen Maßnahmen entsprechend den eingesetzten Systemen und Verfahren hergeleitet werden können. Der enorme Umfang von inzwischen 2520 Seiten sollte nicht abschrecken, da die Arbeitsschritte standardisiert sind und schematisch zügig abgearbeitet werden können.

Der erste und mit großem Abstand wichtigste Schritt ist die Ermittlung derjenigen Menschen und Maschinen, die Daten verarbeiten. Eine solche Aufstellung ist im Normalfall vorhanden, weil sie Grundlage für nahezu alle organisatorischen Maßnahmen und DV-Projekte ist. Wenn diese Aufstellung um die einzelnen Verarbeitungsschritte und deren Reihenfolge ergänzt wird, ist eine Basis für die Erstellung eines **Sicherheitskonzepts** geschaffen. Eine in der Praxis seit langem bewährte Methode ist beispielsweise die **Modellierung von Geschäfts- oder Verwaltungsprozessen**. Sie erfolgt auf einem sehr hohen Abstraktionsniveau, so dass in diesem Stadium vernachlässigt werden kann, ob die Verarbeitung der Daten manuell oder automatisiert erfolgt.

Nach der Identifizierung der Prozesse müssen die verarbeiteten **Daten mit Personenbezug** bestimmt werden. Alle Prozesse, die nicht mit solchen Daten arbeiten, können ausgeblendet werden. Das so geschaffene Modell ent-

hält nun eine Abbildung derjenigen Teile des Datenverarbeitungsprozesses, die für das Sicherheitskonzept relevant sind. Es ist in diesem Zustand ein so genanntes ideales System, das keine technischen Defekte und kein menschliches Versagen berücksichtigt. Das Weglassen dieser Randbedingungen ermöglicht eine relativ übersichtliche Darstellung des Gesamtsystems, in der Systembrüche und Schnittstellen – also die Stellen, an denen Daten potenziell gefährdet sind – schnell identifiziert werden können. Es kann als Grundlage für die eigene Erstellung eines Sicherheitskonzepts oder als Pflichtenheft zur Ausschreibung dienen.

Bei der Erstellung des Sicherheitskonzepts ist zunächst die **IT-Strukturanalyse** durchzuführen. Hier ist zu ermitteln, auf welchen technischen Systemen wie Netzen, Servern und Arbeitsplatzrechnern die Datenverarbeitung stattfindet. Weiterhin ist die Software, die auf den verschiedenen Rechnertypen zum Einsatz kommt, zu erheben. Es empfiehlt sich eine Typisierung oder Paketbildung der Software, um die Komplexität möglichst gering zu halten. Zusammen mit den Software-Typen sind Kategorien von Maschinen zu bilden. Unten stehende Abbildung zeigt ein Beispiel grafischer Aufbereitung einer solchen Bestandsaufnahme.

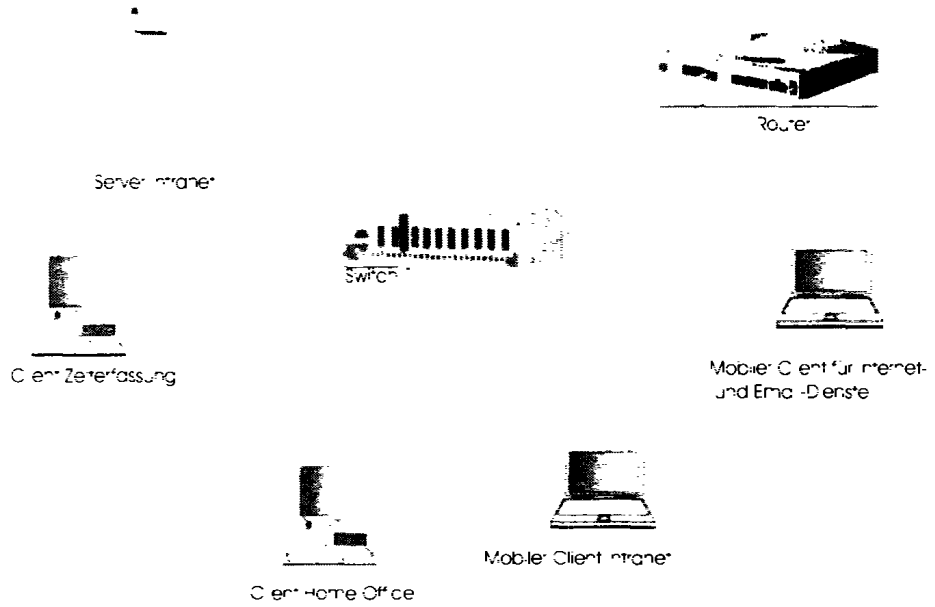


Bild 2: Grafische Darstellung von IT-Komponentengruppen

Den nächsten Schritt bildet die **Schutzbedarfsermittlung der IT-Anwendungen** einschließlich der verarbeiteten Daten. Dazu werden die

durch Verlust von Vertraulichkeit, Integrität und Verfügbarkeit entstehenden Folgeschäden betrachtet. Die Anwendungen werden dementsprechend in verschiedene Schutzstufen eingeteilt.

Das Modell des Grundschutzhandbuchs nimmt eine Gliederung der technischen und organisatorischen Komponenten in eine vorgegebene Anzahl so genannter Bausteine vor. Zu jedem dieser Bausteine wie Netz, Server, IT-Räume und organisatorische Bereiche sind die spezifischen Gefährdungen aufgelistet und die entsprechenden Abwehr- oder Präventivmaßnahmen beschrieben. Werden alle für die eingesetzten IT-Systeme relevanten Bausteine ausgewählt, ist das Ergebnis eine Check-Liste für die **Umsetzung der konkreten Sicherheitsmaßnahmen**. Die weitere Modellierung besteht dann im Wesentlichen darin, einen Soll-Ist-Abgleich der Maßnahmen vorzunehmen. Ergänzend können bei einem hohen Schutzbedarf weitere Maßnahmen notwendig sein. Auch die in § 10 DSG NRW postulierten Schutzziele Authentizität und Revisionssicherheit sind ergänzend zu prüfen.

Da von den zu treffenden Maßnahmen im Normalfall alle Bereiche einer datenverarbeitenden Stelle betroffen sind, sollte ein Sicherheitsmanagement von der Behörden- oder Geschäftsleitung initiiert werden. In diesem Zusammenhang ist auf den **„Leitfaden IT-Sicherheit"** des BSI hinzuweisen. Er gibt auf wenigen Seiten sowohl einen inhaltlichen Überblick, als auch plastische Beschreibungen von sonst eher abstrakten Bedrohungsszenarien. Ein weiterer Fokus liegt auf Maßnahmen, die im organisatorischen Bereich angesiedelt sind. Dieses lediglich 40 Seiten starke Dokument steht kostenfrei zum Download zur Verfügung.

Zusammenfassend bleibt zu sagen, dass auch mit „Rezept" und Unterstützung durch Tools und Check-Listen die Sicherheitspolitik und deren Umsetzung ein komplexes Unterfangen ist. Die explosionsartige Entwicklung der schadensstiftenden Inhalte jeder Form über Internet und E-Mail und die dadurch aufgedeckten Sicherheitslücken in der technischen Infrastruktur belegen aber, dass die Erstellung neben der gesetzlichen Verpflichtung auch im Sinne der Aufrechterhaltung eines ordnungsgemäßen Betriebs unbedingt notwendig ist.

2.6 Datensicherheit in mittelständischen Unternehmen

Eine Überprüfung der technischen und organisatorischen Maßnahmen zur Datensicherheit in mittelständischen Unternehmen führte zu recht

unterschiedlichen Ergebnissen. Überwiegend gab es keine verbindlichen Anweisungen und keine Kontrollen.

So war beispielsweise die Verpflichtung zur Bestellung einer oder eines betrieblichen Datenschutzbeauftragten in einem Unternehmen mit etwa 100 Beschäftigten gänzlich unbekannt. Andere Unternehmen hatten zwar Datensicherheitsmaßnahmen getroffen, die allerdings wegen des Fehlens einer **ganzheitlichen Betrachtung** Lücken aufwiesen. Insgesamt konnte folgendes Resümee gezogen werden:

- Auffallend unzureichend waren Datensicherheitsmaßnahmen insbesondere dann, wenn sie stark in den täglichen Arbeitsablauf hinein gereicht hätten und hierdurch vermeintlich ein Spannungsfeld zwischen Funktionalität und Sicherheit entstanden wäre.
- Zu trennende Betriebsbereiche waren selten mittels Einsatz technischer Hilfsmittel wie Zugangskontrollsystemen oder organisatorischer Regelungen wie dokumentierter Schlüsselverwaltung geschützt.
- Nur selten war ein Datenschutz- oder ein Sicherheitskonzept vorhanden.
- Entgegen der im öffentlichen Bereich durchgängigen Praxis, technische und organisatorische Maßnahmen schriftlich zu fixieren, wurde dies in den Unternehmen vernachlässigt.
- Fast vorbildlich eingehalten und auch durch interne und externe Institutionen kontrolliert waren diejenigen Datensicherheitsmaßnahmen (insbesondere die der Eingabekontrolle), die eine Schnittmenge mit den gesetzlich vorgegebenen buchhalterischen, finanzrechtlichen und geschäftsinternen Anforderungen an DV-gestützte Systeme bilden.

Die Ergebnisse der Kontrollbesuche zeigen, dass dem Thema Datenschutz und Datensicherheit in einer Reihe von mittelständischen Unternehmen ein zu **geringer Stellenwert** eingeräumt wird. Eine diesbezügliche Veränderung kann oft schon durch vermehrte Information bewirkt werden. Positiv können ebenfalls die Zusagen der aufgesuchten Unternehmen gewertet werden, den ausgesprochenen Empfehlungen zur Verbesserung der Datensicherheit uneingeschränkt folgen zu wollen. Auch die Sensibilisierung der Geschäftsleitungen zur Erstellung von Datensicherheitskonzepten konnte häufig erreicht werden.

Die Qualität der Datensicherheit steht und fällt mit den verbindlich vorgegebenen organisatorischen und technischen Maßnahmen. Das

Erreichen eines hohen Sicherheitsniveaus und damit eines hinreichenden Schutzes der zu verarbeitenden Daten ist nicht nur für die Einhaltung gesetzlicher Vorschriften erforderlich, sondern dient insbesondere dem Eigeninteresse eines Unternehmens. IT-Sicherheit als Unternehmensziel sollte daher Leitungssache sein.

2.7 Einzelfragen zur Datensicherheit

2.7.1 Löschen von personenbezogenen Daten auf Speichermedien

Bereits im 15. Datenschutzbericht 2001 unter 2.6.2, S. 53 wurde auf die Notwendigkeit der sicheren Löschung von personenbezogenen Daten auf Festplatten vor deren Weitergabe oder Entsorgung hingewiesen. Die zunehmende Anzahl von Anfragen zeigt, dass das Sicherheitsbewusstsein in dieser Hinsicht bei den Nutzerinnen und Nutzern zugenommen hat. Der sorglose Umgang bei der Reparatur, dem Austausch oder der Ausmusterung von Speichermedien mit personenbezogenen Inhalten macht allerdings ein erneutes Aufgreifen des Themas erforderlich.

2.7.1.1 Gefährlicher Irrtum: vermeintliche Datenlöschung

Da staunte ein Bürger nicht schlecht, als er entdeckte, dass sich hochsensible personenbezogene Daten auf der gerade erworbenen, gebrauchten Festplatte befanden. Er meinte zu Recht, dass ihn die Erbschaftsangelegenheiten anderer Leute nichts angingen.

Aus Anlass dieses Falls wurde in einer Presseerklärung nochmals auf die Risiken beim **Verkauf gebrauchter PCs** aufmerksam gemacht und auf den weitverbreiteten Irrtum hingewiesen, die in den marktgängigen Betriebssystemen implementierten Löschfunktionen könnten Daten irreversibel löschen. Vielmehr sind spezielle Löschprogramme zu verwenden, die beispielsweise Festplatten mehrfach überschreiben.

In einem anderen Fall wurde bei der **Reparatur eines PCs** einfach die Festplatte gegen eine andere gebrauchte Platte ausgetauscht, ohne die hierauf vorhandenen personenbezogenen Daten samt Betriebssystem und Anwendungen zu löschen. Ein Bürger, dessen Notebook-Festplatte beim Händler ausgetauscht worden war, wurde in einem weiteren Fall von einer Kundin

des gleichen PC-Händlers davon in Kenntnis gesetzt, dass auf ihrem neu erworbenen Notebook seine persönlichen Daten (unter anderem die gesamte berufliche und private Korrespondenz der letzten 5 Jahre) gespeichert waren. Die Notebook-Festplatte wurde trotz Zusicherung eines Mitarbeiters des PC-Händlers ungelöscht weitergegeben. Bei einem anderen Unternehmen wurden Datensicherungsbänder mit Firmen- und Personaldaten nach Auflösung der dezentralen Datensicherung nicht ordnungsgemäß gelöscht oder vernichtet. Stattdessen wurden 22 dieser Bänder ungelöscht auf einem Online-Marktplatz von einem Mitarbeiter der Firma angeboten.

In den eben geschilderten Fällen, die leider keine Ausnahmen waren, konnten die betroffenen öffentlichen und nicht öffentlichen Stellen – wie in den anderen Fällen auch – von der Notwendigkeit einer sicheren Löschung der auf den Festplatten gespeicherten personenbezogenen Daten und den hierbei zu treffenden flankierenden technischen und organisatorischen Sicherheitsmaßnahmen überzeugt werden. Insbesondere die in den Reparaturfällen angeschriebenen drei großen PC-Vertriebsketten zeigten sich kooperativ, passten ihre Sicherheitsmaßnahmen an und sagten den verbindlichen Einsatz von geeigneten Datenlöschprogrammen in ihren Filialen zu.

Nur mit speziellen Löschprogammen können Daten irreversibel gelöscht werden.

2.7.1.2 Dilemma: Garantie contra Anspruch auf Löschen

Werden in Garantiefällen oder aus anderen Gründen nicht mehr funktionsfähige Festplatten mit personenbezogenem Speicherinhalt zur Reparatur gegeben und können diese nicht mehr mit Hilfe von Softwareprogrammen gelöscht werden, besteht die Schwierigkeit für den Schutz der Daten eine geeignete Lösung zu finden. Händlerinnen und Händler erhalten von ihren Lieferfirmen in der Regel eine neue Festplatte nur im Austausch gegen das defekte Gerät. In vielen Fällen befindet sich jedoch die Firma im Ausland und das Schicksal der Festplatte bei der Festplattenherstellerin ist ungewiss.

Bringt die Kundin oder der Kunde einen defekten Computer, auf dessen Festplatte Daten gespeichert sind zur Reparatur, umfasst der Auftrag nicht automatisch den **Schutz der gespeicherten Daten**. Kundinnen und Kunden haben selbst die Pflicht, vor Weggabe des Gerätes für die Sicherung der Daten vor unbefugter Kenntnisnahme zu sorgen. Ist eine Löschung aus technischen Gründen nicht möglich, dann ist dem Computergeschäft mitzu-

teilen, dass personenbezogene Daten auf der Festplatte vorhanden sind, verbunden mit der konkreten Anweisung wie zu verfahren ist. Muss die Festplatte an die Lieferfirma weitergegeben werden, so entsteht ein Unterauftragsverhältnis mit all den Pflichten, die das Grundauftragsverhältnis betreffen. Die Kundinnen und Kunden sind hierüber zu informieren und müssen entscheiden, ob sie unter diesen Voraussetzungen einen Reparaturauftrag erteilen wollen.

Das Reparaturunternehmen ist vom Händler oder der Händlerin darauf aufmerksam zu machen, dass personenbezogene Daten auf der Festplatte gespeichert sind. Es ist bei einem Austausch der Festplatte auf das **Löschen** der Daten **zu verpflichten**. Wird die Festplatte mit personenbezogenem Speicherinhalt zum Hersteller ins Ausland geschickt, so ist § 4b BDSG zu beachten.

Letztendlich müssen die betroffenen Bürgerinnen oder Bürger selbst entscheiden, ob sie das Risiko einer möglichen Kenntnisnahme ihrer personenbezogenen Daten bei Wahrnehmung der Garantieleistung eingehen oder aus Sicherheitsgründen lieber auf ihren Garantieanspruch verzichten wollen. Sollten sich sensible personenbezogene Daten von Dritten auf der Festplatte befinden, darf sie grundsätzlich nur mit Einwilligung der betroffenen Dritten oder im gelöschten Zustand weitergegeben werden.

2.7.1.3 Allgegenwärtig: Speichermedien in modernen Geräten

Ordnungsgemäßes Löschen betrifft nicht nur PCs.

Der kontinuierliche Trend zur Miniaturisierung hat mittlerweile dazu geführt, dass sich Festplatten und andere Speichermedien in Elektronikgeräten des täglichen Bedarfs wie in Mobilfunkgeräten, Memory-Sticks, PDAs, Digitalkameras, Videorecordern oder digitalen Fotokopierern wiederfinden. Die Existenz dieser Speichermedien wird in den meisten Fällen gar nicht wahrgenommen. Vor Weitergabe oder Entsorgung dieser Geräte sollte daher geprüft werden, ob damit nicht auch personenbezogene oder sicherheitsrelevante Daten in die Hände **Dritter** gelangen könnten. Sollte dies der Fall sein, ist eine wirksame Löschung der Daten unerlässlich.

Angebotene Löschfunktionen der Geräte sind meistens nicht ausreichend. Im Zweifel sollten die Speicher mehrfach mit unkritischen Daten überschrieben werden.

2.7.2 Unerkannte Datenübermittlung beim Homebanking

Für heftige Empörung unter Käuferinnen und Käufern sorgte eine neue Version der Homebanking-Software eines bekannten Herstellers. Ohne hinreichende Information wurden bei Bank-Transaktionen Daten zunächst an den firmeneigenen Server übermittelt.

Bei der Durchführung von Bank-Transaktionen wurde vor der eigentlichen Verbindung mit dem jeweiligen Bank-Server ohne Kenntnis der Nutzerinnen oder Nutzer zunächst eine Verbindung zum Web-Server der Softwarefirma aufgebaut, um **Transaktionsdaten** mit Ausnahme von PIN und TAN auf **Plausibilität** zu überprüfen. Auf diesen – aus Firmensicht nützlichen und programmabhängigen – Webservice wurde lediglich vage im Bedienungshandbuch hingewiesen. Eine gültige Einwilligung lag deshalb nicht vor. Ebenfalls war die Notwendigkeit der Speicherung dieser Daten für geschäftliche Zwecke nach § 28 oder § 29 BDSG nicht gegeben.

Nach Intervention konnte eine vertretbare Lösung erreicht werden: Anwenderinnen und Anwender der Homebanking-Software besitzen nach aktualisiertem Versionsstand nunmehr die **Wahlmöglichkeit** zwischen einer „Standard"- und einer „Komfort"-Lösung, wobei „Standard" voreingestellt ist. Bei der Standard-Lösung werden lediglich die für eine Funktionalität des Programms zwingend benötigten Daten (Parameter der Versionsnummer der Software und der genutzten Bankmakros, Bankleitzahl sowie die Zugangs- und Transaktionsart) dem Server übermittelt. Der Server überprüft die Gültigkeit der Bankleitzahl sowie die Zulässigkeit von Zugangs- und Transaktionsart. Es werden also weder personenbezogene Daten übertragen noch ist eine nachträgliche Herstellbarkeit des Personenbezugs möglich. Die Komfort-Lösung entspricht der bisherigen Funktionsweise. Hierbei werden alle Transaktionsdaten außer PIN und TAN an den Server der Softwarefirma zwecks Überprüfung übermittelt. Hierüber werden die Nutzerinnen und Nutzer jetzt aber konkret informiert und müssen der Nutzung dieses Verfahrens entsprechend zustimmen.

Softwareprodukte mit einem Online-Datenaustausch müssen genau darüber Auskunft geben, welche Daten zu welchen Zeiten an welche Server übermittelt werden. Kunden und Kundinnen sind entsprechend zu informieren und die erforderlichen Einwilligungen sind einzuholen.

2.7.3 Nachlässiger Umgang mit Prüfungsunterlagen und Patientenakten

Leider gibt es immer wieder Beispiele über den unverantwortlichen Umgang mit personenbezogenen Unterlagen.

So wurden beispielsweise über einen Zeitraum von mehreren Monaten aus Platzgründen **Prüfungsakten** von Kandidatinnen und Kandidaten der zweiten juristischen Staatsprüfung einfach auf dem Flur der Behörde offen zwischengelagert. Sowohl Besucherinnen und Besucher als auch Beschäftigte der Behörde hatten die Möglichkeit der Einsicht in die Examensunterlagen. Eklatant war auch der gemeldete Fund von Patientenakten. Die hochsensiblen **Gesundheitsdaten** landeten während der Renovierung einer Arztpraxis in einem öffentlich abgestellten Papiercontainer.

Kennzeichnend für alle Beschwerden, die den unsachgemäßen Umgang mit personenbezogenen Unterlagen zum Inhalt haben, sind unzureichende oder fehlende verbindliche Aufbewahrungsbestimmungen. Schriftliche Regelungen über die einzuhaltenden Datenschutzbestimmungen sind wesentlich verbindlicher als mündliche Anweisungen und tragen dazu bei, die Datensicherheit bei der Aufbewahrung von personenbezogenen Unterlagen zu erhöhen. Etwas mehr Sorgfalt statt Nachlässigkeit ist ebenfalls anzumahnen.

3 Medien

3.1 Die GEZ und der Adresshandel

Seit einiger Zeit beschafft sich die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ) neben den ihr zur Verfügung stehenden Meldedaten auch noch Adressen auf dem freien Markt. Diese rechtlich umstrittene Praxis soll nunmehr staatsvertraglich legitimiert werden.

Schon in der Entschließung vom 30. April 2003 (Abdruck im Anhang Nr. 9) haben die Datenschutzbeauftragten des Bundes und der Länder gefordert, bei einer grundlegenden Neuorientierung der Rundfunkfinanzierung datenschutzfreundliche Modelle zu bevorzugen. Der achte Rundfunkänderungsstaatsvertrag geht jedoch leider in die genau gegenteilige Richtung. Danach soll sich die von den öffentlich-rechtlichen Rundfunkanstalten mit dem Gebühreneinzug beauftragte GEZ künftig wie ein Privatunternehmen der Daten aus dem Adresshandel bedienen können, obwohl ihr doch schon die Daten der Meldebehörden übermittelt werden. Werden öffentlichen Stellen so weitreichende Datenverarbeitungsbefugnisse wie der Privatwirtschaft zugeschoben, ist dies nicht nur ein Systembruch, sondern auch unter Verhältnismäßigkeitsgesichtspunkten bedenklich.

In einer gemeinsamen Presserklärung vom 08.11.2004 haben die Datenschutzbeauftragten der Länder Berlin, Brandenburg, Bremen, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein deutlich gemacht, dass die Befugnisse zur privaten Adressbeschaffung mit datenschutzrechtlichen Grundsätzen wie Datenvermeidung und Datensparsamkeit nicht zu vereinbaren sind.

3.2 Weniger Datenschutz bei den Neuregelungen zur Telekommunikation

3.2.1 Geltendes Recht? Das lässt sich doch ändern...

Die Datenschutzbeauftragten haben sich stets gegen die gängige Praxis einer Zwangsidentifizierung beim Erwerb vertragsloser (prepaid) Handys gewendet, da die Identifzierung und sogar die Angabe der Personalausweisnummer für den Kauf nicht notwendig sind und dementsprechend eine Datenerhebung durch die Anbieter unzulässig war.

Ein Mobilfunkanbieter zog vor Gericht, weil er entgegen der Weisung der Regulierungsbehörde für Telekommunikation und Post (RegTP) keine Daten von seinen Kundinnen und Kunden bei prepaid-Käufen erheben wollte. Dafür gab es **keine Rechtsgrundlage** und auch gar keine Notwendigkeit. Das Verwaltungsgericht gab ihm im September 2000 Recht. Das Oberverwaltungsgericht hob diese Entscheidung 2002 mit einer so wenig überzeugenden Begründung auf, dass das Bundesverwaltungsgericht sich 2003 genötigt sah, deutliche Worte zu sprechen. Das damalige Telekommunikationsgesetz (TKG) bot keine gesetzliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung, der mit einer Zwangsidentifizierung von Personen beim Kauf eines prepaid-Handys verbunden ist.

Wenig datenschutzfreundlich war die jeweilige Reaktion der Politik auf die Rechtsprechung. Nach der Verwaltungsgerichtsentscheidung wurde ein **Gesetzentwurf** diskutiert, mit dem eine rechtliche Grundlage für die Identifikations- und Datenerhebungspflicht geschaffen werden sollte. Nach der Entscheidung des Oberverwaltungsgerichts verschwand dieser Gesetzentwurf wieder in der Schublade, um nach der grundrechtsfreundlichen Entscheidung des Bundesverwaltungsgerichts wieder hervorgeholt zu werden. Inzwischen ist er Gesetz.

Die Zwangsidentifikation schafft „Datenfriedhöfe", die gar nicht für geschäftliche Zwecke benötigt werden. (Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 21. November 2003, Abdruck im Anhang Nr. 14).

3.2.2 Die Adresse zur Nummer

Ebenfalls gesetzlich geregelt ist die schon lange umstrittene Inverssuche, die es ermöglicht, zu einer Telefonnummer den Namen und die Adresse eines Teilnehmenden zu ermitteln.

Der Vertrieb einer entsprechenden Telefonverzeichnis-CD mit dieser Funktion war bisher durch das Oberlandesgericht Köln mit Beschluss vom 10.11.2000 unterbunden worden. Über die Inverssuche kann beispielsweise eine mühelose **Auswertung von Kleinanzeigen** erfolgen, bei denen lediglich die Telefonnummer angegeben ist. Wird zum Beispiel ein begehrtes Sammlerobjekt in der Kleinanzeigenrubrik einer Tageszeitung angeboten und zur Kontaktaufnahme die Telefonnummer angegeben, ist es mit der Funktion der Inverssuche möglich, zur Unzeit vor der Wohnung der

betreffenden Person zu stehen ohne vorher telefonischen Kontakt aufgenommen zu haben.

Wer nicht möchte, dass anhand der Telefonnummer die eigene Identität und Adresse von der Telefonauskunft beauskunftet wird, sollte sich erst gar nicht in das Verzeichnis eintragen lassen. Zumindest sollte der Funktion der Inverssuche widersprochen werden.

3.2.3 Lückenlose Telekommunikationsüberwachung

Im Zuge der TKG-Novelle muss nun auch die technische Umsetzung von Überwachungsmaßnahmen überarbeitet werden.

Zur Änderung der Telekommunikations-Überwachungsverordnung (TKÜV) liegt derzeit ein erster Referentenentwurf des Bundesministeriums für Wirtschaft und Arbeit vor. Nach redaktionellen Änderungen sind unter anderem folgende Neuregelungen, die die Überwachungsintensität der Telekommunikation erhöhen könnten, in dem TKÜV-Entwurf enthalten: Definiert wird der „Übertragungsweg, der dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dient". Diese Definition stellt klar, dass Dienstleistungen, die über das TCP/IP Protokoll übertragen werden, ebenfalls von der Telekommunikationsüberwachung erfasst werden, also explizit auch das Internet. Auch die Definition der „zu überwachenden Kennung" ist technisch wesentlich offener als der Begriff der Rufnummer nach der bisherigen TKÜV. Mit Kennung ist die **Erfassung sämtlicher Kommunikation** – ob Voice-Mail, E-Mail, Surfen, mobiles oder herkömmliches Telefonieren – gemeint, die von einer zu überwachenden Person ausgeht. Auch wenn die Übermittlung von Telekommunikationsinhalten nicht zustande kommt, sollen nun Überwachungsdaten bereitgestellt werden. Nach dem TKÜV-Entwurf sind die Mobilfunkunternehmen gehalten, die **Angabe des Standortes des Mobilfunkgerätes** mit der größten Genauigkeit zu liefern. Diese Formulierung ist deshalb gewählt worden, weil bei neuen Kommunikationstechniken wie beispielsweise UMTS, die Lokalisierungsdaten präzise erfasst und weitergeleitet werden können.

Die Möglichkeiten zur Überwachung von Telekommunikationsdiensten, werden Stück für Stück erweitert – jetzt gehören dazu auch Dienste, die über das Internetprotokoll abgewickelt werden. Die Bürgerinnen und Bürger werden damit in ihrer freien und unbeobachteten Kommunikation immer weiter eingeschränkt.

3.2.4 Kommt die Vorratsdatenspeicherung durch die Hintertür?

Während der Entstehung des neuen TKG wurde heftig um die Vorratsdatenspeicherung der Verkehrsdaten gerungen, die einige Länder über den Bundesrat einführen wollten. Erfreulicherweise kam es letztendlich nicht dazu.

Der Bundesrat forderte noch fast bis zum Schluss der Beratungen, dass die Diensteanbieter sämtliche Verkehrsdaten, die beim Telefonieren, bei der Benutzung von SMS und bei E-Mails anfallen, sechs Monate lang gespeichert werden sollen. In der Entschließung vom 21. November 2003 (Abdruck im Anhang, Nr. 14) wandten sich die Datenschutzbeauftragten des Bundes und der Länder entschieden gegen diesen massiven Eingriff in das grundgesetzlich verankerte Fernmeldegeheimnis. Glücklicherweise konnte sich der Bundesrat nicht durchsetzen. Aber die Diskussion um die Vorratsdatenspeicherung kommt trotzdem nicht zur Ruhe. Neuen Zündstoff gab eine Initiative der Länder Frankreich, Irland, Großbritannien und Schweden. In einem Entwurf zu einem **EU-Rahmenbeschluss zur Vorratsdatenspeicherung von elektronischen Kommunikationsdaten** vom 28. April 2004 (Ratsdokument 8958/04) forderten sie eine Speicherung von Verkehrs- und Lokalisierungsdaten aller Telekommunikations- und Internetdienste von mindestens einem Jahr bis zu drei Jahren. Am 14. Oktober 2004 hat die Ratspräsidentschaft der EU eine überarbeitete Version des Rahmenbeschlusses zur Vorratsdatenspeicherung vorgelegt, der keine prinzipiellen datenschutzrechtlichen Verbesserungen vorsieht. Daneben hat die Generaldirektion Informationsgesellschaft sowie Justiz und Inneres der **Europäischen Kommission** eine öffentliche Konsultation zur Vorratsdatenspeicherung gestartet.

Die flächendeckende Vorratsspeicherung von Kommunikationsdaten ist ein massiver Eingriff in das **Fernmeldegeheimnis**, dem der Inhalt und die näheren Umstände der Telekommunikation unterliegen. Wer also mit wem wann und wie lange telefoniert hat, oder wer sich wann und wie lange auf welcher Internetseite befunden hat, ist auch davon erfasst. Eine Speicherung dieser Daten ist außer für betriebliche Zwecke, also beispielsweise für die Abrechnung, nur im Falle eines konkreten Verdachts für das Vorliegen einer Straftat von erheblicher Bedeutung und nur mit richterlichem Beschluss zulässig.

Aber nicht nur das Fernmeldegeheimnis wäre bei einer solchen Vorratsdatenspeicherung verletzt, sondern tangiert wäre auch das

Grundrecht auf **freie Meinungsäußerung** und **ungehinderte Unterrichtung** aus allgemein zugänglichen Quellen. Jede Suchanfrage an eine Suchmaschine würde nach dem Entwurf des Rahmenbeschlusses mitgespeichert werden. Eine Auswertung von Interessen, Vorlieben und politischen Präferenzen der Nutzenden wäre dann leicht möglich.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich schon wiederholt entschieden gegen eine Vorratsdatenspeicherung von Verkehrsdaten gewandt. Denn die flächendeckende und anlassunabhängige Speicherung aller Daten über die Nutzung öffentlicher Kommunikationsnetze schießt weit über das Ziel der Vorbeugung und Verfolgung von Straftaten hinaus. Der Entwurf des Rahmenbeschlusses verstößt gegen die Menschenrechtskonvention und gegen das Grundrecht auf unbeobachtete und freie Kommunikation.

Die Bundesregierung wurde von den Datenschutzbeauftragten des Bundes und der Länder aufgefordert, den Entwurf des Rahmenbeschusses über die Vorratsdatenspeicherung abzulehnen.

3.3 Melderegisterauskunft online

Einfache elektronische Melderegisterauskünfte können bald auch online erteilt werden. Nicht zuletzt die Nutzung des Internet als Transportweg erhöht jedoch die Risiken für die Verarbeitung der personenbezogenen Daten.

Bereits heute gibt es den Probebetrieb der einfachen elektronischen Melderegisterauskunft (eMA) mit einer **Portallösung** im Vorgriff auf das Meldegesetz Nordrhein-Westfalen, welches an die Vorgaben des Melderechtsrahmengesetzes angepasst wird. Hierdurch soll ermöglicht werden, Auskünfte in sehr kurzer Zeit elektronisch abzurufen. Bei der Anwendung handelt es sich um einen Teledienst mit allen Pflichten aus dem Teledienstedatenschutzgesetz. Nutzende dieses Verfahrens sind Großkundinnen und -kunden, die jeden Tag Datenbestände aus dem Melderegister benötigen. Melderegisteranfragen können nur durchgeführt werden, wenn ein Vertrag mit der Betreiberin oder dem Betreiber des Routers abgeschlossen worden ist, über den die eMA durchgeführt wird.

Die Grundstruktur des Verfahrens kann folgendermaßen dargestellt werden:

Großkundinnen und -kunden setzen beim durch Passwort zugriffsgeschützten Portal, dem zentralen eMA-Router, Auskunftsersuchen

zum Melderegister ab. Die Daten werden SSL verschlüsselt übertragen. Der eMA-Router bestellt die für die Bearbeitung der Aufträge notwendigen Daten bei den zuständigen Kommunen über eine sichere Verbindung. Die zurückgelieferten Auskünfte werden den Aufträgen zugeordnet und an die Kundinnen und Kunden weitergeleitet. Der eMA-Router betreibt **keine eigene Datenhaltung**, die über die Vorgangsdatenverarbeitung der Kundenaufträge hinausgeht. Die Daten werden nach Bearbeitung und nach Abrechnung gelöscht. Es entsteht schon deshalb kein virtuelles zentrales Melderegister, weil die Bearbeitung der Meldeanfragen bei den zuständigen Kommunen verbleibt. Für die Auftragsdurchführung muss die gesuchte Person mit Vor- und Familiennamen sowie mit mindestens zwei weiteren Daten im Antrag benannt sein, damit eine hinreichend sichere Identifizierung des oder der Betroffenen möglich ist.

Es ist insbesondere darauf zu achten, die zu schaffenden Portale so zu gestalten, dass die Vertraulichkeit der Kommunikation sichergestellt ist, keine zentralen Melderegister entstehen sowie Anfrage- und Auskunftsdaten nur im zwingend notwendigen Umfang zwischengespeichert werden. Es dürfen in der „Online-Welt" nicht neue Datenbanken geschaffen und Verknüpfungen zugelassen werden, die in der „Offline-Welt" nicht erlaubt wären.

3.4 Einzelfragen zu Telekommunikation, Internet und E-Mail

3.4.1 Etwas mehr Schutz gegen unerwünschte Werbung per Telekommunikation erreicht

Viele ärgern sich über die lästige Werbeflut. Mit einer Gesetzesänderung soll versucht werden, sie immerhin etwas einzudämmen.

Am 08.07.2004 ist die Neufassung des Gesetzes gegen den unlauteren Wettbewerb (UWG) (BGBl. I S. 1414) in Kraft getreten. Damit ist der Gesetzgeber der Forderung nach Umsetzung unter anderem des Art. 13 der EG-Richtlinie 2002/58 „Datenschutzrichtlinie für elektronische Kommunikation" in deutsches Recht gefolgt.

Wie bisher ist die **Telefonwerbung** nur mit Einwilligung der Verbraucherin oder des Verbrauchers erlaubt. Im gewerblichen Bereich muss hierfür zumindest eine mutmaßliche Einwilligung der Werbeadressatinnen und -adressaten gegeben sein. Die **Werbung mit Mitteln der elektronischen Kommunikation** bedarf der Einwilligung der Adressatinnen und

Adressaten. Eine Ausnahme lässt das Gesetz zu, falls das Unternehmen die E-Mail im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erlangt hat. Es darf diese zur **Direktwerbung** für eigene ähnliche Waren oder Dienstleistungen nutzen, sofern die Kundin oder der Kunde jederzeit die Möglichkeit hat, einer solchen Werbung zu widersprechen.

Ungeachtet der gesetzlichen Änderungen sowie der Klage- und Beschwerdemöglichkeiten bleibt ein **verantwortlicher Umgang mit Mail-Adressen** der beste Schutz vor Spam. Grundsätzlich sollte die Mail-Adresse nur den Personen und Institutionen gegeben werden, die vertrauenswürdig sind. Beim Versand von Mails an mehrere Personen, die einander unbekannt sind, ist die Möglichkeit der Blind Copy zu nutzen, damit die Adressen der jeweiligen Dritten für die Empfänger und Empfängerinnen verborgen bleiben. Vor jeder Nutzung von E-Commerce-Angeboten sind die Nutzungsbedingungen und Datenschutzerklärungen genau zu studieren. Für Newsgroups und Chats sollte eine zweite Mail-Adresse genutzt werden, die gegebenenfalls geändert werden kann. Längere und ungewöhnliche Zeichenfolgen als Adressenbestandteil verhindern das Erraten der Adresse durch Zufallsgeneratoren. Soweit die eigene Adresse auf einer eigenen Homepage veröffentlicht wird, sollte diese als Grafik dargestellt werden. Auf Spam und Werbemails ist nach Möglichkeit nicht zu antworten. Auch die beigefügten Abmeldelinks sollten besser ignoriert werden. Darüber hinaus empfiehlt sich noch der Einsatz von Spam-Filtern und Virenschutzsoftware.

Wegen der unüberschaubaren Masse an Spam und Werbung haben auch Vereine, Unternehmen und die Provider diesem Phänomen den Kampf angesagt. **Spam-Abwehr** ist das Thema, welches momentan von allen Seiten angegangen wird. Gearbeitet wird mit Blacklists, mit der Verschleierung von Adressen, mit Verfahren, die eine komplizierte Prüfsummenbildung zur Erkennung von Spam einsetzen sowie mit einer automatischen oder manuellen Inhaltsanalyse. Eine generelle Bewertung der Verfahren ist nicht möglich.

Häufig werden Spamfilter neben dem eigentlichen E-Mail-Dienst als zusätzlicher Dienst angeboten. Dabei sind die Nutzer und Nutzerinnen vor Vertragsschluss ausführlich über die näheren Umstände zu informieren. Semantische oder manuelle Spamfilter dürfen nur mit ausdrücklicher freiwilliger Zustimmung der Empfängerin oder des Empfängers sowie mit Zustimmung der Betriebs- oder Personalräte eingesetzt werden.

3.4.2 Die private Homepage

Bei der Veröffentlichung personenbezogener Daten im Internet, sei es die Darstellung eines Familienstammbaums oder die Beschreibung von Schulfesten oder Klassenfahrten durch Schüler und Schülerinnen, wird häufig vorgetragen, dass es sich um eine rein private Homepage handele und daher eine Anwendung des BDSG auszuschließen sei. Ein Urteil des Europäischen Gerichtshofes (EuGH) von November 2003 ist in diesem Zusammenhang von Bedeutung.

Auf die Vorlagefrage eines schwedischen Gerichts war darüber zu urteilen, ob die Veröffentlichung von Daten dritter Personen wie Namen, Telefonnummern und Angaben zu Freizeitbeschäftigungen auf einer Homepage im Internet als **automatisierte Verarbeitung** personenbezogener Daten im Sinne der EG-Datenschutzrichtlinie 95/46 anzusehen sei und ob diese Verarbeitung nicht eine rein private oder familiäre Tätigkeit darstellen könne und somit als Ausnahme der Richtlinie zu betrachten sei.

Der EuGH stellt hierzu fest, dass der in der Richtlinie verwendete Wortlaut „Verarbeitung personenbezogener Daten" sich auf alle Informationen über eine bestimmte oder bestimmbare Person bezieht. Damit ist die Nennung des Namens einer Person in Verbindung mit weiteren Angaben erfasst und die Übermittlung, Verbreitung oder jede andere Form der Bereitstellung der Daten im Internet ist unter den Begriff „Verarbeitung" zu subsumieren. Die Ausnahme, dass eine Verarbeitung personenbezogener Daten zu **persönlichen und familiären Zwecken** nicht in den Anwendungsbereich der Datenschutzvorschriften fällt, ist nach dem Urteil des EuGH dahin auszulegen, dass mit ihr nur Tätigkeiten gemeint sind, die zum Privat- oder Familienleben von Einzelpersonen gehören. Dies ist jedoch bei der Verarbeitung personenbezogener Daten Dritter im Internet nicht der Fall, da durch deren Veröffentlichung im Internet diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden.

Der private Charakter einer Verarbeitung personenbezogener Daten Dritter verliert sich, sobald eine Seite im Internet für die Allgemeinheit erreichbar ist.

3.4.3 Mobbing im Internet

Nicht nur unseriöse Warndateien und zweifelhafte Unternehmen nutzen das Medium des Internet in rechtswidriger Weise als Pranger (vgl. 16. Datenschutzbericht 2003 unter 8.4.5, S. 94 ff.), sondern auch Privatpersonen. So inszenieren manche Leute ihre privaten Auseinandersetzungen als öffentliches Schauspiel auf der weltweit einsehbaren Bühne des World Wide Web.

In einem besonderen Fall mobbten vier Schüler ihre Mitschülerinnen und Mitschüler aus der achten Klasse eines Gymnasiums. Auf einer gemeinsamen Web-Seite veröffentlichten sie zum einen kleine Videosequenzen (Zeichentrick-Animationen), in denen Strichmännchen geschlagen, misshandelt sowie auf unterschiedliche Weise massakriert und hingerichtet wurden. Ein Bezug zu konkreten Personen wurde in den Sequenzen selbst nicht hergestellt. Nach Auskunft von Eltern teilten die vier Betreiber der Seite ihren Mitschülerinnen und Mitschülern mündlich mit, wen die Strichmännchen symbolisieren sollten. Eindeutiger war der **Personenbezug** bei einer zweiten Rubrik der Internet-Seite. Dort veröffentlichten die vier unter dem Titel „news" abwertende „Nachrichten" und abfällige Kommentare über Mitschülerinnen und Mitschüler ihrer Klasse. Das Gästebuch der Seite zeigte, dass leider nicht nur die vier Schüler ihre Freude an den brutalen Darstellungen und personenbezogenen Gemeinheiten hatten. Nach einem Anruf bei den Eltern wurde die entsprechende Seite innerhalb von einer Stunde gesperrt und aus dem öffentlich zugänglichen Netz genommen.

Datenschutzrechtlich ist das Veröffentlichen personenbezogener Daten im Internet keineswegs eine „ausschließlich persönliche oder familiäre Tätigkeit". Vielmehr werden damit Daten weltweit zum Abruf bereitgehalten. Das ist grundsätzlich nur mit der ausdrücklichen Einwilligung der Betroffenen erlaubt.

3.4.4 Personenbezogene Internet-Umfrage einer Initiative

Das Internet bietet als modernes Informationsmedium die Möglichkeit, Daten und Informationen jeder Art auf schnellem und einfachem Weg an möglichst viele Personen in Umlauf zu bringen. So dient das Internet immer wieder der Durchführung von Online-Umfragen. Werden in diesem Zusammenhang personenbezogene Informationen im Internet

veröffentlicht, können datenschutzrechtliche Belange der betroffenen Personen verletzt werden.

Grundsätzlich dürfen personenbezogene Daten nur mit Einwilligung der betroffenen Personen ins Internet gestellt werden. Als einzige Ausnahme kommt der Fall in Betracht, dass die Daten bereits vorher **im Internet öffentlich zugänglich** waren. Namentlich genannte oder sonst identifizierbare Personen haben schutzwürdige Interessen, die zu beachten sind. Schließlich kann weltweit ein unbestimmter Personenkreis auf die Daten im Internet zugreifen. Sofern es sich nicht um öffentlich zugängliche Daten entsprechend der genannten Ausnahme handelt, besteht für die betroffenen Personen insbesondere die Gefahr, dass diskriminierende personenbezogene Daten und Informationen eine Prangerwirkung auslösen. Zudem sind derart veröffentlichte Informationen gerade wegen des unbegrenzten Zugriffs kaum vollständig rückholbar.

Werden darüber hinaus personenbezogene **Werturteile**, die zuvor im Wege einer Umfrage erhoben wurden, im Internet als Umfrageergebnis öffentlich zugänglich gemacht, ist dies anders zu bewerten. Eine personenbezogene Veröffentlichung dieser Informationen ist immer nur mit **ausdrücklicher Einwilligung** der betroffenen Personen zulässig. Daher ist eine Veröffentlichung von Umfrageergebnissen im Internet ohne Einwilligung in jedem Fall so zu gestalten, dass diese keine personenbeziehbaren Informationen oder Werturteile über einzelne Personen enthält.

In Nordrhein-Westfalen wollte im Berichtszeitraum eine Sozialinitiative mittels eines virtuellen Fragebogens auf ihrer Internetseite Erwerbslose über ihre persönlichen Erfahrungen mit der örtlichen Agentur für Arbeit befragen. In diesem Fragebogen wurden die Beschäftigten der Agentur für Arbeit konkret mit Namen und Zimmernummer aufgelistet, um von den Umfrageteilnehmenden namentlich bewertet zu werden. Schließlich sollten die Ergebnisse der **Umfrage** auf der Internetseite der Initiative veröffentlicht werden. Nachdem die Initiative über die datenschutzrechtliche Unzulässigkeit der Aktion unterrichtet worden war, entfernte sie umgehend die Namensliste der Beschäftigten sowie sämtliche personenbezogene Fragen aus dem virtuellen Fragebogen. Die bis zu diesem Zeitpunkt personenbezogen erhobenen Daten hat die Initiative gelöscht und die Umfrage anonym ausgewertet.

Wer das Internet für Online-Umfragen nutzen möchte, muss neben den technischen Voraussetzungen sicherstellen, dass die datenschutzrechtlichen

Belange betroffener Personen berücksichtigt werden. Liegt keine entsprechende Einwilligung vor, hat die Umfrage anonym zu erfolgen und darf keine personenbeziehbaren Informationen oder Werturteile über einzelne Personen enthalten.

3.4.5 Mitteilungen aus Zwangsversteigerungs- und Insolvenzverfahren im Internet durch private Stellen

Die Veröffentlichung von Zwangsversteigerungs- und Insolvenzdaten im Internet durch private Stellen, beispielsweise Verlage, ist unzulässig, da hierfür keine Rechtsgrundlage besteht.

Teilweise war festzustellen, dass die Eingabe eines Personennamens in eine herkömmliche Internet-Suchmaschine einen Link zu einer durch einen Verlag veröffentlichten Liste von **Privatinsolvenzen** anzeigte. Die schon als belastend genug empfundene Privatinsolvenz wird so zu einem weltweit abrufbarem Stigma. Die Daten waren schließlich für jede Internetnutzerin und jeden Internetnutzer – teilweise nach vorheriger, aber voraussetzungsfreier Registrierung – ohne weiteres zugänglich.

Für den Bereich der Insolvenzdaten macht § 9 Abs. 2 Insolvenzordnung (InsO) deutlich, dass die Veröffentlichung im Internet **nur** durch die dort genannten staatlichen **Gerichte** erfolgen darf; andere Veröffentlichungsstellen werden im Gesetz nicht genannt. Insbesondere ist die Veröffentlichung von Zwangsversteigerungs- und Insolvenzdaten im Internet nicht durch § 28 Abs. 1 Nr. 3 BDSG gedeckt. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Eine Erlaubnis aufgrund dieser Vorschrift scheitert bereits an der Voraussetzung der Nutzung der Daten für die Erfüllung eigener Geschäftszwecke. Dies ist bei der Veröffentlichung von Zwangsversteigerungs- und Insolvenzdaten durch Private nicht der Fall, da die Veröffentlichung der Daten hier zum Selbstzweck wird und die Daten sich quasi in eine Ware verwandeln, die Ziel und Gegenstand der Verarbeitungstätigkeit bestimmen. In keinem der untersuchten Fälle diente die Veröffentlichung der Daten den Geschäftzwecken der verantwortlichen Stelle;

sie war lediglich ein Extra-Service für die Kundinnen und Kunden im Rahmen anderer Dienstleistungen, etwa Fachpublikationen zum Insolvenzrecht.

Auch § 29 BDSG ist keine geeignete Rechtsgrundlage. Nach der ersten Alternative des § 29 Abs. 2 BDSG wäre die Übermittlung nur an Personen oder Stellen zulässig, die ein **berechtigtes Interesse** an der Kenntnis der Daten nachweisen können. Genau daran fehlt es aber, wenn Schuldnerdaten auf weltweit offenen Internetseiten präsentiert und von jeder und jedem ohne Zugriffskontrolle abgerufen werden können. Auch die zweite Alternative des § 29 Abs. 2 BDSG kommt als Rechtsgrundlage nicht in Betracht, weil die Daten nicht Zwecken der Werbung oder Markt- bzw. Meinungsforschung dienen. Die überprüften privaten Stellen, insbesondere Verlage, veröffentlichen die Daten lediglich als besonderen Service für ihre meist im Wirtschaftsbereich angesiedelten Kundinnen und Kunden. Zudem bezieht sich § 29 BDSG seinem Sinn und Zweck nach auf Werbung für gerade die Personen, deren Daten übermittelt werden sollen. Davon kann hier keine Rede sein.

Ebenso wenig kann das Grundrecht der Pressefreiheit als Rechtfertigung für eine Veröffentlichung von Insolvenz- und Zwangsversteigerungsdaten herangezogen werden. Das **Medienprivileg** – das Presseorgane auch für die Veröffentlichung von Publikationen im Internet in Anspruch nehmen können – verlangt eine journalistisch-redaktionelle oder literarische Verarbeitungsabsicht, also einen Beitrag zur Meinungsbildung. Die Pressefreiheit ist daher nicht einschlägig bei Anzeigen- oder Offertenblättern, wenn diese nicht zusätzlich in nennenswertem Umfang Informationen redaktionell aufbereiten und abdrucken. Für Veröffentlichungen von amtlichen Mitteilungen oder aus dritten Quellen unverändert übernommenen Texte im Internet gilt das Medienprivileg des § 41 BDSG folglich nicht.

Die Veröffentlichung von Zwangsversteigerungs- und Insolvenzdaten von natürlichen Personen im Internet ist unzulässig, wenn sie von privater Seite aus erfolgt und keine Einwilligung der Betroffenen vorliegt.

4 Videoüberwachung

4.1 Videoüberwachung an Schulen

Immer mehr Schulträger überwachen Schulhöfe oder Schulgebäude mit Videokameras. Aber auch innerhalb der Schulen meinen viele, nicht mehr ohne Videoüberwachung auskommen zu können.

Videoüberwachung verträgt sich grundsätzlich nicht mit dem Auftrag der Schulen, Schülerinnen und Schüler auf ihrem Weg zu selbstbestimmten, mündigen Persönlichkeiten zu unterstützen. Deshalb gehören Videokameras nicht in Unterrichtsräume, schon gar nicht während des Unterrichts. Dort sind nämlich in erster Linie Lehrerinnen und Lehrer zur Aufsicht über die Schülerinnen und Schüler verpflichtet. Insoweit sind Umstände, die eine Videoüberwachung in diesem Bereich erforderlich erscheinen ließen, nur schwer vorstellbar. Die Videoüberwachung käme allenfalls bei **konkreten Gefährdungen** erheblicher Rechtsgüter in Frage. Rein abstrakte Gefahren können eine dauerhafte Videoüberwachung dagegen auch dann nicht rechtfertigen, wenn Sachwerte von hohem Wert geschützt werden sollen. So wurde in einem Fall schon die bloße Inbetriebnahme von neuen Informatikräumen, die mit teurer Hard- und Software ausgestattet waren, zum Anlass einer Überwachung mit Videokameras genommen, um eventuelle Beschädigungen zu verhindern oder gegebenenfalls besser verfolgen zu können. Hier offenbart sich die Unverhältnismäßigkeit einer Videoüberwachung: Ohne zunächst andere Möglichkeiten zum Schutz der Sachgüter in Erwägung zu ziehen und insbesondere das Verantwortungsbewusstsein der Schülerinnen und Schüler zu fördern, wurde Videoüberwachung als einzige Lösung präsentiert. Leider hat auch das Ministerium für Schule, Jugend und Kinder diesen erzieherischen Impetus außer Acht gelassen und eine Videoüberwachung nur davon abhängig gemacht, dass die betroffenen Personen wirksam in die Datenverarbeitung eingewilligt haben.

Auch die Beobachtung des Schulhofes oder des Eingangsbereichs zum Schulgebäude stellt **während des laufenden Schulbetriebs** regelmäßig einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte der Schülerinnen und Schüler sowie der Lehrerinnen und Lehrer dar. Diese können sich der Überwachung nicht entziehen und sind in ihrer selbstbestimmten Bewegungsfreiheit auf dem Schulgelände in erheblicher Weise eingeschränkt. Auch diesbezüglich ist – wenn auch nicht in gleichem Maße wie während des Unterrichts – zu berücksichtigen, dass die Lehrerinnen und

Lehrer eine Aufsichtspflicht haben. Zudem dürfte anzunehmen sein, dass mit der regelmäßigen Bevölkerung des Schulgeländes während der Unterrichtszeiten im Hinblick auf möglichen Vandalismus, mit dem eine Videoüberwachung in den meisten Fällen gerechtfertigt wird, eine verstärkte soziale Kontrolle einhergeht.

Eine Videoüberwachung an Schulen kann somit nur **ausnahmsweise** und grundsätzlich nur **außerhalb der Unterrichtszeiten** gerechtfertigt sein. Gleichwohl muss auch in diesen Fällen abgewogen werden, ob die Videoüberwachung in dem vorgesehenen oder bereits praktizierten Umfang das zur Wahrung des Hausrechts des Schulträgers erforderliche und verhältnismäßige Mittel ist oder ob nicht andere Schutzmaßnahmen (etwa der Einsatz von Scheinwerfern, Bewegungsmeldern oder eine Einzäunung des Schulgeländes) ergriffen werden müssten, um den verfolgten Zweck zu erreichen. Darüber hinaus sind die bei jeder Videoüberwachung zum Schutz der Persönlichkeitsrechte der Betroffenen bestehenden rechtlichen Einschränkungen zu beachten. Hierzu gehört insbesondere, das aufgezeichnete Material nur anlassbezogen in Augenschein zu nehmen und die Bilder im Übrigen unbesehen zu löschen, die Speicherdauer nur so lange wie unbedingt erforderlich zu wählen, den Kreis der zugriffsberechtigten Personen so eng wie möglich zu fassen sowie die Videoüberwachung durch Hinweisschilder bereits vor Betreten der beobachteten Bereiche erkennbar zu machen.

Videoüberwachung an Schulen ist in der Regel allenfalls außerhalb der Unterrichtszeiten zu rechtfertigen. Eine Überwachung in Unterrichtsräumen während des laufenden Unterrichts verletzt die Persönlichkeitsrechte der betroffenen Schülerinnen und Schüler sowie Lehrerinnen und Lehrer und ist deshalb mit dem schulischen Erziehungs- und Bildungsauftrag nicht in Einklang zu bringen.

4.2 Sonnenbad auf dem Balkon – live im Internet

Mit dem Spaß am technischem Fortschritt gehen häufig unbedachte Beeinträchtigungen schützenswerter Interessen einher. Private Web-Cams können zwar ohne großen Aufwand installiert und alle gefertigten Aufnahmen ins Internet übertragen werden. Welche schwerwiegenden Eingriffe in Persönlichkeitsrechte anderer damit verbunden sein können, wird zumeist nicht bedacht.

So wurde von einer Privatperson, die im 12. Stock eines Hochhauses wohnt, eine WebCam in Betrieb genommen. Die Kamera war über das Internet steuerbar und konnte auf verschiedene Punkte des Ortes ausgerichtet werden. Die entsprechenden Bilder konnten auf jedem PC, der mit dieser Website verbunden war, gespeichert und beliebig weiterverarbeitet werden. Das bleibt nur solange harmlos, wie lediglich Übersichtsbilder aufgenommen werden können. Sobald jedoch durch Zoomen Personen erkennbar werden, ist deren allgemeines Persönlichkeitsrecht verletzt. Die Beeinträchtigung ist besonders dann schwerwiegend, wenn – wie in unserem Fall bei der WebCam anfangs möglich – der Wohnungsbereich einschließlich Balkon oder Terrasse in den Blick genommen werden können. In diesem Bereich der Privatsphäre stellt jede Beobachtung – von einer Veröffentlichung der Bilddaten im Internet ganz zu schweigen – eine **erhebliche Verletzung der Persönlichkeitsrechte** der Bewohnerinnen und Bewohner dar. Wohnung und der zur Wohnung gehörende Balkon oder die Terrasse sind dem höchstpersönlichen Lebensbereich zuzurechnen, der gegen Eingriffe in besonderer Weise geschützt ist. Selbst bei einer reduzierten Bildqualität ist es für Personen, die die örtlichen Gegebenheiten kennen, unschwer möglich, die aufgenommenen Menschen zu identifizieren. Kurz nach unserem Tätigwerden wurden die Zoomfunktion an der WebCam abgestellt und die Ausrichtung der Kamera in der Weise verändert, dass Wohnhäuser nicht mehr unmittelbar angesteuert werden konnten.

Eine vergleichbare Beeinträchtigung war durch WebCam-Aufnahmen eines Hauses ermöglicht worden, weil bei Dunkelheit erkennbar war, ob die alleinstehende Bewohnerin in ihrer Wohnung anwesend war. Verständlicherweise war diese Bewohnerin erschrocken, als sie im Internet ihre eigene Wohnung gut identifizierbar entdecken musste. Das Haus ist inzwischen nicht mehr im Internet beobachtbar.

Der besonderen Schutzbedürftigkeit des Wohnbereichs hat der Gesetzgeber erst jüngst im Rahmen eines Strafrechtsänderungsgesetzes durch einen neuen § 201a StGB Rechnung getragen. Hiernach wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer von einer anderen Person, die sich in einer Wohnung oder einen gegen Einblick besonders geschützten Raum befindet, **unbefugt Bildaufnahmen herstellt** oder überträgt. Diese Vorschrift ergänzt die Regelung des § 33 Kunsturhebergesetz (KUG), nach der eine Verletzung des Rechts am eigenen Bild (§§ 22, 23 KUG) strafbewehrt sein kann. Darüber hinaus bestehen für die Betroffenen auf Grund der Verletzung der

Persönlichkeitsrechte gegebenenfalls zivilrechtliche Abwehr- und/oder Schadensersatzansprüche entsprechend der §§ 1004, 823 des Bürgerlichen Gesetzbuchs.

Die Beobachtung von Personen im Internet über eine WebCam stellt – insbesondere im Bereich ihrer Privatsphäre – einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Jeder, der WebCam-Aufnahmen ins Netz stellt, ist dafür verantwortlich, dass er weder Personen abbildet, noch bestimmte Verhaltensweisen von Personen öffentlich macht.

4.3 Wer ein Taxi benutzt, wird videoüberwacht!

Die zunehmende Überwachung von Gebäuden, öffentlichen Plätzen und Verkehrsmitteln durch Videokameras bereitet Unbehagen. Nun werden in Taxis Videoaufnahmen von Fahrgästen gefertigt.

Die Nutzung eines Taxis steht – wie die anderen öffentlichen Verkehrsmittel auch – jedem Menschen offen (allgemeine Beförderungspflicht). Taxis sind daher öffentlich zugänglich, so dass eine Videoüberwachung nur unter den Voraussetzungen des § 6b BDSG vorgenommen werden darf. Zweck der Videoüberwachung in Taxis wird in der Regel die Verhinderung von Überfällen sein. Soweit konkrete Vorkommnisse passiert sind, kann eine Überwachung im Rahmen der Wahrnehmung des Hausrechts durch das Taxiunternehmen in Betracht kommen, also zur Abwehr von Gefahren für Leib, Gesundheit oder Freiheit der Fahrerinnen und Fahrer zulässig sein. Bei jeder Prüfung eines Einsatzes von Videoüberwachung muss allerdings beachtet werden, dass schon die **Beobachtung** von Fahrgästen im Taxi einen schwerwiegenden Eingriff in ihr allgemeines Persönlichkeitsrecht darstellt. Die **Aufnahme** von Fahrgästen muss daher zur Gefahrenabwehr erforderlich und verhältnismäßig sein; es dürfen keine schutzwürdigen Interessen der Betroffenen überwiegen. Sie überwiegen aber, wenn von den zu befördernden Personen in keinem Fall ein Angriff auf das Fahrpersonal oder eine nachhaltige Beschädigung des Taxis zu erwarten ist. Dann darf keine Beobachtung und erst recht keine Aufzeichnung stattfinden. Es ist nicht ersichtlich, aus welchen Gründen eine Videoüberwachung beispielsweise älterer Fahrgäste oder von Müttern mit Kindern notwendig und angemessen sein sollte. Erforderlich ist die Videoüberwachung außerdem erst dann, wenn es keine andere, weniger eingreifende Schutzmaßnahme gibt. Dasselbe gilt für die Aufzeichnung der Bilder.

In einer nordrhein-westfälischen Stadt betreiben nahezu alle dort ansässigen Taxiunternehmen rund um die Uhr ein Überwachungssystem, das automatisch über das Zündschloss aktiviert wird. Mit dem Öffnen der Autotüren durch die Fahrgäste erstellt eine Kamera von jedem Fahrgast mehrere Bilder. Es ist mit dem so installierten System der Fahrerin oder dem Fahrer technisch nicht möglich, das System situationsbedingt selbst einzuschalten oder aber – soweit keine Gefahrenlage besteht – ausgeschaltet zu lassen. Die Vereinigung der Taxiunternehmen hat behauptet, dass eine eigene Entscheidungsmöglichkeit den Schutz der Fahrerinnen und Fahrer beeinträchtigen würde.

Nunmehr ist von den Taxiunternehmen zu überprüfen, ob eine Videoüberwachung in dem Umfang, wie sie betrieben wird, zur Abwehr von Gefahren für Leib, Gesundheit oder Freiheit ihrer Fahrerinnen und Fahrer überhaupt erforderlich ist. Dabei sind Vorkommnisse und Umstände nachzuweisen, die Veranlassung geben, eine Videoüberwachung in den Taxis weiterhin als erforderlich anzusehen. Bei einer noch bestehenden Gefahrenlage müsste auch überprüft werden, ob nicht durch den Einbau eines Schalters das Überwachungssystem erst dann aktiviert wird, wenn die Fahrerin oder der Fahrer es für erforderlich hält, weil nach eigener Beurteilung eine **bedrohliche Situation** entstehen könnte. Diese Beurteilung kann unter Umständen bereits vor einer konkreten Fahrt geschehen, etwa bei Einbruch der Dunkelheit, bei einer Fahrt zu einem als unsicher eingeschätzten Auftrag oder vor Aufnahme eines bestimmten Fahrgastes. Es wäre auch zu prüfen, ob nicht ein GPS gestütztes Notsignal an die Notrufzentrale einen ausreichenden Schutz bietet, so dass der Einsatz eines Videoüberwachungssystems eingeschränkt werden könnte. Dem Gebot der Datenvermeidung wäre damit Rechnung getragen.

Eine flächendeckende rund um die Uhr erfolgende Beobachtung in Taxis sowie eine damit verbundene automatische Registrierung aller Fahrgäste greift unverhältnismäßig in das Recht der Fahrgäste ein, Taxis als öffentliche Verkehrsmittel prinzipiell auch unbeobachtet nutzen zu können.

4.4 Videoüberwachung am Arbeitsplatz

Vertrauen ist gut, Kontrolle ist besser. Weiterhin versuchen viele Betriebe, diese Redewendung sinngemäß zur Vorbeugung von Straftaten am Arbeitsplatz in die Praxis umzusetzen.

Nunmehr hat das Bundesarbeitsgericht (Beschluss vom 29.06.2004 - 1 ABR 21/03 -) zugunsten der Beschäftigten entschieden, dass die dauerhafte, verdachtsunabhängige **Videoüberwachung der Belegschaft eines Briefverteilungszentrums** unverhältnismäßig und als ungerechtfertigter Eingriff in das grundrechtlich geschützte allgemeine Persönlichkeitsrecht der Beschäftigten zu werten ist. Das Gericht stellt zwar ausdrücklich klar, dass dem Persönlichkeitsrecht, das auch das Recht am eigenen Bild umfasst, kein absoluter Vorrang einzuräumen sei und deshalb stets eine Interessenabwägung im Einzelfall zu erfolgen habe. Dennoch verdeutlicht der dem Beschluss zugrunde liegende Fall, dass die Rechtsprechung dem Schutz des Persönlichkeitsrechts auch im Verhältnis zu anderen grundrechtlich geschützten Rechten, wie hier zum Beispiel dem Postgeheimnis oder der Sicherheit des Briefverkehrs, einen hohen Stellenwert beimisst.

Ein Staatliches Amt für Arbeitsschutz machte darauf aufmerksam, dass bei einem mittelständischen Unternehmen Überwachungskameras im Toilettenbereich installiert wären. Die Überprüfung hat ergeben, dass mit einer Kamera Bilder aus dem Vorraum einer Herrentoilette gemacht und diese PC-unterstützt aufgezeichnet wurden. Der Unternehmer begründete die Videoüberwachung damit, dass die Toilettenanlagen fortwährend beschädigt, insbesondere aber immer wieder erheblich verunreinigt worden wären. Der Betriebsrat hatte der Installation der Überwachungskamera zugestimmt.

Da die Videoüberwachung innerhalb des Unternehmens erfolgte, findet die Regelung des § 6b BDSG zur Videoüberwachung öffentlich zugänglicher Räume keine Anwendung. Allerdings gilt wegen der eingesetzten Technik der digitalen Speicherung des Bildmaterials § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach rechtfertigen die berechtigten Interessen der verarbeitenden Stelle eine Verwendung personenbezogener Daten nur, solange kein Grund zur Annnahme besteht, dass die Speicherung gegen ein überwiegend schutzwürdiges Interesse der Betroffenen verstößt. Solche Interessen überwiegen nahezu immer, wenn die Intimsphäre verletzt wird. Da der Vorraum über die üblichen Waschgelegenheiten verfügt, ist davon auszugehen, dass bei Benutzung auch hier die Intimsphäre der Mitarbeiter tangiert ist. Darüber hinaus ist nach der Rechtsprechung eine Videoüberwachung am Arbeitsplatz nur durch besondere Sicherheitsinteressen des Arbeitgebers gerechtfertigt. Auch durch Mitbestimmung des Betriebsrats lässt sich diese Maßnahme nicht legitimieren. Das Unternehmen ist der Empfehlung gefolgt, die Videoüberwachung abzuschalten.

Auch im Arbeitsverhältnis ist den Persönlichkeitsrechten der Beschäftigten Rechnung zu tragen.

4.5 Videoüberwachung in Umkleidekabinen eines Fitness-Studios

Fit for Fun – es liegt auf der Hand, dass dies nicht Motto einer Überwachung von Umkleide-, Dusch- und Toilettenräumen in Sportstätten sein darf. Dennoch gehen einige Sportstätten bei Einrichtung und Betrieb von Videoüberwachungsanlagen erschreckend sorglos mit dem allgemeinen Persönlichkeitsrecht ihrer Besucherinnen und Besucher um.

Aus Anlass eines Diebstahls ließ beispielsweise der Betreiber eines Fitness-Studios zwei Videokameras in den **Damenumkleidekabinen** installieren, um die Täterin oder den Täter zu überführen. Die im Rahmen der Videoüberwachung gewonnenen Bilder wurden auf der Festplatte eines PC aufgezeichnet. Dass die von der Überwachung Betroffenen auch nackt der Beobachtung preisgegeben waren, hielt der Verantwortliche für nicht weiter problematisch. Er verwies darauf, dass die Aufzeichnungen nur durch zwei weibliche Angestellte nach doppelter PIN-Eingabe gesichtet werden könnten. Hinweisschilder, die auf den Umstand der Beobachtung aufmerksam gemacht hätten, fehlten in der Umkleidekabine.

Rechtsgrundlage für die Videoüberwachung im nicht öffentlichen Bereich, das heißt durch private Personen oder Unternehmen, ist die Regelung des § 6b Abs. 1 BDSG, soweit es um die Überwachung öffentlich zugänglicher Räume geht. Die in den Umkleidekabinen durchgeführte Videoüberwachung wäre nach dieser Vorschrift zulässig gewesen, wenn sie für einen der dort genannten Zwecke erforderlich gewesen wäre und schutzwürdige Interessen der davon Betroffenen die Überwachung nicht ausgeschlossen hätten. Berechtigte Zwecke sind auch die Aufklärung und Verhinderung von Straftaten wie die des Diebstahls. Jedoch ist die zu diesem Zweck in Bereichen wie öffentlich zugänglichen Umkleide-, Dusch- und Toilettenräumen durchgeführte Videoüberwachung, die naturgemäß in besonderer Weise die Intimsphäre der Betroffenen berührt, grundsätzlich **unzulässig**. Gleiches gilt für eine Videoüberwachung von nicht öffentlich zugänglichen Umkleide-, Dusch- und Toilettenräumen, auf die die Vorschrift des § 28 Abs. 1 Nr. 2 BDSG Anwendung findet. Auch nach dieser Regelung wäre eine Videoüberwachung nur dann zulässig, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich

ist und schutzwürdige Interessen der Betroffenen nicht entgegen stehen. Diese Voraussetzungen sind jedoch bei einer Überwachung in Umkleide-, Dusch- und Toilettenräumen niemals gegeben.

Regelmäßig wird es eine Möglichkeit geben, die mit der Überwachung verfolgten Zwecke auch auf andere, weniger einschneidende Weise zu erreichen. So könnte der Schutz vor Diebstählen beispielsweise auch durch den Einbau von Schließfächern und regelmäßige Kontrollgänge des Personals erreicht werden. Oder aber der Umkleidebereich könnte räumlich vom Schrankbereich getrennt und die Videoüberwachung nur in letzterem vorgesehen sein. Die Videoüberwachung im Umkleidebereich selbst ist daher in der Regel **nicht erforderlich**.

Einer Überwachung von Umkleide-, Dusch- und Toilettenräumen stehen zudem stets auch die schutzwürdigen Interessen der Benutzerinnen und Benutzer entgegen. Sie werden durch die Beobachtung der dort vorgenommenen Verrichtungen in nicht hinnehmbarer Weise in ihrem allgemeinen Persönlichkeitsrecht beeinträchtigt. Das Aus- und Ankleiden betrifft ebenso wie der Toilettengang den Intimbereich der Betroffenen, die sich bei diesen Handlungen unbeobachtet fühlen. Wenn die Überwachung den gesamten Bereich der Umkleide-, Dusch- oder Toilettenräume erfasst, aber auch dann, wenn nicht deutlich durch entsprechende Hinweisschilder auf die eingesetzten Kameras hingewiesen wird, haben die Betroffenen noch nicht einmal eine Chance, der Beobachtung auszuweichen. Der mit der Videoüberwachung im Ausgangsfall verfolgte legitime Zweck der Aufklärung und Vorbeugung von Diebstählen war daher geringer zu gewichten als die schutzwürdigen Interessen der sich im überwachten Bereich aufhaltenden Personen. Dementsprechend wurde der Betreiber des Fitness-Studios aufgefordert, die Kameras aus den Damenumkleidekabinen zu entfernen.

Auch die Überwachung eines **Vorraums einer Kundentoilette** kann problematisch sein, wenn etwa - wie in einem anderen Fall - die Kamera **versteckt** über den Waschbecken angebracht ist und kein Hinweisschild auf den Umstand der Beobachtung aufmerksam macht. Auch hier sind die Betroffenen in besonderer Weise in ihrem **Intimbereich** berührt.

Immer wenn eine Überwachung im räumlichem Umfeld von Umkleide-, Dusch- und Toilettenräumen stattfinden soll, hat vor Einrichtung der Anlage eine Vorabkontrolle zu erfolgen. Dabei müssen die spezifischen Risiken, die der Einsatz der Überwachungstechnik für die Rechte und Freiheiten der

betroffenen Personen bereithält, vor Beginn mit seinem Nutzen abgewogen werden. Nur wenn die mit der Überwachung verbundenen Gefahren wirksam beherrscht werden, ist sie zulässig. Zuständig für die **Vorabkontrolle** ist die oder der betriebliche Datenschutzbeauftragte.

Dies bedeutet gleichzeitig, dass jede Stelle, die plant, mittels einer Kamera das Umfeld von Umkleide-, Dusch- oder Toilettenkabinen zu überwachen, zwingend eine betriebliche Datenschutzbeauftragte oder einen betrieblichen Datenschutzbeauftragten bestellen muss. Dies gilt unabhängig von der Zahl der bei ihr tätigen Mitarbeiterinnen und Mitarbeiter und unabhängig davon, ob sich das Vorhaben später als zulässig erweist, sowohl für die Durchführung der Vorabkontrolle, als auch während des späteren Einsatzes der Kamera.

5 Handel und Wirtschaft

5.1 Radio Frequency Identification im Handel

Die Technologie der Radio Frequency Identification (RFID) im Handel einzusetzen, bietet vielfältige Anwendungsmöglichkeiten von der Diebstahlsicherung bis zur Identifizierung von Ware. Werden RFID-Chips direkt im Endkundenbereich auf einzelnen Produkten oder auf Kundenkarten verwendet, können verschiedenste Informationen erfasst und miteinander in Verbindung gebracht werden. So ist etwa die Vorstellung vom „Supermarkt der Zukunft" zwar zum Greifen nah, doch wie groß ist die Gefahr einer Durchleuchtung und Bespitzelung der Kundinnen und Kunden?

Gegenüber den heute im Handel üblichen Barcodes können mit **RFID-Chips** deutlich mehr Informationen über Produkte gespeichert und zusätzlich vollautomatisch und ohne Sichtkontakt ausgelesen werden (technische Funktionsweise siehe unter 2.1).

Hinsichtlich der Anwendung von RFID im Handel fand in Nordrhein-Westfalen im Berichtszeitraum eine Überprüfung des „Extra Future Store" der Metro AG in Rheinberg statt. Es handelt sich dabei um einen gewöhnlichen Supermarkt, der im Endkundenbereich vereinzelt RFID-Technologie einsetzt. Der Rundgang in diesem Supermarkt zeigte, dass an vier Produkttypen ausgewählter Hersteller zusätzlich zum Barcode RFID-Chips angebracht waren. Bei diesen Produkten handelte es sich im Einzelnen um Frischkäse, Rasierklingen und Haarpflegeprodukte sowie um CDs, DVDs und Videos. Der Extra Future Store setzt die RFID-Etiketten zu Logistikzwecken und teilweise zur Diebstahlsicherung ein. Darüber hinaus dienen die Funketiketten auch der Einrichtung „intelligenter Regale" im Verkaufsbereich. Diese sorgen durch einen Funkkontakt zur Lagerverwaltung dafür, dass es zu keinem Zeitpunkt an bestimmten Artikeln fehlt. Dadurch soll zugleich vermieden werden, dass die Kundinnen und Kunden vor leeren Regalen stehen.

Die verwendeten Funketiketten enthalten keine personenbezogenen Daten und werden auch zu keinem Zeitpunkt mit solchen verknüpft. Allerdings sind im Rahmen der Einführung dieses technischen Konzeptes zunächst 10.000 speziell für den Extra Future Store hergestellte Payback-Karten, die ebenfalls mit einem RFID-Chip versehen waren, an die Kundinnen und Kunden ausgegeben worden. Insoweit setzte der Extra Future Store eine

RFID-Technologie mit Personenbezug ein, wobei diese RFID-Chips insbesondere dem Zweck dienten, die Kontrolle der Altersbeschränkung für das Abspielen von Filmausschnitten der DVDs sicherzustellen, die in diesem Supermarkt zum Kauf angeboten werden. Als erfreuliche Reaktion auf den Protest von Datenschutz-Aktivistinnen und -Aktivisten sind diese speziellen Kundenkarten inzwischen jedoch gegen herkömmliche Payback-Karten ohne RFID-Chip umgetauscht worden.

Die Nummer jedes verwendeten RFID-Chips wird vom Extra Future Store grundsätzlich für die Dauer von **15 Monaten gespeichert.** Diese auf den RFID-Etiketten enthaltene Nummer ist in vier Kategorien unterteilt: zuerst ein Freifeld, das ausschließlich der Diebstahlsicherung dient, darauf folgt eine produktspezifische Nummer, die mit dem Barcode identisch ist, darauf wiederum folgt eine Seriennummer, die als individuelle Nummer des einzelnen Produktes dient. Den Abschluss bildet die RFID-Hersteller-Nummer.

Die Kundinnen und Kunden haben die Möglichkeit, die RFID-Chips auf den gekauften Einzelprodukten nach dem Bezahlvorgang vor Verlassen des Supermarktes selbst aktiv zu **löschen**. Allein die Seriennummer des RFID-Chips, die bei der Produktion eingebracht wird, kann aus technischen Gründen noch nicht gelöscht werden. Dies wird erst in der nächsten Chipgeneration möglich sein.

Die Verwendung von RFID-Chips im Handel ist datenschutzrechtlich dann relevant, wenn eine Verknüpfung mit personenbezogenen Daten hergestellt wird. Für die betroffenen Kundinnen und Kunden ist es daher wichtig auszuschließen, dass aus den zum Zeitpunkt des Kaufs anonymen RFID-Daten nachträglich personenbezogene werden. In diesem Zusammenhang tritt die Befürchtung auf, dass später die Daten eines RFID-Chips – beispielsweise in einem Kleidungsstück – von einem Lesegerät erfasst und mit personenbezogenen Informationen der die Kleidung tragenden Person verknüpft werden. Da im vorliegenden Fall die Daten der RFID-Chips zum Zeitpunkt des Kaufs anonym sind und auch nach dem Kauf kein Personenbezug hergestellt wird, hat die hier erfolgte Überprüfung der eingesetzten RFID-Technologie im Ergebnis keinen Anlass zu datenschutzrechtlicher Beanstandung gegeben.

Es darf nicht zu einer heimlichen Kundenüberwachung und einem unbemerkten Ausspionieren von Verbrauchergewohnheiten im Alltag kommen. Um den Betroffenen die nötige Transparenz zu bieten, sollte auf

den Einsatz von RFID-Technologie hingewiesen werden. Jeder Kundin und jedem Kunden ist dabei zu empfehlen, verwendete RFID-Chips beim Verlassen eines Geschäftes selbst aktiv zu löschen, um weiterhin die Möglichkeit eines anonymen Einkaufs wahrnehmen zu können.

5.2 Dubiose Datenverarbeitung im Call-Center

Call-Center beschaffen sich häufig Adressdaten, um Bürgerinnen und Bürger im Wege der Telefonwerbung für neue Produkte zu gewinnen. Dabei sorgen der beträchtliche Umfang und Inhalt der Datenbestände und ihre häufig ungeklärte Herkunft immer wieder für Irritationen - nicht nur bei den betroffenen Werbeadressaten, sondern auch bei den Beschäftigten des Call-Centers.

Aufgrund eines Hinweises erfolgte im Berichtszeitraum die Überprüfung eines Call-Centers in Nordrhein-Westfalen. Dort bestand der Verdacht, dass das Unternehmen in großem Umfang Adresslisten zur Kundenaquise einsetzte, die nicht nur **Name** und **Adresse,** sondern auch Angaben zu **Bankverbindungen** und **Spendenbeträgen** der Betroffenen enthielten. Dieser Verdacht bestätigte sich umgehend im Rahmen des Kontrollbesuchs:

Das Call-Center betrieb mit den Daten telefonische Neukundenwerbung und bot als Produkt eine Art „**Kartenschutzversicherung**" an. Das bedeutete, dass das Call-Center im Falle des Verlustes von EC-, Kredit- oder anderweitigen Karten für die Kundinnen und Kunden die Sperrung der Karten nebst Neuanmeldung und Beschaffung von Ersatzkarten vornehmen würde. Bei dem Kontrollbesuch konnte zudem beobachtet werden, dass sich die Beschäftigten des Call-Centers im Rahmen des Werbeanrufs als „Bundesverband für Kartenschutz" auszugeben hatten, der jedoch tatsächlich nicht existierte. Dadurch sollte gegenüber den Betroffenen der Anschein erweckt werden, die angebotene Dienstleistung stamme von eben dieser Einrichtung und nicht von einem Wirtschaftsunternehmen. Im Rahmen des Werbeanrufs wurden Name, Adresse und Bankverbindung des Betroffenen verifiziert.

Zum Zwecke der Werbe- und Verkaufsaktion hatte das Call-Center zuvor in erheblichem Umfang Bestandslisten der Mitgliedsverwaltung eines größeren deutschen Vereins auf nicht mehr zurückverfolgbaren Wegen erworben. Diese **Mitgliederlisten** enthielten neben Namen und Adressen der Betroffenen personenbezogene Angaben zu Telefonnummern, Bankverbindungen und Spendenbeträgen. Ferner stellte sich bei der Überprüfung heraus, dass das Unternehmen darüber hinaus über eine Adressdatei mit

umfassenden **Aktionärsdaten** verfügte. Diese enthielt neben Namen und Adressen der Betroffenen personenbezogene Angaben zu Bankverbindungen, Aktienbestand und Bewegungen im Aktiendepot.

Diese Adresslisten umfassten einen **Datenumfang**, der inhaltlich weit über die Daten hinausgeht, die nach dem BDSG zulässigerweise listenmäßig an Dritte zu Werbezwecken übermittelt werden dürfen. Andere Daten als die in § 28 Abs. 3 Nr. 3 BDSG genannten Daten, wie zum Beispiel Telefonnummern und Bankdaten, dürfen nur mit Einwilligung der Betroffenen an Dritte übermittelt und für Werbezwecke genutzt werden. Darüber hinaus bedarf es für eine Datennutzung gerade zum Zwecke der Telefonwerbung grundsätzlich einer gesonderten Einwilligung der Betroffenen. Nach eigenen Angaben war dem Call-Center zum Zeitpunkt des Erwerbs der Adressdaten sogar durchaus bewusst, dass es an der Einwilligung der Betroffenen zur Verarbeitung der Daten zu Werbezwecken sowie zur Nutzung für Telefonwerbung fehlte.

Im Rahmen des Kontrollbesuchs wurde das Call-Center daher aufgefordert, die Adresslisten nicht weiter zu verwenden und umgehend zu vernichten, was im Wege einer erneuten unangemeldeten Kontrolle eine Woche später überprüft wurde.

Das Call-Center hat trotz der fehlenden Einwilligung der Betroffenen vorsätzlich deren Adressdaten im Rahmen der Werbeanrufe zur Datenerhebung genutzt und zudem durch unrichtige Angaben personenbezogene Daten erschlichen. Da das Unternehmen mit den unzulässig erlangten Daten Vertragsabschlüsse fördern und daraus einen wirtschaftlichen Vorteil ziehen wollte, handelte es sogar mit Bereicherungsabsicht. Dadurch hat das Unternehmen zugleich den Straftatbestand gemäß § 44 Abs. 1 BDSG verwirklicht.

Das Unternehmen wurde umgehend aufgefordert, jede weitere Nutzung der Daten zu unterlassen und die Adresslisten zu vernichten. Zudem wurde gegen das Unternehmen bei der Staatsanwaltschaft ein Strafantrag gestellt.

5.3 Weitergabe von Abonnentendaten durch insolvente Zeitungsverlage

Sicherlich waren die Leserinnen und Leser einer Wochenzeitung überrascht, als sie statt des von ihnen abonnierten Blattes plötzlich eine von einem anderen Verlag herausgegebene Wochenzeitung ganz anderen

politischen Zuschnitts in ihrem Briefkasten fanden. Mehr noch als der aufgezwungene Wechsel des Produktes machte einigen Betroffenen die Frage danach zu schaffen, wie die neuen Verlage in den Besitz ihrer Abonnentendaten kamen. Auch Konto- und Abrechnungsdaten wurden weitergegeben.

Mit Zunahme der Insolvenzen im Zeitungswesen greift offenbar die Praxis um sich, zusammen mit den letzen Vermögenswerten des insolventen Unternehmens auch den Geldwert der **Abonnentendaten** zu realisieren. Die Verlage erklären ihr Vorgehen jeweils damit, die bestehenden Abonnementverträge auch nach dem Stopp der Zeitung weiter ausführen zu wollen, da andernfalls das im Voraus entrichtete Entgelt an die Leserinnen und Leser hätte zurückgewährt werden müssen. Gleichwohl entbindet die Insolvenz die Unternehmen nicht von der Einhaltung der datenschutzrechtlichen Bestimmungen. Für die Weitergabe der Abonnentendaten an die neuen Verlage hätten die alten Verlage die vorherige **Einwilligung** der betroffenen Leserinnen und Leser benötigt.

Etwas anderes hätte allenfalls dann gegolten, wenn die neuen Verlage als so genannte Auftragsdatenverarbeiter eingeschaltet worden wären und sie die personenbezogenen Daten der Abonnentinnen und Abonnenten daher lediglich im Auftrag der alten Verlage verarbeitet hätten. Eine **Auftragsdatenverarbeitung** liegt immer dann vor, wenn der Auftragnehmerin oder dem Auftragnehmer die Entscheidungsbefugnis über die Daten fehlt, die Auftraggeberin oder der Auftraggeber gleichsam „Herr der Daten" bleibt und daher nach außen die Verantwortung für die Datenverarbeitung trägt. In den beurteilten Fällen blieben die alten Verlage jedoch nicht mehr in diesem Sinne „Herren der Daten". Sie hatten sich vertraglich keine Kontroll- und Weisungsrechte einräumen lassen und sämtliche Einflussmöglichkeiten aus der Hand gegeben. Die neuen Verlage führten fortan ihre Tätigkeiten selbständig durch, wie zum Beispiel den Forderungseinzug.

In der Weitergabe der Kundendaten an die neuen Verlage lag daher eine Übermittlung personenbezogener Daten an Dritte außerhalb des Verantwortungsbereichs der alten Verlage, welche einer eigenständigen Rechtsgrundlage bedurfte. Eine gesetzliche Grundlage, die die Übermittlung an den neuen Verlag rechtfertigen konnte, lag nicht vor. Zwar beriefen sich die Verlage zunächst auf die Vorschrift des § 28 Abs. 1 Nr. 1 BDSG. Nach dieser Bestimmung wäre das Übermitteln personenbezogener Daten an die neuen Verlage zulässig gewesen, wenn es der **Zweckbestimmung** der Abonnementverträge mit den betroffenen Leserinnen und Lesern gedient

hätte. Jedoch handelte es sich bei den neuen Zeitungen um einen ganz anderen als den ursprünglichen Vertragsinhalt. Außerdem war in den Abonnementverträgen auch nicht vereinbart worden, dass die alten Verlage das Recht haben sollten, ihre Leistung einseitig durch die eines anderen Verlages zu ersetzen. In der kommentarlosen Zusendung der neuen Zeitschrift lag vielmehr ein Angebot auf Abschluss eines Änderungsvertrages, der als neuer Vertrag den alten hätte ersetzen sollen. Es konnte daher nicht mehr davon gesprochen werden, dass die Zusendung der neuen Zeitungen der Zweckbestimmung der alten Verträge diente.

Auch auf die Regelung des § 28 Abs. 1 Nr. 2 BDSG konnten sich die Verlage nicht berufen, da die **schutzwürdigen Interessen** der betroffenen Leserinnen und Leser einer Übermittlung ihrer Daten an die neuen Verlage entgegen standen. Zwar waren bei der nach dieser Vorschrift vorzunehmenden Interessenabwägung durchaus das wirtschaftliche Interesse der alten Verlage an der Vermeidung von etwaigen Rückforderungsansprüchen sowie das Werbe- und Akquiseinteresse der neuen Verlage zu berücksichtigen. Jedoch standen diesen Anliegen im Ergebnis überwiegende Interessen der Leserinnen und Lesern entgegen, die bei dem Versuch der Überleitung ihrer Abonnements in keiner Weise beteiligt worden waren. Weder wurde ihnen im Vorfeld ein Hinweis auf die geplante Überleitung gegeben, noch wurde ihnen die Möglichkeit eines Widerspruchs eingeräumt. Das eigenmächtige Vorgehen der alten Verlage nahm ihnen vielmehr die Freiheit, selbst darüber zu entscheiden, welchem Verlag sie ihre Vertragsdaten zur Verfügung stellen wollten.

Für die Übermittlung der Daten an die neuen Verlage sowie ihre Nutzung dort war daher mangels einer gesetzlichen Grundlage die **Einwilligung** der betroffenen Leserinnen und Leser vor der Übermittlung erforderlich. Da eine solche fehlte, waren die Übermittlung und anschließende Nutzung der Abonnementdaten unzulässig und die Daten bei den neuen Verlagen zu löschen. Dies galt jedoch nicht für die Daten der Kundinnen und Kunden, die dem Bezug der neuen Zeitung zugestimmt hatten, da der neue Verlag diese Daten als Vertragsdaten für die Durchführung der neuen Abonnementverträge benötigte.

Auch in Fällen der Insolvenz sind die datenschutzrechtlichen Bestimmungen bei der Weitergabe von Abonnementdaten zu beachten und die Rechte der Betroffenen zu wahren. Die Übermittlung von personenbezogenen Daten der Leserinnen und Leser bedarf grundsätzlich ihrer vorherigen Einwilligung, wenn beabsichtigt ist, dass der neue Verlag die Kundinnen

und Kunden in Eigenregie mit anderen als den vertraglich vereinbarten Zeitungen beliefert.

5.4 Adressen machen Leute? - Statistische Daten zu Kaufkraft und Zahlungsmoral

Das Interesse an Informationen zu Finanzstatus und Bonität privater Haushalte wächst stetig. So möchten sich Unternehmen vor zahlungsunfähigen oder -unwilligen Kundinnen und Kunden schützen und zugleich erfahren, in welchen Wohngebieten sich eine gezielte Werbung überhaupt lohnt. Auch Privatpersonen haben Interesse daran, etwa vor dem Kauf einer Immobilie Informationen über die Wohngegend einzuholen. Zu diesem Zweck können interessierte Personen auf einer CD statistische Adressbewertungen abrufen, die jedoch an datenschutzrechtliche Grenzen stoßen.

Dieses gestiegene Informationsbedürfnis diente auch einem Unternehmen in Nordrhein-Westfalen im Berichtszeitraum als Anlass zu einer Geschäftsidee: die Firma entwickelte eine CD, die Auskunft über statistische Kaufkraftdaten und Risikoklassen privater Haushalte in Deutschland gab. Diese Software bietet der Nutzerin oder dem Nutzer die Möglichkeit, Kaufkraft und Risikostruktur eines ausgewählten **Straßenabschnittes** zu bestimmen. An dieser Geschäftsidee war neu, die CD in einer Massenauflage in den Handel zu bringen, um sie an beliebig viele Personen verkaufen zu können. Diese CD sorgte für große Aufregung in den Medien und führte zu zahlreichen Beschwerden von Bürgerinnen und Bürgern.

Das Unternehmen hat in seiner Werbung das Programm als „**Kaufkraft- und Risikoauskunft**“ und als „statistische Daten zu privaten Haushalten“ bezeichnet. Allerdings vermittelten verschiedene Vertriebspartner des Unternehmens in ihren Werbeschreiben, dass es sich um einzigartige Informationen von besonderem Wert handele und warben zugleich mit dem Anreiz zu „Neugierauskünften“. So hieß es beispielsweise in den Werbeschreiben: „Wüssten Sie nicht auch gerne, wie es in der Nachbarschaft mit dem Geld aussieht? Oder im Wohngebiet von Kollegen und Bekannten? Sie werden überrascht sein!“.

Um die Software entwickeln zu können, bediente sich das Unternehmen Zulieferer, die entsprechende Basisdaten aufbereiteten und mit den zugehörigen Straßenabschnitten verknüpften. Der Bewertung der Kaufkraft liegen Datenbestände aus dem **Versandhandel** zugrunde. Zur Bewertung der

Zahlungsmoral hingegen verwendete das Unternehmen Bonitätsdaten einer **Auskunftei**, die auf Straßenabschnittsebene zusammengefasst wurden und Durchschnittswerte darstellen. Da diese Datenlieferanten ihren Sitz nicht in Nordrhein-Westfalen haben, musste sich die Prüfung durch die LDI auf die Bewertung der CD selbst beschränken. Die Datenverarbeitungsvorgänge, die zur Erstellung der CD führten, werden von der zuständigen Aufsichtsbehörde in Süddeutschland geprüft.

Das Programm zeigt bei einer Adressanfrage für den betreffenden Straßenabschnitt in Form einer optischen Anzeige unter Verwendung der **Schulnoten 1 – 5** sowohl die Kaufkraft als auch das Zahlungsrisiko an. Im Rahmen der Kaufkraftbewertung erhält die Nutzerin oder der Nutzer zudem eine graphische Darstellung in Form einer Tabelle, wie viele Häuser in dem Straßenabschnitt berücksichtigt wurden und bei wie vielen Häusern welche Kaufkraft vorhanden ist. In gleicher Weise ermittelt das Programm das Zahlungsrisiko hinsichtlich des betreffenden Straßenabschnittes. Ein sehr geringes Zahlungsrisiko wird mit der Schulnote 1, ein sehr hohes Zahlungsrisiko mit der Schulnote 5 bewertet. Bei der Bewertung des Zahlungsrisikos erfolgt jedoch keine zusätzliche Aufschlüsselung auf einzelne Häuser wie bei der Kaufkraftbewertung.

Bei der Prüfung des Produkts hat sich herausgestellt, dass bei der Kaufkraftbewertung einzelner Straßen das Ergebnis derart ausfallen kann, dass ein Rückschluss auf **einzelne Haushalte und Personen** in einigen Konstellationen möglich ist. Personenbeziehbare Daten liegen vor, wenn der Bezug zu einer konkreten natürlichen Person mit den üblicherweise zur Verfügung stehenden Mitteln hergestellt werden kann. Dies ist für zahlreiche Einfamilienhäuser der auf der CD bewerteten Straßenabschnitte der Fall. Entscheidend ist dabei nicht die Zahl der Häuser, sondern dass das Programm für bestimmte Fälle die zusätzliche Information enthält, dass alle Häuser bewertet wurden und diese in der Bewertung die gleiche oder eine ähnliche Note erhalten haben. Dies führt dazu, dass nicht nur über einen Straßenabschnitt, sondern auch über ein konkretes Haus eine Aussage getroffen wird, beispielsweise Kaufkraftbewertung mit der Note „gut". Die Personenbeziehbarkeit ist jedenfalls immer dann gegeben, wenn es sich um ein Einfamilienhaus handelt, da die Information zur Kaufkraftbewertung dann auf einen einzelnen Haushalt und sogar auf Einzelpersonen heruntergebrochen werden kann.

Insbesondere bei „**Neugierauskünften**" über persönlich bekannte Personen wie Nachbarn und Freundinnen oder Freunde ist eine Personenbeziehbarkeit

möglich. Gerade diese Verwendungsmöglichkeit wurde in der Werbung für das Programm besonders hervorgehoben. In diesen Fällen bedarf es nicht einmal der Nachforschung mittels eines Adressbuchs, da die Programmnutzenden die Software zur Bewertung konkreter Adressen verwenden, zu denen sie den persönlichen Bezug unmittelbar selbst herstellen können.

Da anhand der getroffenen Feststellungen eine Personenbeziehbarkeit der ermittelten Daten gegeben ist und es keine rechtliche Grundlage gibt, nach der eine Kaufkraftbewertung bei möglicher Personenbeziehbarkeit zulässig wäre, ist ein **Ordnungswidrigkeitsverfahren** gegen das Unternehmen wegen unbefugter Übermittlung personenbezogener Daten eingeleitet worden. Zugleich wurde das Unternehmen aufgefordert, dafür Sorge zu tragen, dass die CD mit dem Programm aufgrund der damit verbundenen unbefugten Übermittlung personenbezogener Daten nicht weiter in Umlauf gebracht wird. Daraufhin hat sich das Unternehmen bereit erklärt, die CD aus dem Vertrieb zurückzunehmen.

Statistische Adressbewertungen zu Kaufkraft und Zahlungsrisiko sind unzulässig, sobald die ermittelten Daten personenbeziehbar sind und die betroffenen Personen keine Einwilligung erteilt haben.

5.5 Auskunfteien: Bonitätsauskünfte an Versicherungen

Auskunfteien wie beispielsweise die SCHUFA haben ein großes Interesse daran, ihr Geschäftsfeld zu erweitern, um die vorhandenen Daten zu Zigmillionen Bürgerinnen und Bürgern auch anderen Unternehmensbranchen anbieten zu können. Ein lukrativer Kundenkreis sind Versicherungen, die gerne vor Abschluss bestimmter Verträge eine Auskunft über die Bonität ihrer potentiellen Versicherungsnehmerinnen und Versicherungsnehmer erhalten würden. Die Frage, ob die Versicherungen Bonitätsauskünfte überhaupt einholen dürfen, hat die Aufsichtsbehörden im Berichtszeitraum wiederholt beschäftigt.

Nach § 29 Abs. 2 BDSG müssen die Versicherungen im konkreten Einzelfall ein **berechtigtes Interesse** an der Kenntnis der Bonitätsdaten haben und es darf kein Grund zu der Annahme bestehen, dass die potentielle Versicherungsnehmerin oder der potentielle Versicherungsnehmer ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung ihrer oder seiner Daten durch die Auskunftei an die Versicherung hat.

Ein erhebliches finanzielles **Ausfallrisiko** hinsichtlich eines konkret bevorstehenden Versicherungsabschlusses wäre ein berechtigtes Interesse des Versicherungsunternehmens für die Einholung einer Bonitätsauskunft. Jedoch birgt das bei jedem Versicherungsabschluss nicht auszuschließende Risiko, dass die Versicherungsnehmerin oder der Versicherungsnehmer die erste oder einmalige Versicherungsprämie nicht rechtzeitig zahlt, für die Versicherung grundsätzlich kein Ausfallrisiko. Denn die Versicherung ist in diesem Fall berechtigt vom Vertrag zurückzutreten, beziehungsweise sie wird, wenn die Prämie zur Zeit des Eintritts des Versicherungsfalles noch nicht gezahlt ist, von der Verpflichtung zur Leistung frei.

Daher dürfen Versicherungen nur ausnahmsweise Bonitätsauskünfte einholen und zwar bei

- **Kreditversicherungen;**
- **Kfz-Versicherungen** bei einer vorläufigen Deckungszusage (Doppelkarte), jedoch erst ab dem Zeitpunkt des unterzeichneten Versicherungsantrags. Unzulässig ist die Bonitätsabfrage, wenn die Versicherung die Doppelkarte erst nach Zahlung der ersten Versicherungsprämie überreicht oder wenn nur eine unverbindliche Anfrage und kein Versicherungsantrag vorliegt;
- **Hypothekendarlehen** im Rahmen der Kreditvergabe durch Versicherungen;
- **Vermietungen** von Immobilien durch Versicherungen und bei
- konkretem **Betrugsverdacht** im jeweiligen Einzelfall.

Die **Versicherungswirtschaft** selbst hat gegenüber den Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich keine weiteren Fallgruppen genannt, in denen Versicherungen vor Abschluss eines Versicherungsvertrags Bonitätsauskünfte einholen möchten. Dagegen haben die an einer Ausweitung ihres Geschäftsbereiches interessierten **Auskunfteien** vorgetragen, die Versicherungen hätten über die aufgeführten Fälle hinaus auch in einigen anderen Sparten ein berechtigtes Interesse, bei ihnen eine Bonitätsauskunft über potentielle Versicherungsnehmerinnen und Versicherungsnehmer einzuholen. Als Beispiel wurden die **Lebensversicherungen** angeführt. Dort bestehe wegen der **Provisionszahlungen** an die Versicherungsmaklerin oder den Versicherungsmakler ein Ausfallrisiko, weil im Falle der Rückabwicklung eines Vertrages ein vermehrter Verwaltungsaufwand und hohe Stornierungskosten entstünden. Dieses Problem betrifft

jedoch allein die vertragliche Beziehung zwischen der Versicherung und der Maklerin oder dem Makler und kann nicht zu Lasten Dritter gelöst werden, nämlich der Personen, die eine Versicherung abschließen wollen. Mangels eines berechtigten Interesses der Versicherung an der Kenntnis der Bonitätsdaten über diese Personen, ist die Einholung einer Bonitätsauskunft in derartigen Fällen unzulässig.

Regelmäßig gehen die Versicherungen bei Abschluss eines Versicherungsvertrags kein finanzielles Ausfallrisiko ein, das zu einer Bonitätsabfrage bei Auskunfteien berechtigt. Nur in Ausnahmefällen dürfen sie Informationen über die potentiellen Versicherungsnehmerinnen und Versicherungsnehmer einholen.

5.6 Heiße Luft statt harter Fakten: Schätzdaten in Bonitätsauskünften

Wirtschaftsauskunfteien wie die Creditreform bedienen sich zur Auskunft über Unternehmenszahlen häufig branchenüblicher Durchschnittswerte – also Schätzdaten. Dies geschieht, weil den Auskunfteien die tatsächlichen Daten nicht vorliegen. Die Aufsichtsbehörden verlangen in den Fällen, in denen die Daten dem Schutz des BDSG unterliegen, also personenbezogene Daten enthalten, eine deutliche Kennzeichnung dieser Daten als Schätzdaten. Doch wie sieht es mit der Verwendung von Schätzdaten in Auskünften über Privatpersonen aus?

„Ein PKW steht zur Verfügung", „Die Wohnräumlichkeiten an obiger Anschrift werden für über EUR 550,-- zur Miete unterhalten", „Im Wohnungsmobiliar sind entsprechende Mittel angelegt", „geschieden" – Schätzdaten, wie die betreffende Auskunftei auf Nachfrage mitteilte. Die **Angaben über Privatpersonen** hatte die Auskunftei an Vertragspartner übermittelt ohne die „Informationen" als Schätzdaten zu kennzeichnen. Darüber hinaus fanden sich auch Angaben zum Vorhandensein von Haus- und Grundeigentum sowie zur Ausbildung und der derzeitigen Berufstätigkeit – nach Angabe der Auskunftei ebenfalls geschätzte Daten.

Grundsätzlich lässt sich sagen, dass nur die Speicherung objektiver, richtiger bonitätsrelevanter Merkmale unter den gesetzlichen Voraussetzungen des § 29 BDSG durch Wirtschaftsauskunfteien zulässig ist. Unabhängig von der Frage, ob es sich bei all den genannten Daten auch tatsächlich um bonitätsrelevante Daten handelt, ist die Zulässigkeit einer Speicherung in jedem Fall daran geknüpft, dass es sich um objektiv richtige Daten handelt. Die Ver-

wendung von Schätzdaten wäre in jedem Fall deutlich als solche zu kennzeichnen. Daten in Privatauskünften eignen sich zudem kaum für eine Schätzung, etwa des Familienstandes. Im Ergebnis wurden sämtliche Schätzdaten in den vorliegenden Auskunftsdatensätzen gelöscht.

Die Fälle haben Veranlassung gegeben zu überprüfen, ob es sich hierbei um Einzelfälle gehandelt hat oder ob Schätzdaten regelmäßig in Privatauskünften Verwendung finden. Der Verband der betreffenden Auskunftei teilte hierzu mit, bei den ihm bekannten Fällen habe es sich um Ausnahmefälle gehandelt. Die angeschlossenen Auskunfteien würden in Privatpersonenauskünften in der Regel gar nicht mit Schätzungen arbeiten.

Betroffene können gegenüber der Auskunftei von ihrem Auskunftsrecht nach § 34 BDSG Gebrauch machen. Danach kann die betroffene Person grundsätzlich Auskunft über die zu ihrer Person gespeicherten Daten verlangen, auch soweit es um die Herkunft dieser Daten geht.

5.7 Living by numbers – Bonitätsbewertungen durch Scoring

Zunehmend setzen Unternehmen, die im Massengeschäft die Bonität von möglichen Kundinnen und Kunden prüfen, statistische Persönlichkeitsprofile und -bewertungen in Form so genannter Scoring-Verfahren ein: beispielsweise bei Abschluss eines Mobilfunkvertrags, bei Bestellungen im Versandhandel, im Internet oder bei der Vergabe von Krediten. Ziel ist eine schnelle, kostengünstige und auf rationalen Kriterien beruhende Entscheidungsfindung. Mit möglichst geringem personellen Aufwand soll zügig und nicht nach Intuition oder Laune über den Vertragsabschluss und seine Ausgestaltung entschieden werden.

Beim Scoring werden die zu bewertenden Personen statistisch gebildeten Risikoklassen zugeordnet. Dafür werden ihre Daten mit den Daten statistischer Vergleichsgruppen bisheriger Kundinnen und Kunden verglichen und dann einer Risikoklasse mit ähnlichen oder gleichen Merkmalen zugeordnet. Das **statistische Ausfallrisiko** der gefundenen Vergleichsgruppe wird damit auch der konkreten Person zugeschrieben. Das Ergebnis drückt sich in einem so genannten Score-Wert aus, der die statistische Bonitätsbewertung der konkreten Person in einen Zahlenwert zusammenfasst, beispielsweise in Form einer Schulnote oder einer %-Zahl. Der **Score-Wert** ist damit ein personenbezogenes Datum, dessen Erhebung,

Verarbeitung und Nutzung nach datenschutzrechtlichen Vorschriften zu beurteilen ist.

Die Qualität derartiger Bewertungs- und Prognoseverfahren hängt wesentlich von der Qualität der in das Scoring-Verfahren einfließenden Daten ab. Je seriöser ein Scoring-Verfahren ist, desto mehr wird auf Merkmale abgestellt, die eine **unmittelbare Aussagekraft** über das Zahlungsverhalten oder die persönlichen Einkommens- und Vermögensverhältnisse haben. Ausschlaggebend für die Bewertung sind dann vor allem das individuelle Verhalten in der Vergangenheit und die aktuelle persönliche Leistungsfähigkeit.

Unseriöse Scoring-Verfahren dagegen verwenden leicht zugängliche, aber für sich genommen wenig bonitätsrelevante Kriterien wie beispielsweise das Geschlecht, das Alter, das Wohnumfeld, die Zahl der Umzüge in den letzten Jahren – ermittelbar über die Zahl der Voranschriften – oder die Anzahl der Kreditanträge ohne anschließenden Vertragsschluss. Viele dieser Kriterien sind individuell kaum steuerbar und allen liegt eine Verallgemeinerung eines statistischen Zusammenhangs zugrunde, der für die bewertete Person nicht bestehen muss und einer **„statistischen Sippenhaft"** gleicht.

So bietet auch die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) ein Scoring-Verfahren an, mit dem eine Prognose über das zukünftige Zahlungsverhalten einer Person getroffen wird. Welche Auswirkungen dies haben kann, zeigt folgendes Beispiel: Ein Mann unter 30 Jahren, der in den vergangenen Jahren häufig umgezogen ist und sich in den letzten Wochen online bei mehreren Kreditinstituten nach den jeweiligen Kreditkonditionen erkundigt hat, ohne dass es anschließend zu einem Vertragsschluss kam, würde wahrscheinlich einen sehr schlechten **SCHUFA-Score** erhalten – selbst wenn er sich bislang stets vertragstreu verhalten hat und eine sichere Beschäftigung mit hohem Einkommen hat. Der Mann würde aufgrund eines statistischen Zusammenhangs benachteiligt, wonach Männer unter 30 Jahren, die häufig umziehen und viele Kreditanfragen stellen, sich in der Vergangenheit häufig als Personen mit hohem Ausfallrisiko herausstellten. Bei dieser Verallgemeinerung bliebe unberücksichtigt, dass nicht alle jungen Männer leichtsinnig mit Geld umgehen; dass Personen, die häufig umziehen, nicht zwangsläufig vor ihren Schulden flüchten oder auf dem sozialen Abstieg sind – vielleicht macht die Person Karriere und die dadurch bedingten Wohnsitzwechsel sind ein Zeichen zunehmenden Einkommens. Auch die zahlreichen Kreditanfragen ohne späteren Vertragsschluss deuten nicht zwingend darauf hin, dass die Banken keinen Kredit bewilligt hätten. Genauso gut kann sich die Person

einen Marktüberblick verschafft haben, aber von den Angeboten nicht überzeugt gewesen sein. Diese Ausnahmen von der statistischen Regel bleiben beim SCHUFA-Score unberücksichtigt. Unbescholtene Kreditsuchende laufen Gefahr, Opfer eines statistischen Vorurteils zu werden; hervorgerufen durch ein Scoring-Verfahren, das auch auf Kriterien beruht, denen es an unmittelbarer Bonitätsrelevanz fehlt.

In andere Scoring-Verfahren fließen teilweise auch so genannte **mikro-geografische und sozio-demografische Daten** ein. Dabei wird beispielsweise das **Wohnumfeld** einer Person klassifiziert: Lebt sie in einem Stadtteil, der angeblich vorwiegend durch Personen mit „niedrigem sozialen Status" geprägt ist, wirkt sich dies negativ auf ihren Score-Wert aus – unabhängig von den tatsächlichen Eigentums- und Vermögensverhältnissen. Das kann zu fehlerhaften Bonitätsbewertungen führen, weil sich vielleicht zwischenzeitlich die soziale Zusammensetzung des Viertels verändert hat, oder eine wohlhabende Person lieber in einem lebendigen, sozial gemischten Innenstadtkern lebt als in einer ruhigen, besser bewerteten Reihenhaussiedlung. Wenn nun diese Person künftig wegen ihres Wohnumfelds höhere Zinsen zahlen muss, wird sie sich allerdings überlegen, ob sie nicht doch in ein besser bewertetes Viertel umzieht. Die Verwendung mikro-geografischer und sozio-demografischer Daten für die Bonitätsprüfung birgt auch das Risiko, dass ganze Bevölkerungsgruppen und Stadtteile sozial ausgegrenzt werden und eine **Ghettoisierung** eintritt.

Datenschutzrechtlich lassen sich Art und Umfang der berücksichtigten Merkmale einer Person im Scoring so bewerten: Grundsätzlich zulässig für die Berechnung eines Score-Wertes ist die Verwendung von relevanten, objektiv richtigen Daten zum **Zahlungsverhalten** sowie zu den **Einkommens- und Vermögensverhältnissen** der Person. Datenschutzrechtlich problematisch ist es dagegen, auf Basis von **Daten ohne eigene Bonitätsaussage** wie die Anzahl der Umzüge in den letzten Jahren einen Score-Wert zu berechnen. Auch das Alter der Betroffenen ist nur bedingt bonitätsrelevant, zum Beispiel für die Dauer der Einkommenserzielung. Stets unzulässig ist die Verwendung **sensitiver Daten** wie „rassische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftsangehörigkeit, Gesundheit, Sexualleben".

Besonders kritisch an vielen Scoring-Verfahren ist ihre mangelnde **Transparenz**. Für die Betroffenen ist das gesamte Verfahren der Score-Wertberechnung eine **„Black Box"**, in der teilweise sogar ohne ihr Wissen ihre Daten eingegeben und nach geheimgehaltenen Kriterien bewertet

werden. Wenn das Unternehmen den Score-Wert nicht selbst errechnet, sondern von einem Dienstleistungsunternehmen oder einer Auskunftei erhält, ist auch für das Unternehmen selbst häufig nicht erkennbar, welche Merkmale die konkrete Bewertung maßgeblich prägen. Es erfährt nur, dass die Person zur Risikoklasse „F" mit einem „Ausfallrisiko 34,73 %" gehört. Das verrät nichts über die eventuell zweifelhaften Kriterien oder eine veraltete Datenbasis, die der Berechnung zugrunde liegen können.

Die mangelnde Transparenz schränkt die Möglichkeit der Betroffenen ein, gegebenenfalls Mängel der dem Scoring zugrunde liegenden Daten festzustellen. Zugleich können sich die Betroffenen auch nicht als Ausnahme von der statistischen Regel beweisen. Das ist besonders dann verhängnisvoll, wenn der negative Score-Wert automatisiert ohne Beteiligung eines Menschen zur Ablehnung des Vertrags führt. Beeinträchtigende Entscheidungen wie die Ablehnung eines Vertragsschlusses dürfen nach dem BDSG nicht ausschließlich auf Basis von Scoring-Verfahren getroffen werden.

Scoring-Verfahren zur Bonitätsprüfung sollten neben dem gesetzlichen Verbot der automatisierten Einzelentscheidung die folgenden drei Eckpunkte beachten:

1. **Solide Datengrundlage**: Beschränkung auf branchenrelevante und zutreffende Informationen zu Zahlungsverhalten, Einkommens- und Vermögensverhältnissen.
2. **Diskriminierungsverbot**: Geschlecht, Herkunft, Wohnumfeld sowie sensitive Daten der Bewerteten dürfen nicht in den Score einfließen. Auch das Alter der Betroffenen ist nur bedingt bonitätsrelevant.
3. **Transparenz**: Die Beurteilten müssen nachvollziehen können, welche Daten zu ihrer Person in die Berechnung einfließen und welche Merkmale ihren aktuellen Score-Wert maßgeblich prägen.

Damit Scoring-Verfahren zur Bonitätsbewertung nicht zu Benachteiligungen führen, müssen die Verfahren in jedem Fall auf einer soliden Datengrundlage arbeiten und Transparenz gewährleisten.

5.8 Kreditfabriken

Jede zweite deutsche Bank plant, innerhalb der nächsten Zeit Teile ihres Geschäfts wie zum Beispiel den Zahlungsverkehr oder das Wertpapiergeschäft an externe Dienstleistungsbetriebe auszulagern.

Immer häufiger wird dabei auch die Auslagerung des Kreditbereichs an so genannte Kreditfabriken ins Auge gefasst.

Kreditfabriken sind externe Dienstleistungsunternehmen, die sich auf die Bearbeitung und Abwicklung von Kreditprozessen spezialisieren und zum Teil auch selbst über die Vergabe von Krediten entscheiden. Sie existieren bislang vor allem im Bereich der Privatkredite und Baudarlehen.

Ziele der Auslagerung in Kreditfabriken sind die **industrielle Abwicklung** der Kreditprozesse und die mit dem **Massengeschäft** verbundenen Kosteneinsparungen. Statt der bislang in der herkömmlichen Kreditsachbearbeitung jährlich bearbeiteten circa 250 Kreditanträge pro Sachbearbeitung sollen durch die industrielle Abwicklung 600 und mehr bearbeitete Anträge möglich werden. Dies wird erreicht über vollautomatische Abwicklungsabläufe und standardisierte Arbeitsprozesse, die zentral bei der Kreditfabrik geführt werden. Die Vorbereitung der Kreditentscheidung durch die Kreditfabrik läuft dann beispielsweise nach dem folgenden Muster ab: Die Banken, die die Kreditentscheidung über die Kreditfabrik abwickeln, schicken den Kreditantrag mit den dazugehörigen Unterlagen wie etwa Einkommensnachweisen und Grundbuchauszug per Post oder Internet an die Kreditfabrik. Dort wird eine digitale Kreditakte angelegt, automatisch die Bonitätsauskunft bei der SCHUFA eingeholt und anschließend eine Berechnung über die Ausfallwahrscheinlichkeit durchgeführt. Gegebenenfalls wird dafür auf einen extern durch die SCHUFA errechneten Wert zurückgegriffen. Der errechnete Entscheidungsvorschlag wird schließlich von der Sachbearbeitung auf seine Plausibilität geprüft, bevor er zusammen mit der digitalen Kreditakte an die Bank zurückgeschickt wird.

Die von den Kreditfabriken angebotenen Dienstleistungen können neben der Kreditprüfung und -vergabe auch die Sanierung und Abwicklung „notleidender" Kreditengagements umfassen. In diesem Fall übernimmt die Kreditfabrik auch die Übernahme des **Mahn- und Inkassogeschäfts**. Unter den Kreditfabriken vertreten sind ebenso Modelle des reinen Back-Office-Betriebes innerhalb einer Tochtergesellschaft der auslagernden Bank wie unternehmensübergreifende Angebote einer externen Kreditsachbearbeitung für verschiedene Institute. Ähnlich wie in den USA, wo bei den Bankprodukten bereits seit geraumer Zeit der Trend hin zur Spezialisierung geht, sollen sich künftig auch in Deutschland Spezialbanken entwickeln, an die komplette Kreditengagements vermittelt werden. Kreditanträge von Kundinnen und Kunden, die nicht in das Angebot der Vertriebsbank passen, können dann gegen eine Provision über die Kreditfabrik an andere Banken

als Kreditgeberin vermittelt werden. In den USA sind inzwischen beispielsweise Baufinanzierungen aus einer Hand – wie in Deutschland noch traditionell der Fall – gänzlich unbekannt. Die Kreditnehmenden wissen dort oft nicht, welches Institut hinter der Finanzierung ihrer Vorhaben steht.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hält eine Auslagerung des Kreditbereichs unter bestimmten im Kreditwesengesetz (KWG) geregelten Voraussetzungen grundsätzlich für möglich. Neben den Anforderungen des KWG, deren Einhaltung von der BaFin beaufsichtigt werden, sind jedoch auch datenschutzrechtliche Vorschriften zu beachten. Dabei stellt sich zunächst die Frage, ob die Auslagerung des Kreditgeschäfts in eine Kreditfabrik als **Auftragsdatenverarbeitung** oder im Rahmen einer so genannten **Funktionsübertragung** erfolgt. Bei einer Auftragsdatenverarbeitung könnte für die mit der Auslagerung verbundene Weitergabe der Kundendaten an die Kreditfabrik auf eine besondere Rechtsgrundlage verzichtet werden. Ist dagegen mit der Auslagerung des Kreditbereichs die Übertragung selbständiger Funktionen verbunden, ist wegen des Bankgeheimnisses in jedem Einzelfall die Einwilligung der Antragstellerinnen und Antragsteller in die Übermittlung ihrer Daten an die Kreditfabrik erforderlich. Die Unterscheidung zwischen Auftragsdatenverarbeitung und Funktionsübertragung ist darüber hinaus entscheidend dafür, welche Stelle für die Einhaltung der datenschutzrechtlichen Vorgaben und die Wahrung der Rechte der Betroffenen wie zum Beispiel die Erfüllung des Auskunftsanspruchs verantwortlich ist. Im Falle einer Auftragsdatenverarbeitung bleibt im Verhältnis zu den Kundinnen und Kunden die auslagernde Bank nach außen verpflichtet. Übernimmt dagegen die Kreditfabrik selbständige Funktionen, wird sie selbst zur **verantwortlichen Stelle** und muss in Bezug auf die bei ihr vorgenommene Datenverarbeitung Auskunfts-, Löschungs- und Berichtigungsansprüche der Betroffenen erfüllen.

Eine pauschale Aussage zur Abgrenzung kann nicht getroffen werden. Entscheidend ist die individuelle Gestaltung der Beziehung zwischen der auslagernden Bank und der Kreditfabrik. Dabei spielt allerdings keine Rolle, ob die Kreditfabrik als konzernangehörige Tochtergesellschaft der Bank die Kreditbearbeitung übernimmt. Die gesellschaftsrechtlichen und wirtschaftlichen Zusammenhänge bleiben bei der datenschutzrechtlichen Beurteilung unberücksichtigt.

Die mit der Einschaltung einer Kreditfabrik verfolgten Automatisierungseffekte werden nicht zuletzt durch den Einsatz von Verfahren zum **Credit-**

Scoring bei der Bonitätsprüfung erreicht. Der Einsatz derartiger Verfahren führt aufgrund der mit ihnen verbundenen Standardisierung zu einer Reduzierung des Aufwandes für die kostenintensive Bonitätsprüfung. Der ermittelte Score-Wert zeigt an, wie hoch das statistische Ausfallrisiko für den beantragten Kredit ist. Wird ein bestimmter Score-Wert erreicht, wird der Kreditantrag in der Regel ohne weitere Prüfung abgelehnt. Spätestens mit Inkrafttreten der **Eigenkapitalvereinbarung Basel II** wird das Ergebnis des Credit-Scorings auch ausschlaggebend für die Höhe der aus dem Darlehensverhältnis verlangten Zinsen sein. Der Score-Wert wird dann selbst im Falle der Kreditbewilligung direkt finanziell spürbar.

Es bestehen verschiedene Möglichkeiten des Credit-Scorings. Entweder führt die Kreditfabrik ein eigenes internes Scoring-Verfahren durch oder sie bedient sich eines externen Dienstleisters wie der SCHUFA. In diesem Fall verknüpft die SCHUFA die bei ihr vorhandenen Daten zur Zahlungswilligkeit und -fähigkeit mit den bei Antragstellung erhobenen persönlichen Daten der Antragstellerin oder des Antragstellers, welche ihr von der Kreditfabrik zur Verfügung gestellt werden. Die SCHUFA errechnet daraus den Score-Wert, der dann in die anschließend von der Kreditfabrik vorgenommene Bonitätsbewertung einfließt. Soweit dabei ein negativer Score-Wert automatisch zur Ablehnung des Kreditantrags führen soll, gilt § 6a BDSG. Nach dieser Vorschrift dürfen beeinträchtigende Entscheidungen wie die Ablehnung eines Kreditantrags nicht ausschließlich auf Basis automatisierter Datenverarbeitungen getroffen werden. Ein Score-Verfahren ist nach Auffassung des Gesetzgebers ein Musterfall für eine derartige automatisierte Datenverarbeitung. Eine Ausnahme von dem **Verbot der automatisierten Einzelentscheidung** gilt nur dann, wenn die berechtigten Interessen der Kreditsuchenden beispielsweise dadurch gewahrt werden, dass sie ihren Standpunkt geltend machen können und die Entscheidung daraufhin noch einmal von einem Menschen überprüft wird.

Die Gefahr, dass bei der Bonitätsbewertung ein schiefes Bild entsteht und die Betroffenen in ihrer Kreditfähigkeit nicht hinreichend gewürdigt werden, ist gerade beim Einsatz von softwarebasierten Verfahren zur Bonitätsbewertung groß. Den Betroffenen wird in der Regel keine Auskunft über den zu ihrer Person errechneten Score-Wert erteilt. Oftmals fehlt auch den kreditbearbeitenden Sachbearbeiterinnen und Sachbearbeitern selbst der Einblick in die Art der verwendeten Daten und die Methodik der Errechnung des Score-Wertes. Nach dem BDSG haben die betroffenen Kreditsuchenden, deren Antrag aufgrund eines negativen Score-Wertes

abgelehnt wurde, jedoch nicht nur einen **Anspruch** auf Mitteilung des zu ihrer Person errechneten **Score-Wertes,** sondern auch zu der **Methodik** und der **Bewertungsgrundlage** des Credit-Scorings.

Die Aufsichtsbehörden werden im nächsten Jahr unter Vorsitz der LDI NRW gerade mit Blick auf die Umsetzung von Basel II dem Credit-Scoring besondere Aufmerksamkeit widmen und datenschutzrechtliche Rahmenbedingungen des Einsatzes von Verfahren zum Credit-Scoring erarbeiten.

5.9 Kleine Gefälligkeiten – kein Kavaliersdelikt!

Auch die Verpflichtung auf das Datengeheimnis scheint einige Beschäftigte nicht davon abzuhalten, im Rahmen einer „kleinen Gefälligkeit" Bekannten oder Verwandten Informationen über Kundendaten zukommen zu lassen. Da die Beschäftigten meist mit dem Vorsatz handeln, sich oder einen anderen zu bereichern beziehungsweise einen anderen zu schädigen, liegt vielfach nicht nur der Tatbestand einer Ordnungswidrigkeit, sondern sogar einer datenschutzrechtlichen Straftat vor. Oft fällt es jedoch schwer, den Verstoß nachzuweisen. Technische und organisatorische Maßnahmen könnten das ändern und sind daher datenschutzrechtlich geboten.

Im Berichtszeitraum häuften sich Beschwerden von Bürgerinnen und Bürgern, die überwiegend im Rahmen eines gerichtlichen Unterhalts- oder Scheidungsverfahrens von der Gegenseite mit **Informationen** zur eigenen Person konfrontiert wurden, von denen die gegnerische Partei normalerweise keine Kenntnis haben konnte.

In einem Fall legte der geschiedene Ehemann im Unterhaltsprozess die Kopie einer Versicherungskundenkarte vor, wonach die Exehefrau zwischenzeitlich einen neuen Lebenspartner im eigenen Haushalt mit versichert hatte. Unabhängig davon, dass der Eintrag des angeblichen Lebenspartners fälschlicherweise vorgenommen wurde, hätte der Exehemann nicht im Besitz der Kundenkarte sein dürfen. Wie sich herausstellte, wurde er von einem Mitarbeiter der betreffenden Versicherungsagentur wegen des Abschlusses einer Kfz-Versicherung aufgesucht. Bei den hierfür erforderlichen Unterlagen habe der Vermittler ‚versehentlich' die Kundenkarte der geschiedenen Ehefrau zur Hausratversicherung zum Besprechungstermin mitgenommen und beim geschiedenen Ehemann liegen gelassen. Hier steht der Verdacht im Raum, dass der Mitarbeiter des Versicherungsunternehmens unrichtige Daten zur Exehefrau gespeichert und diese Daten an den geschiedenen Gatten

übermittelt hat, um ihm gegebenenfalls einen Vorteil in der nachehelichen Unterhaltsklage zu verschaffen. Daher wurde die Angelegenheit zur Prüfung des entsprechenden **Straftatbestandes** an die zuständige Staatsanwaltschaft abgegeben. Sollte die vorsätzliche Weitergabe der Daten mit Bereicherungs- oder Schädigungsabsicht nicht nachweisbar sein, käme eine Ordnungswidrigkeit in Betracht, die mit einer Geldbuße bis maximal 250.000,-- Euro geahndet werden kann.

In einem anderen Fall wurde dem Betroffenen von seiner geschiedenen Ehefrau nahegelegt, auch das Konto „xy" bei der Aufstellung für die Zugewinngemeinschaft mit anzugeben. Überraschenderweise konnte sie ihm in diesem Gespräch des Weiteren den exakten aktuellen Kontostand benennen. Das Konto war allerdings weit nach der Trennung angelegt worden, so dass der Exehefrau hierzu keine Informationen vorliegen konnten, insbesondere auch nicht zu dem aktuellen Kontostand. Sie selbst war Mitarbeiterin eines Kreditinstitutes und befreundet mit einer Beschäftigten der Bank des Betroffenen. Die Umstände lassen vermuten, dass die Bankangestellte die Informationsquelle war. Das betreffende Kreditinstitut hatte jedoch kein technisches System eingesetzt, mit dem im Nachhinein festgestellt werden kann, welche Mitarbeiterinnen und Mitarbeiter welche Kundendaten eingesehen haben. Ohne diese **Protokollierung** von so genannten lesenden Zugriffen auf Kundendaten kann daher letztendlich nicht mehr festgestellt werden, welche Beschäftigten an dem entsprechenden Tag das Konto des Beschwerdeführers aufgerufen und gesichtet haben.

Eine solche Protokollierung hat in einem weiteren Fall den Filialleiter einer Bank veranlasst, bei der Staatsanwaltschaft eine Selbstanzeige zu erstatten. Durch die bankeigene **Innenrevision** war festgestellt worden, dass der Filialleiter die Kontodaten des geschiedenen Ehemannes seiner Schwägerin abgerufen hatte. Auf diesem Konto waren die Gehälter des Exehemannes eingegangen, welche für die Berechnung des Kindesunterhaltes von Bedeutung waren.

Die vermehrte Zahl der Beschwerden zeigt, dass grundsätzlich die Gefahr besteht, dass einzelne Mitarbeiterinnen oder Mitarbeiter in der verantwortlichen Stelle Verstöße gegen Datenschutzbestimmungen begehen, die entweder eine Ordnungswidrigkeit oder sogar eine Straftat darstellen, aber in keinem Fall zu den „Kavaliersdelikten" zählen. Wird der Aufsichtsbehörde die Möglichkeit genommen, diese Verstöße zu ahnden, ist hierin ein **Organisationsmangel** nach der Anlage zu § 9 BDSG zu sehen (vgl. Urteil des Verwaltungsgerichts Hamburg vom 21.11.2002, Aktenzeichen 22 VG

2830/99). Dieser Mangel liegt im Verantwortungsbereich des Kreditinstituts, da es als verantwortliche Stelle technische und organisatorische Maßnahmen zu treffen hat, die erforderlich sind, um die Ausführung der Vorschriften des BDSG in einem angemessenen Verhältnis zum angestrebten Schutzzweck zu gewährleisten. Es liegt somit im Interesse des Kreditinstituts selbst, zum einen präventiv Maßnahmen einzuführen, die die ‚kleinen Gefälligkeiten' weitestgehend verhindern und zum anderen repressiv in einem Verdachtsfall zumindest feststellen zu können, wer von den Beschäftigten in unzulässiger Weise auf Kundendaten zugegriffen hat.

Die Obersten Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich haben daher der Kreditwirtschaft empfohlen, ihre innerbetriebliche Organisation den Anforderungen des Datenschutzgesetzes anzupassen. Insbesondere wenn sehr viele Beschäftigte auf die Daten der Kundinnen und Kunden zugreifen können, ist eine generelle Protokollierungspflicht auch der Lesezugriffe datenschutzrechtlich geboten. Die insoweit vorbildliche Praxis einiger Kreditinstitute zeigt, dass dies technisch und organisatorisch durchaus möglich ist.

6 Verkehr

6.1 Passagierdatenübermittlung an U.S.-Zollbehörden

Seit dem 5. März 2003 sind die europäischen Fluggesellschaften aufgrund amerikanischer Antiterrorismusgesetzgebung von den US-Zollbehörden schrittweise verpflichtet worden, den Zugriff auf ihre Passagierdatenbanken zu eröffnen. Nach langen Verhandlungen zwischen den Vereinigten Staaten und der Europäischen Union wurde am 28. Mai 2004 ein Abkommen unterzeichnet, das die bis dahin fehlende Rechtsgrundlage für diesen Datentransfer bilden soll. Die Datenschutzgarantien, die dieses Abkommen bietet, werden zu Recht von den Europäischen Datenschutzbehörden und dem Europäischen Parlament als nicht ausreichend angesehen.

Nach den Anschlägen vom 11. September 2001 haben die Vereinigten Staaten verständlicherweise ein erhöhtes Sicherheitsbedürfnis. Das hat unter anderem auch unmittelbare **Auswirkungen auf in Europa stattfindende Datenverarbeitungen**. Diese Auswirkungen gehen allerdings über das hinaus, was sich noch als Maßnahme zur Terrorismusbekämpfung begreifen lässt. Schon lange vor den Anschlägen war es beim Flugverkehr zwischen Europa und den Vereinigten Staaten Praxis, dass mit dem Abflug in Europa die Identitätsdaten aus Reisepass und Visum oder Aufenthaltsgenehmigung der an Bord befindlichen Personen an die US-Einwanderungsbehörde übermittelt wurden. Die Zollbehörde der Vereinigten Staaten, das United States Bureau of Customs and Border Protection, verlangte auf der Grundlage der nach den Anschlägen erfolgten US-amerikanischen Gesetzgebung zur Terrorismusbekämpfung - The Aviation and Transportation Security Act vom 19.11.2001 - von den Fluggesellschaften darüber hinaus bei Flügen in und aus den USA Zugriff auf deren Passagierdatenbanken. In Nordrhein-Westfalen sind die Lufthansa und die LTU von diesem Verlangen betroffen.

Die **Passagierdatenbanken** enthalten alle Informationen, die für die Durchführung einer Flugreise erforderlich sind. Diese Informationen werden als „passenger name record" – kurz **PNR** – bezeichnet. Im PNR sind etwa alle mit dem Buchungsvorgang in Zusammenhang stehenden Auskünfte enthalten, die die reisende Person macht. So sind Angaben zur Zahlungsweise, zum Beispiel die Kreditkartennummer, oder der Name des Reisebüros, in dem gebucht wurde, im PNR zu finden. Die Sitzplatznummer beim Flug, etwaige Speisewünsche während des Fluges oder aufgrund von

Erkrankungen oder Behinderungen einer reisenden Person zu treffende Vorkehrungen sind ebenfalls in der Passagierdatenbank vermerkt. Gängige Bezeichnungen im PNR für solche Vorkehrungen sind cosher, moslem, hindu oder vegetarian meal für die Speisewünsche. Hinter den Systemkürzeln WCHR, BLD, DIS verbergen sich die Begriffe wheal chair, blind passenger, disabled passenger. Die meisten Passagiersysteme enthalten auch Felder, die mit einem beliebigen so genannten Freitext ausgestattet sein können. Es sollen sich darin vereinzelt sogar Vermerke dazu finden, dass Personen auf Flugreisen durch Alkoholmissbrauch oder Randalieren aufgefallen sind.

Der von den Vereinigten Staaten verlangte **Zugriff** auf diese Passagierdaten war nach europäischem und deutschem Datenschutzrecht **unzulässig**. Ein wesentliches Problem bereitete die Tatsache, dass es in den Vereinigten Staaten insbesondere für Personen, die nicht die amerikanische Staatsbürgerschaft besitzen, keine angemessenen Datenschutzrechte gibt. Die Fluggesellschaften wurden daher mit den sich widersprechenden Rechtsanforderungen der Vereinigten Staaten zum Zwecke der Terrorismus- und Kriminalitätsbekämpfung einerseits und der Europäischen Union zum Datenschutz andererseits konfrontiert. Beide Rechtssysteme belegen ihre Nichtbefolgung mit empfindlichen Geldbußen. In diesem Dilemma für die Fluggesellschaften wollte die Europäische Kommission Unterstützung leisten und hat Verhandlungen mit den Vereinigten Staaten über die Bedingungen, unter denen die Übermittlung von Passagierdaten möglich ist, aufgenommen. Die Ergebnisse dieser Verhandlungen sind in einer Verpflichtungserklärung der US-Zollbehörde vom 11.05.2004 festgehalten. Mit einer Entscheidung vom 14.05.2004 hat die Europäische Kommission daraufhin festgestellt, dass das **Datenschutzniveau** bei der Verarbeitung der Passagierdaten in den USA angemessen sei. Des Weiteren wurde am 28.05.2004 ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten über die Passagierdatenübermittlung unterzeichnet. Aus Sicht der Kommission sind damit die Rechtsgrundlagen geschaffen, die die Übermittlung ermöglichen. Die einzelnen Dokumente sind nachzulesen unter www.europa.eu.int.

Das Europäische Parlament hat Klage vor dem Europäischen Gerichtshof erhoben, um überprüfen zu lassen, ob die Rechte der Fluggäste aufgrund der **Anerkennungsentscheidung** vom 14.05.2004 und des Abkommens vom 28.05.2004 verletzt werden und eine Zustimmung des Parlamentes zu dem Abkommen erforderlich gewesen wäre. Tatsächlich sind auch nach

Abschluss des Abkommens einige kritische Punkte im Zusammenhang mit der Passagierdatenübermittlung noch gar nicht oder nur unbefriedigend gelöst. Der Umfang der Daten, auf die ein Zugriff besteht, ist nach europäischen Maßstäben nicht verhältnismäßig, weil ein Zusammenhang zur Terrorismusbekämpfung bei vielen Datenfeldern nicht erkennbar ist. Es besteht auch nach wie vor ein Zugriff auf **sensible Informationen** wie Gesundheitsdaten. Weiter ist die Notwendigkeit einer Mindestspeicherdauer von 3 1/2 Jahren für alle Daten, die keine besonderen Auffälligkeiten ergeben haben, nach wie vor nicht nachvollziehbar.

In einigen Fragen soll eine so genannte **„Push-Lösung"** Abhilfe schaffen. Das bedeutet, dass der unmittelbare Zugriff der US-Zollbehörden auf die Datenbanken abgelöst werden soll durch eine Übermittlung der Datenpakete, die in den Verhandlungen festgelegt wurden. Unklarheiten bestehen noch bei der Frage, wie und welche Daten mit sensitivem Charakter vor einer Übermittlung herausgefiltert werden können. Der Betreiber der Reservierungsdatenbank, aus der Lufthansa und LTU den Datenzugriff ermöglichen, ist mit der Entwicklung einer „Push-Lösung" befasst.

Ein wesentlicher Punkt, der von den Europäischen Datenschutzbeauftragten immer wieder bemängelt wurde, war die **fehlende Transparenz** bei der Passagierdatenübermittlung. Hierzu konnte erfreulicherweise auf europäischer Ebene ein einheitlicher Informationstext verabschiedet werden. Er kann unter www.europa.eu.int abgerufen werden. Die Fluggesellschaften und die an der Buchung beteiligten Reisegesellschaften wurden verpflichtet, bei jeder Buchungen von Flügen in die USA auf diesen Text hinzuweisen und ihn zur Information für die Reisenden vorzuhalten.

Außer den USA erheben weitere Staaten inzwischen vergleichbare Forderungen. Die Europäische Kommission verhandelt mit Kanada und Australien über die Modalitäten einer Passagierdatenübermittlung. Auch Großbritannien möchte auf die Reservierungsdaten der Fluggesellschaften zugreifen. Im Hinblick auf diese Forderungen ist es angezeigt, die Passagierdatenübermittlung endlich mit einer **europäischen Rechtsvorschrift** zu regeln, in der die Voraussetzungen für eine zulässige Übermittlung normenklar und einheitlich festgelegt sind.

In der weltweiten Diskussion um die Sicherheit im Flugverkehr müssen und werden die Datenschutzbeauftragten dafür eintreten, dass die Passagierdatenübermittlung auf ein den Sicherheitsanforderungen entsprechendes Maß

zurückgeführt wird. Den Reisenden ist zu raten, bei der Buchung sehr bewusst zu überlegen, welche Informationen sie von sich preisgeben.

6.2 Fluggepäck wird schon vor der Landung elektronisch durchgecheckt

Über ihr ankommendes Gepäck weiß der Zoll in Frankfurt bereits vor der Landung mehr als die Fluggäste. In einem zeitlich begrenzten Pilotprojekt erhält der Zoll am Flughafen Frankfurt Daten über das auf dem Weg dorthin beförderte Fluggepäck.

Die Daten werden beim Check-In am Schalter der Lufthansa am Abflughafen erhoben und in das internationale **Dateninformationssystem** (Baggage Management System) eingespeist, das für den Transport des Gepäcks zum richtigen Flugzeug über den richtigen Umsteigeflughafen zum richtigen Zielflughafen sorgen soll. Der Zoll erhält so Auskunft über Namen und Geschlecht der Passagiere sowie über die Flugrouten (Abflughäfen/Zwischenstopps/Anschlussverbindungen).

Diese Datenübermittlung findet ohne Wissen der Flugpassagiere statt und wird allein gerechtfertigt aus einer weiten Auslegung unklarer Zollbestimmungen und des Betäubungsmittelgesetzes. Deshalb hat der Bundesbeauftragte für den Datenschutz in Abstimmung mit der LDI darauf bestanden, dass eine Weiterführung des Pilotprojektes nur auf der Grundlage einer bereichspezifischen **gesetzlichen Bestimmung** (etwa im Luftverkehrsgesetz) möglich ist. Außerdem muss für eine ausreichende **Information** der Fluggäste Sorge getragen werden. Die Fluggesellschaft fühlt sich aber für die Unterrichtung ihrer Fluggäste nicht verantwortlich, weil die Daten nicht von ihr, sondern vom Frankfurter Flughafen an den Zoll übermittelt werden. Der Flughafen erhält die Gepäckdaten aus dem internationalen Gepäck-Informationssystem, das allerdings von den Check-In-Schaltern der Fluggesellschaften gefüttert wird. Deshalb trifft die Fluggesellschaft, die im Übrigen allein den Kontakt zu den Passagieren hat, die Unterrichtungspflicht. Sie weist in ihren Geschäftsbedingungen zwar allgemein auf eine Übermittlung personenbezogener Daten im Zusammenhang mit der durchgeführten Reise an Behörden im In- und Ausland hin. Dieser Hinweis genügt jedoch nicht, weil die Fluggäste nicht erkennen können, dass die Daten ihres Gepäcks neuerdings und ohne ihre Mitwirkung an den Zoll übermittelt werden.

Die Fluggesellschaft, die Frankfurt anfliegt, muss ihre Fluggäste ausdrücklich darüber unterrichten, dass der Zoll bereits vor ihrer Ankunft erfährt, von wo aus und auf welcher Reiseroute sie nach Franfurt kommen. Der allgemeine Hinweis, Passagierdaten würden auch an Behörden übermittelt, reicht nicht.

7 Verfassungsschutz

Überrascht reagierte ein Bürger, als er anlässlich einer Recherche im Internet seinen Namen im Zusammenhang mit extremistischen Aktivitäten fand. Die Spur führte zu einem 15 Jahre alten Verfassungsschutzbericht, der gemeinsam mit anderen alten Berichten von der Verfassungsschutzbehörde in ihre Internetpräsentation eingestellt worden war.

Ausnahmsweise dürfen in den für die Veröffentlichung bestimmten Berichten des Verfassungsschutzes auch personenbezogene Daten genannt werden. Zulässig ist dies nur, wenn die Bekanntgabe für das Verständnis des Zusammenhangs oder der Darstellung von Organisationen erforderlich ist und die Interessen der Allgemeinheit das schutzwürdige Interesse der betroffenen Personen überwiegen. Eine besondere Qualität erfährt der damit verbundene Eingriff in das Recht auf informationelle Selbstbestimmung, wenn die in gedruckter Form veröffentlichten Berichte **dauerhaft ins Internet** gestellt werden. Die Berichte einschließlich der namentlichen Erwähnungen der Betroffenen bleiben auf diese Weise jahrzehntelang weltweit abrufbar und können etwa über die einfache Eingabe des Namens in eine gängige Internet-Suchmaschine aufgefunden werden. Die Betroffenen werden mit der Veröffentlichung im Internet täglich neu in einen Zusammenhang mit extremistischen Organisationen und Aktivitäten gestellt, der längst der Vergangenheit angehören kann, und müssen schlimmstenfalls berufliche oder private Nachteile befürchten.

Eine dauerhafte Veröffentlichung personenbezogener Daten aus Verfassungsschutzberichten im Internet greift in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung ein und ist für die Erfüllung der Aufgaben des Verfassungsschutzes nicht erforderlich. Die Verfassungsschutzbehörde wird deshalb Verfassungsschutzberichte nach Ablauf von fünf Jahren seit der ersten Veröffentlichung nicht mehr im Internet zum Abruf bereitstellen.

8 Polizei

8.1 Änderungen des Polizeigesetzes

Das Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW) ist im Berichtszeitraum in wichtigen Punkten überwiegend zum Nachteil des Rechts auf informationelle Selbstbestimmung geändert worden. Hervorzuheben sind insbesondere die Änderungen der Voraussetzungen der Videoüberwachung (§ 15a PolG NRW) und der Rasterfahndung (§ 31 PolG NRW) durch die Polizei sowie die neuen Rechtsgrundlagen für den Einsatz von Videokameras in Streifenwagen und für die Aufzeichnung von Anrufen über die Notrufnummer 110.

Erstmals im Mai 2000 ist der Polizei durch den neu geschaffenen § 15a PolG NRW unter engen Voraussetzungen die **Videoüberwachung** einzelner öffentlich zugänglicher Orte erlaubt worden. Bereits damals bestanden erhebliche Zweifel an dem praktischen Nutzen der Videoüberwachung durch die Polizei. Tatsächlich hatte nach dem In-Kraft-Treten der Gesetzesänderung auch nur die Polizei in Bielefeld von der neu eingeräumten Eingriffsbefugnis Gebrauch gemacht, obwohl für die überwachten Bereiche das Vorliegen eines Kriminalitätsbrennpunkts nicht überzeugend begründet werden konnte (siehe 15. Datenschutzbericht 2001 unter 3.1.4, S. 63 und 3.1.5, S. 64). Die naheliegende Schlussfolgerung, auf die Videoüberwachung durch die Polizei künftig wieder zu verzichten und § 15a PolG NRW zu streichen, hat der Gesetzgeber indes nicht gezogen. Vielmehr ist die Schwelle für den Kameraeinsatz bedauerlicherweise gesenkt worden, ohne dass valide wissenschaftliche Erkenntnisse vorlägen, die eine tatsächliche Reduzierung des Straftatenaufkommens durch den Einsatz von Videoüberwachungen belegen.

Nach dem neu gefassten § 15a PolG NRW kann die Polizei nunmehr zur Verhütung von Straftaten einzelne öffentlich zugängliche Orte, an denen wiederholt Straftaten begangen wurden und deren Beschaffenheit die Begehung von Straftaten begünstigt, mittels Bildübertragung beobachten und die übertragenen Bilder aufzeichnen, solange Tatsachen die Annahme rechtfertigen, dass an diesem Ort weitere Straftaten begangen werden. Die auf höchstens 14 Tage begrenzte **Speicherdauer** der übertragenen Bilder darf nur ausnahmsweise überschritten werden, etwa wenn die Aufzeichnung zur Verfolgung einer Straftat benötigt wird.

Wie sich aus der Begründung zur Änderung des § 15a PolG NRW ergibt, waren neben anderen Gesichtspunkten erhebliche Zweifel an der Verfassungsmäßigkeit der bisherigen Regelung Anlass für die Änderung. Insbesondere die der Polizei durch die frühere Fassung des § 15a PolG NRW eingeräumte Befugnis, die übertragenen Bilder bei Verdacht einer begonnenen oder unmittelbar bevorstehenden Straftat aufzuzeichnen und die Aufzeichnungen zum Zweck der Strafverfolgung zu verwenden, stellte einen unzulässigen Eingriff des Landesgesetzgebers in das der Gesetzgebungskompetenz des Bundes unterliegende Strafverfahrensrecht dar (LT-Drs. 13/2854, S. 54). Diese kompetenzrechtlichen Probleme werden durch die Neuregelung nicht überzeugend gelöst. Dem Wortlaut der Neuregelung folgend soll die Aufzeichnung der Bilder nunmehr der Verhütung von Straftaten dienen. Diesen Zweck kann die **bloße Dokumentation** des Geschehens nicht erfüllen. Vielmehr kann die Aufzeichnung und Speicherung in der Praxis immer nur der Beweissicherung in einem künftigen Strafverfahren, also der Strafverfolgung, dienen. Hierfür steht mit § 100c Abs. 1 Strafprozessordnung (StPO) eine Rechtsgrundlage im Strafverfahrensrecht zur Verfügung. Zu anderen Zwecken ist die Aufzeichnung ungeeignet. Denn entweder wird der erstrebte Abschreckungs- oder Verdrängungseffekt bereits durch die Existenz der Kamera und den Umstand der Beobachtung erzielt oder es ist zur Gefahrenabwehr oder zur Verhütung einer Straftat das sofortige polizeiliche Eingreifen vor Ort notwendig.

Die fortbestehenden Probleme werden bei der Umsetzung des novellierten § 15a PolG NRW in die Praxis deutlich. So sehen sich die meisten Polizeibehörden, die bereits Überwachungskameras auf der Grundlage des neu gefassten § 15a PolG NRW einsetzen oder planen, häufig nicht in der Lage, eine **fortlaufende Beobachtung** der beständig übertragenen und gespeicherten Bilder durch Polizeibeamtinnen und Polizeibeamte sicherzustellen. Dies führt nicht nur dazu, dass den Bürgerinnen und Bürgern, die auf eine ständige Beobachtung durch die Polizei vertrauen, eine trügerische Sicherheit vorgespiegelt wird. Vielmehr widerspricht eine Aufzeichnung der übertragenen Bilder „auf Vorrat", ohne dass eine Beobachtung durch einen Polizeivollzugsbeamten erfolgt, auch dem Wortlaut des § 15a Abs. 1 Satz 1 PolG und ist mit dem ausschließlich präventiven Charakter der Regelung, die eine Videoüberwachung ausschließlich „zur Verhütung von Straftaten" erlaubt, unvereinbar. Zur Regelung einer ausschließlich repressiv wirkenden Videoaufzeichnung fehlt dem Landesgesetzgeber nach wie vor die Gesetzgebungskompetenz.

Konsequent wäre es deshalb, auf die Befugnis zur Aufzeichnung von Bildern im Polizeigesetz ganz zu verzichten.

Darüber hinaus beschränkt die Neuregelung eine Videoüberwachung nicht mehr nur auf Straftaten von erheblicher Bedeutung. Erlaubt ist eine Videoüberwachung nunmehr bei **allen Straftaten**. Auch dagegen bestehen erhebliche Bedenken. Eine spürbare **Ausweitung des Kameraeinsatzes** durch die Polizei wird damit wahrscheinlich. Von jeder einzelnen Kamera ist jeweils eine Vielzahl von Menschen betroffen, die sich rechtstreu verhält. Die Videobeobachtung auf öffentlichen Straßen und Plätzen muss deshalb die Ausnahme bleiben. Ist die Möglichkeit unbeobachteter Bewegung auch und gerade bei einer kleinräumigen Betrachtung, etwa im Innenstadtbereich, nicht mehr die Regel, wird der Verhältnismäßigkeitsgrundsatz verletzt.

Erlaubt ist die Videoüberwachung durch die Polizei nunmehr an öffentlich zugänglichen Orten, an denen wiederholt Straftaten begangen wurden, und – das ist neu – deren Beschaffenheit die Begehung von Straftaten begünstigt. Damit soll nach der Begründung des Gesetzes verhindert werden, dass eine Videoüberwachung an Örtlichkeiten erfolgt, an denen ausschließlich mit einem Verdrängungseffekt zu rechnen ist. Ergänzend wird in den zwischenzeitlich neu gefassten Verwaltungsvorschriften zu § 15a PolG NRW ausdrücklich festgestellt, dass eine Videoüberwachung unzulässig ist, wenn sie aller Wahrscheinlichkeit nach nur zu einem **Verdrängungseffekt** führt. Eingesetzt werden darf die Videoüberwachung nach den Verwaltungsvorschriften darüber hinaus nur im Rahmen eines **Gesamtkonzepts,** das auf die spezifischen Gegebenheiten abgestimmt ist und ergänzende Maßnahmen vorsieht. Schließlich ist § 15a PolG NRW noch im Gesetzgebungsverfahren um weitere formale Regelungen ergänzt worden: Über die Einrichtung einer Videoüberwachung entscheidet ausschließlich die Behördenleiterin oder der Behördenleiter. Videoüberwachungsmaßnahmen sind grundsätzlich auf ein Jahr – allerdings mit der Möglichkeit der Verlängerung – befristet und zu dokumentieren. Ob diese Beschränkungen ausreichen werden, eine erhebliche Ausweitung der Videoüberwachung durch die Polizei zu verhindern, darf bezweifelt werden.

Neue **Funkstreifenwagen** der Polizei werden in Nordrhein-Westfalen künftig mit **Videosystemen** zur Eigensicherung ausgestattet. Personen- und Fahrzeugkontrollen können damit durch Videoaufzeichnung dokumentiert werden. Rechtsgrundlage für den Einsatz der Überwachungskameras ist der neu in das Polizeigesetz aufgenommene § 15b PolG NRW. Die Kamera wird aktiviert, wenn das optische Anhaltesignal des Streifenwagens

eingeschaltet wird, um ein vorausfahrendes Fahrzeug anzuhalten. Die laufende Bildaufzeichnung wird nach außen durch eine nach vorn sichtbare rote Leuchte und im Fahrzeug durch ein im Bedienknopf integriertes grünes Blinklicht erkennbar gemacht. Darüber hinaus sind die Beamtinnen und Beamten angewiesen, die Betroffenen auf den Einsatz des Videosystems zu Beginn der Kontrolle hinzuweisen. Die Bildaufzeichnungen sind am Tage nach der Aufzeichnung zu löschen, wenn sie nicht ausnahmsweise als Beweismittel für die Verfolgung einer Straftat oder einer Ordnungswidrigkeit benötigt werden.

Die gegen jede Form einer Ausweitung der Videoüberwachung durch öffentliche oder private Stellen grundsätzlich bestehenden Bedenken gelten auch hier. Anders als bei der Überwachung öffentlich zugänglicher Straßen und Plätze nach §15a PolG NRW ist es bei dem Einsatz von Kameras in Streifenwagen allerdings nicht ausgeschlossen, dass damit die Eigensicherung der Beamtinnen und Beamten gefördert wird.

Die **Aufzeichnung** der unter der **Notrufnummer 110** bei der Polizei eingehenden Anrufe hat nach langen Jahren endlich in § 24 Abs. 5 PolG NRW eine gesetzliche Grundlage. Die Aufzeichnungen sind spätestens nach einem Monat zu löschen, wenn sie nicht zur Verfolgung von Straftaten benötigt werden oder der Verdacht besteht, dass die anrufende Person Straftaten begehen wird und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten erforderlich ist.

Eine weitreichende Änderung hat auch die Regelung der **Rasterfahndung** in § 31 PolG NRW erfahren. Vor der Novelle des Polizeigesetzes war eine Rasterfahndung auf polizeirechtlicher Grundlage nur zulässig, wenn eine gegenwärtige Gefahr vorlag. Das schadenstiftende Ereignis musste also unmittelbar bevorstehen oder bereits eingetreten sein. Ausreichend ist nunmehr jede, auch zeitlich entfernte Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person. Schon bisher erlaubte die Rasterfahndung als **Verdachtsschöpfungsmethode** schwerwiegende Eingriffe in das informationelle Selbstbestimmungsrecht einer Vielzahl unbescholtener und unverdächtiger Bürgerinnen und Bürger. Mit dem Verzicht auf eine gegenwärtige Gefahr wurden die Anforderungen an die Zulässigkeit der polizeilichen Rasterfahndung noch einmal deutlich abgesenkt. Das Instrument der Rasterfahndung entfernt sich damit weiter von dem Grundsatz des Polizeirechts, dass in die Rechte von Bürgerinnen und Bürgern, die sich gesetzestreu verhalten und von denen keine Gefahr ausgeht, nur

ausnahmsweise eingegriffen werden darf, wenn eine erhebliche Gefahr bereits eingetreten ist oder unmittelbar bevorsteht.

Die Novellierung des Polizeigesetzes hat zu weiteren Einschränkungen des Grundrechts auf informationelle Selbstbestimmung geführt. Die ohnehin gegen das Instrument der polizeilichen Rasterfahndung unter grundrechtlichen und rechtsstaatlichen Gesichtspunkten bestehenden erheblichen Bedenken werden durch die weitere Absenkung der Einsatzschwelle weiter verstärkt. Die Neuregelung der Videoüberwachung hat die bestehenden rechtlichen Probleme nicht gelöst, sondern neue geschaffen. Die weitere Entwicklung der Videoüberwachung durch die Polizei wird kritisch zu begleiten sein. Die Möglichkeit der unbeobachteten Bewegung auch in den Innenstädten muss der Regelfall bleiben.

8.2 Nachlese Rasterfahndung

Sämtliche Daten, die im Rahmen der auch in Nordrhein-Westfalen als Reaktion auf die Terroranschläge vom 11. September 2001 in den USA vom Polizeipräsidium Düsseldorf noch auf der Grundlage des § 31 PolG NRW in seiner alten Fassung durchgeführten Rasterfahndung zur Aufdeckung potentieller islamistischer Terroristen erhoben wurden, sind zwischenzeitlich gelöscht.

Auf der Grundlage eines Beschlusses des Amtsgerichts Düsseldorf von Oktober 2001 wurden allein in Nordrhein-Westfalen etwa **5 Mio. Datensätze** von den Einwohnermeldeämtern, aus dem Hochschulbereich sowie aus dem Ausländerzentralregister erhoben. Dabei hatte das Oberlandesgericht Düsseldorf (Beschluss vom 8. Februar 2002 – 3 Wx 357/01) der Rasterfahndung in Nordrhein-Westfalen Grenzen gesetzt und die Einbeziehung deutscher Staatsangehöriger in die Suchaktion ausdrücklich als unverhältnismäßig bezeichnet. Allerdings hat das Gericht gleichzeitig entschieden, dass die nach § 31 PolG NRW in seiner alten Fassung erforderliche **gegenwärtige Gefahr** vorgelegen habe, und die Einbeziehung von Personen aus islamischen Ländern gebilligt (siehe 16. Datenschutzbericht 2003 unter 16, S. 151 – 153). Abzuwarten bleibt, ob die gegen diese Entscheidung gerichtete **Verfassungsbeschwerde** eines in Deutschland lebenden marokkanischen Studenten Erfolg haben wird. Die Begründung des Beschwerdeführers, der Beschluss des Oberlandesgerichts Düsseldorf sei willkürlich gewesen, da es für die Annahme einer **gegenwärtigen** Gefahr an hinreichenden Tatsachen gefehlt habe, ist

jedenfalls – wie Entscheidungen anderer Fachgerichte zeigen – nicht ohne weiteres von der Hand zu weisen. So hat das Oberlandesgericht Frankfurt (Beschluss vom 21. Februar 2002 – 20 W 55/02) im Hinblick auf die auch in Hessen vorgesehene Rasterfahndung festgestellt, vom Vorliegen einer gegenwärtige Gefahr könne nicht ausgegangen werden.

Aus den erhobenen ca. 5 Mio. Datensätzen wurden etwa **11.000 Datensätze** von Personen mit potentieller Gefährdungsrelevanz „ausgerastert". Im Rahmen der sich anschließenden polizeilichen Überprüfungen wurden bis Juni 2003 zunächst die Datensätze von etwa 9.500 dieser Personen gelöscht. Im Frühjahr 2004 erfolgte die Vernichtung der restlichen Daten. Alle etwa 11.000 im Rahmen der Rasterfahndung überprüften Personen wurden nach Abschluss der Überprüfungen durch das Polizeipräsidium Düsseldorf schriftlich über die erfolgte Datenerhebung und den Zeitpunkt der beabsichtigten Löschung informiert. Die Entwürfe dieser Anschreiben und die Adresslisten wurden im Anschluss vernichtet beziehungsweise gelöscht, so dass auch insoweit keine personenbezogenen Daten aus der Rasterfahndung zurückgeblieben sind. Die Landesbeauftragte für Datenschutz und Informationsfreiheit wurde durch das Polizeipräsidium beständig über den Sachstand unterrichtet und hat das Verfahren zur Benachrichtigung der Betroffenen und Löschung der Daten kontinuierlich begleitet. Im August 2004 wurde auf der Grundlage von etwa 900 der zuvor zu Kontrollzwecken kopierten Datensätzen eine **Stichprobe** beim Polizeipräsidium Düsseldorf durchgeführt. Der **Kontrollbesuch** erbrachte keine Hinweise darauf, dass Daten aus der Rasterfahndung zurückbehalten oder Eingang in andere polizeiliche Dateien gefunden hätten. Sämtliche zu Kontrollzwecken kopierten Datensätze wurden unmittelbar im Anschluss an den Kontrollbesuch vernichtet. Kritisch bleibt anzumerken, dass auch in Nordrhein-Westfalen durch die Rasterfahndung tausende unbescholtener Bürgerinnen und Bürger in das Blickfeld der Polizei geraten und zum Gegenstand polizeilicher Überprüfungen geworden sind, ohne dass messbare Erfolge bei der Suche nach Verdächtigen oder potentiellen islamistischen Terroristen bekannt wurden.

Die bestehenden Zweifel an der Eignung und Verhältnismäßigkeit der Rasterfahndung als Verdachtsschöpfungsmethode werden durch dieses ernüchternde Ergebnis und den erforderlichen erheblichen personellen Aufwand bestätigt und verstärkt. Die anhängige Verfassungsbeschwerde bietet deshalb eine willkommene Gelegenheit, die Rasterfahndung insgesamt auf den Prüfstand der Verfassung zu stellen und dem

computergestützten Pauschalverdacht gegen ganze Teile der Bevölkerung Grenzen zu setzen.

8.3 Von der Demo in die Datei

Die Beschwerde eines Betroffenen offenbarte technische und organisatorische Mängel bei der Durchführung des Kriminalpolizeilichen Meldedienstes in Fällen so genannter politisch motivierter Kriminalität.

Um auf eine umweltpolitische Forderung aufmerksam zu machen, entrollten fünf Personen auf einer Rheinbrücke ein Transparent. Zu diesem Zweck seilten sich drei von ihnen von der Brücke ab. Ein Vorgang, der einem Beteiligten nicht nur eine Strafanzeige wegen eines möglichen Verstoßes gegen das Versammlungsgesetz einbrachte, sondern auch eine vom Landeskriminalamt veranlasste Erfassung in der beim Bundeskriminalamt bundesweit geführten Verbunddatei **APIS** (Arbeitsdatei PIOS-Innere Sicherheit) als politisch motivierter Straftäter. Grundlage dieses Verfahrens sind die seit 2001 neu gefassten, bundesweit gültigen **Richtlinien für den kriminalpolizeilichen Meldedienst in Fällen politisch motivierter Kriminalität (KPMD-PMK)**. Danach werden politisch motivierte Straftaten von den Staatsschutzstellen der örtlich zuständigen Polizeibehörden über das Landeskriminalamt an das Bundeskriminalamt gemeldet. Gleichzeitig werden die meldepflichtigen Fälle vom Landeskriminalamt in die Verbunddatei APIS eingestellt.

Auch die nur zwei Wochen später erfolgte **Einstellung** des Ermittlungsverfahrens gegen den Betroffenen durch die Staatsanwaltschaft änderte nichts an dessen Erfassung in APIS. Hier ist nicht nur ein Betroffener vorschnell mit dem Etikett eines politischen Straftäters versehen worden. Vielmehr offenbarte der Einzelfall gleichzeitig erhebliche organisatorische Mängel, da die zuständige Polizeibehörde einräumen musste, es sei nicht mehr nachzuvollziehen, wann und wie der Sachverhalt an wen mit der Folge der Erfassung in der beim Bundeskriminalamt geführten bundesweiten Datei gemeldet worden sei.

Die aus dem Vorfall gespeicherten Daten sind zwischenzeitlich **gelöscht** worden. Die Polizeibehörde hat organisatorische Maßnahmen ergriffen, die es künftig ermöglichen, entsprechende Meldungen nachzuvollziehen. Außerdem wird einer Empfehlung der Landesbeauftragten für Datenschutz und Informationsfreiheit folgend in dem die Einführung der Richtlinien

begleitenden Runderlass des Innenministeriums nunmehr eindeutig auf bestehende Veränderungs- und Löschungspflichten hingewiesen.

Steht aufgrund einer Entscheidung einer Staatsanwaltschaft oder eines Gerichts fest, dass die Meldung und Erfassung einer Person als politisch motivierter Straftäter vorschnell oder zu Unrecht erfolgt ist, hat auch darüber eine Meldung an das Landeskriminalamt zu erfolgen. Das Landeskriminalamt hat sodann die Löschung der Daten in der beim Bundeskriminalamt geführten Verbunddatei APIS zu veranlassen.

8.4 Verbesserter Datenschutz bei der Führung von Kriminalakten

Einer Entscheidung des Bundesverfassungsgerichts folgend sind die Regelungen zur Aufbewahrung und Löschung von Daten in Kriminalakten präzisiert worden.

Nach dem neugefassten Runderlass sind bei einem rechtskräftigen Freispruch wegen erwiesener Unschuld in einer gerichtlichen Hauptverhandlung die verfahrensbezogenen Daten nunmehr ausnahmslos zu löschen. Grundsätzlich gilt dies auch bei einem Freispruch aus anderen Gründen, etwa weil der Tatvorwurf nicht mit hinreichender Sicherheit nachgewiesen werden kann, sowie bei Verfahrenseinstellungen. In diesen Fällen ist ein Verbleib der Daten in den Kriminalakten nur ausnahmsweise zulässig. Die weitere Aufbewahrung setzt dann voraus, dass weiterhin Verdachtsmomente gegen die betroffene Person bestehen, die eine Fortdauer der Speicherung zur präventiv-polizeilichen Verbrechensbekämpfung rechtfertigen und eine Würdigung aller relevanten Umstände des Einzelfalls zu dem Ergebnis führt, dass eine Wiederholungsgefahr besteht. Notwendig ist in diesen Fällen also nicht nur, dass trotz Freispruchs oder Einstellung des Verfahrens ein Restverdacht gegen die betroffene Person bestehen bleibt, sondern vor allem auch eine Prognoseentscheidung darüber, dass sie in ähnlicher Weise erneut straffällig werden könnte. Außerdem berücksichtigt der Runderlass die Empfehlung, die **Gründe** für die weitere Speicherung **aktenkundig** zu machen. Hierdurch wird sowohl der Ausnahmecharakter einer weiteren Aufbewahrung der Daten unterstrichen als auch die Nachprüfung der Entscheidungen der Polizei verbessert.

Damit die über eine Person geführte Kriminalakte stets eine aktuelle und verlässliche Grundlage für die Beurteilung der Frage bildet, ob eine weitere Speicherung von Daten erforderlich oder eine Löschung von Daten zu veranlassen ist, hat die Staatsanwaltschaft die Polizei über den Ausgang

strafrechtlicher Ermittlungsverfahren zu unterrichten; die Polizei hat die Mitteilungen der Staatsanwaltschaft zur Akte zu nehmen, sofern nicht aufgrund der Mitteilung des Verfahrensausgangs ohnehin eine Löschung zu veranlassen ist. Verschiedene Einzelfälle geben Anlass, hieran zu erinnern.

8.5 Zweifelhafter Fernsehruhm

Wer die Polizei etwa wegen eines nächtlichen Einbruchs oder eines anderen Notfalls anruft, erwartet schnelle und kompetente Hilfe. Eine neue Erfahrung ist allerdings für viele Betroffene, dass diese Hilfe auch in Begleitung eines kompletten Filmteams, ausgestattet mit Fernsehkamera und Mikrophon, am Tatort erfolgt.

Hintergrund sind Fernsehsendungen des so genannten Reality-TV, bei denen Polizeibeamtinnen und Polizeibeamte mit Zustimmung der Polizeibehörde von Journalistinnen und Journalisten begleitet werden, die den gesamten Einsatz filmen. So geschehen etwa in Köln, Bielefeld und Bochum. Manche Polizeibeamte, wie etwa die zeitweise sehr populären Bochumer Polizisten „Toto und Harry", sind auf diese Weise zu Fernsehstars geworden. Die Kehrseite dieser Art von Öffentlichkeitsarbeit sind indes immer wieder Beschwerden – ja sogar Strafanzeigen – betroffener oder besorgter Bürgerinnen und Bürger, die sich durch die Filmaufnahmen oder deren Ausstrahlung in ihrem Recht am eigenen Bild und anderen Teilen ihres Allgemeinen Persönlichkeitsrechts erheblich verletzt fühlen. Eine Rechtsgrundlage, die es erlaubt, an Polizeieinsätzen beteiligte Bürgerinnen und Bürger zu filmen, existiert nicht. Zulässig sind entsprechende Aufnahmen deshalb nur, wenn die Betroffenen zuvor über den genauen Verwendungszweck der Filmaufnahmen aufgeklärt worden sind und in die Fertigung der Aufnahmen eindeutig und unmissverständlich **schriftlich eingewilligt** haben.

In der Hektik des polizeilichen Einsatzalltags können diese strengen rechtlichen Anforderungen kaum erfüllt werden. Es sei denn, den zu einem Einsatz herbeigerufenen Polizeibeamtinnen und Polizeibeamten sowie den betroffenen Bürgerinnen und Bürgern würde zugemutet werden, vor dem polizeilichen Tätigwerden zunächst einmal abzuwarten, ob den begleitenden Journalisten alle erforderlichen **schriftlichen Einverständniserklärungen** der Beteiligten erteilt werden. Stehen Beteiligte offensichtlich unter dem Einfluss von Alkohol oder Drogen oder befinden sie sich – wie dies im polizeilichen Alltag nicht selten anzutreffen sein wird – aus anderen Grün-

den in einem Zustand starker psychischer Belastung, dürfte es zudem schon an der Fähigkeit fehlen, eine rechtlich verbindliche Einwilligung in Film- und Tonaufnahmen zu erteilen.

Erfolgen Filmaufnahmen und deren Ausstrahlung im Fernsehen ohne eine rechtswirksame Einwilligung der gefilmten Personen, so stellt dies eine – unter Umständen schwerwiegende – Verletzung des Rechts am eigenen Bild und gegebenenfalls auch anderer Teile des Allgemeinen Persönlichkeitsrechts dar. Es ist deshalb erfreulich, dass die Ständige Konferenz der Innenminister und -senatoren der Länder zwischenzeitlich eine grundsätzliche Ablehnung der Mitwirkung der Polizei an Medienproduktionen im Rahmen von Reality-Formaten beschlossen hat. Leider ist das Innenministerium einer bereits länger zurückliegenden entsprechenden Empfehlung der Landesbeauftragen für Datenschutz und Informationsfreiheit, eine Begleitung der Polizei durch Filmteams generell zu verbieten, bisher nicht gefolgt.

9 Justiz

9.1 Bundesverfassungsgericht stärkt das Allgemeine Persönlichkeitsrecht

In seinem Urteil vom 3. März 2004 (BVerfGE 109/279) hat das Bundesverfassungsgericht den „großen Lauschangriff" in weiten Teilen für verfassungswidrig erklärt. Die Bezeichnung „großer Lauschangriff" steht für die in der Strafprozessordnung (StPO) geregelte akustische Überwachung des nichtöffentlich gesprochenen Wortes in einer Wohnung zum Zweck der Strafverfolgung.

Die hervorgehobene Bedeutung dieser Entscheidung liegt insbesondere in den klaren Worten, die das Gericht zum Schutz des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung gefunden hat. Insbesondere bestätigt das Bundesverfassungsgericht unmissverständlich, dass es einen absolut geschützten Kernbereich privater Lebensgestaltung gibt, der **jeglichen staatlichen Eingriffen entzogen** ist. Die bestehenden Regelungen in der StPO tragen dem nicht hinreichend Rechnung und müssen in weiten Teilen überarbeitet werden. Das Gericht hat damit einer Strafverfolgung um jeden Preis eine deutliche Absage erteilt. Den Gesetzgeber hat das Bundesverfassungsgericht aufgefordert, spätestens bis zum 30. Juni 2005 die entsprechenden Vorschriften in der StPO zu ändern und einen verfassungsgemäßen Rechtszustand herzustellen.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die strafprozessuale akustische Überwachung des gesprochenen Wortes in Wohnungen von Bedeutung. Vielmehr ist bei allen staatlichen Eingriffs- und Überwachungsmaßnahmen der grundrechtlich **absolut geschützte unantastbare Kernbereich privater Lebensgestaltung** zu respektieren. Dies gilt nicht nur für Eingriffsbefugnisse zum Zweck der Strafverfolgung, sondern auch für staatliche Maßnahmen, die der Gefahrenabwehr oder der Verhütung von Straftaten dienen, sowie für die Eingriffsbefugnisse der Nachrichtendienste. Keine Rolle spielt auch, ob es sich um bundes- oder landesrechtliche Regelungen handelt.

In ihrer Entschließung vom 25./26. März 2004 (Abdruck im Anhang, Nr. 16) weisen die Datenschutzbeauftragten des Bundes und der Länder deshalb darauf hin, dass nunmehr alle Formen verdeckter Datenerhebung, wie etwa auch die Telekommunikationsüberwachung, auf den Prüfstand gehören und

sich an den vom Bundesverfassungsgericht aufgestellten Maßstäben messen lassen müssen.

9.2 Keine Erweiterung der DNA-Analyse zulassen

Die Entnahme und Untersuchung von Körperzellen und die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren greift in das Recht auf informationelle Selbstbestimmung ein.

Nach der geltenden Rechtslage ist ein solcher Eingriff nur bei Straftaten von erheblicher Bedeutung oder bei Straftaten gegen die sexuelle Selbstbestimmung zulässig. Darüber hinaus ist in jedem Einzelfall eine begründete Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen die Betroffene oder den Betroffenen künftig erneut Strafverfahren wegen des Verdachts derartiger Straftaten zu führen sein könnten. Die Entscheidung über die Untersuchung von Körperzellen ist stets einer **richterlichen Entscheidung** vorbehalten.

Allerdings mehren sich die Stimmen, die sich für eine Absenkung der rechtlichen Schranken für die Entnahme und Untersuchung von Körperzellen und die Speicherung der gewonnenen DNA-Identifizierungsmuster einsetzen. So hat leider auch der nordrhein-westfälische Innenminister gefordert, der Polizei die Möglichkeit einzuräumen, bei allen Tatverdächtigen, die erkennungsdienstlich behandelt werden, auch eine DNA-Analyse vornehmen zu lassen. Eine solche Gleichstellung des so genannten „genetischen Fingerabdrucks" mit den routinemäßigen erkennungsdienstlichen Behandlungen von Beschuldigten (beispielsweise der Abnahme von Fingerabdrücken oder der Aufnahme von Lichtbildern) verkennt die besonderen Gefahren, die von einer undifferenzierten Durchführung von DNA-Analysen ausgehen. Selbst wenn die Untersuchung entnommener Körperzellen auf die nichtcodierenden Teile beschränkt bleibt, können theoretisch auch schon daraus Zuatzinformationen zur Persönlichkeit der Betroffenen gewonnen werden. Zudem ist technisch immer auch eine Untersuchung des codierenden Materials denkbar, die wesentlich tiefere Erkenntnisse über die Betroffenen ermöglicht. Schon dieses besonders **hohe abstrakte Gefährdungspotential** hebt die DNA-Analyse von einem herkömmlichen Fingerabdruck ab und verbietet ihren Einsatz als routinemäßige polizeiliche Maßnahme. Zudem haben es die Betroffenen nicht in der Hand, an welchen Orten genetische Spuren zurückgelassen werden, etwa in Form von Haaren oder kleinen

Hautpartikeln. In weitaus höherem Maß als bei Fingerabdrücken besteht deshalb die Gefahr, dass genetisches Material einer Nichttäterin oder eines Nichttäters – zufällig oder bewusst – an Tatorten, beispielsweise durch eine nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation, platziert wird.

Die Datenschutzbeauftragen des Bundes und der Länder fordern deshalb in ihrer Entschließung vom 16. Juli 2003 (Abdruck im Anhang, Nr. 10), dass die DNA-Analyse nicht zu einem alltäglichen Routinewerkzeug jeder erkennungsdienstlichen Behandlung werden darf und an dem bestehenden Vorbehalt einer richterlichen Anordnung für die Untersuchung von Körperzellen festgehalten wird.

9.3 Telefonverbindungsdaten ohne richterliche Anordnung – die Spitze eines Eisbergs?

Anlässlich eines strafrechtlichen Ermittlungsverfahrens gegen einen Journalisten verlangte die Staatsanwaltschaft ohne richterliche Anordnung von einem Ministerium die Herausgabe von Telefondaten. Für einen bestimmten Zeitraum sollte vorgelegt werden, mit welchen Personen die dort Beschäftigten wann telefoniert hatten.

Zunächst wurde pauschal um die Übermittlung derjenigen gespeicherten Telekommunikationsverbindungsdaten gebeten, die in einer bestimmten Kalenderwoche angefallen waren. Dieses Ansinnen wurde nach kontroversem Schriftwechsel auf die dienstlich geführten Gespräche beschränkt. Eine **gesetzliche Grundlage** dafür gibt es jedoch **nicht** – weder für die eine noch für die andere Maßnahme.

In öffentlichen Stellen ist es gängige Praxis, die Nutzung der Telefone nicht nur für dienstliche Gespräche, sondern ebenfalls für **Privatgespräche** zu gestatten. Privatgespräche müssen aber auch privat bezahlt werden. Um eine korrekte Abrechnung zu ermöglichen, werden die Privatgespräche nach Dauer und Kosten erfasst. Dabei wird auch die angewählte Rufnummer gespeichert, allerdings in aller Regel verkürzt um die letzten zwei oder drei Ziffern. Damit wird dem Schutz des Fernmeldegeheimnisses der Beschäftigten Rechnung getragen, ihnen aber auch zugleich ermöglicht, nachzuvollziehen, ob sie die betreffenden Gespräche tatsächlich geführt haben. Werden in öffentlichen Stellen Telekommunikationsanlagen nicht nur für die ausschließlich dienstliche, sondern auch für die private Nutzung zur Verfügung gestellt, so wird der Dienstherr im Bereich der erlaubten Privatnutzung im

Verhältnis zu den Beschäftigten als insoweit Dritten zum geschäftsmäßigen Telekommunikationsanbieter im Sinne des Telekommunikationsgesetzes (TKG) und hat entsprechend den Bestimmungen des TKG den **Schutz des Fernmeldegeheimnisses** zu wahren. Die hier vertretene Auffassung, dass grundsätzlich nicht einmal der Dienstherr Kenntnis vom Inhalt und von den sonstigen Umständen der privaten Telefonate nehmen darf, zu denen eben auch die Verbindungsdaten gehören, ist in Literatur und Rechtsprechung – soweit ersichtlich – unstreitig. Will eine Strafverfolgungsbehörde Verbindungsdaten der dem grundrechtlich geschützten Fernmeldegeheimnis unterliegenden Telekommunikation bekommen, so benötigt sie dafür nach der Strafprozessordnung grundsätzlich eine richterliche Anordnung. Um so erstaunlicher war das ursprüngliche Ansinnen der Staatsanwaltschaft.

Im Bereich der **dienstlich** geführten Telefonate ist – ebenso unstreitig – der Dienstherr im Verhältnis zu seinen Beschäftigten **kein Telekommunikationsanbieter**, weil die Beschäftigten ihm gegenüber keine Dritten im Sinne des TKG sind (zu den insoweit vergleichbaren Fragen von dienstlicher und privater Nutzung von E-Mail am Arbeitsplatz siehe schon im 15. Datenschutzbericht 2001 unter 2.1.4.1, S. 20 f. und im 16. Datenschutzbericht 2003 unter 9.1, S. 99 ff.). Im Dienstverhältnis gibt es – allerdings allein und ausschließlich gegenüber dem Dienstherrn – für die Beschäftigten keinen Schutz ihrer dienstlichen Telefonate durch das Fernmeldegeheimnis, wohl aber in einem demgegenüber eingeschränkten Umfang durch ihr Allgemeines Persönlichkeitsrecht.

Was aus der Perspektive der Beschäftigten gegenüber dem Dienstherrn gilt, kann allerdings nicht ohne weiteres auf diejenigen Personen übertragen werden, die am anderen Ende der Leitung mit einer oder einem Beschäftigten telefonieren. Da das Fernmeldegeheimnis sachlich einen **Kommunikationsvorgang** schützt, schützt es personell somit **alle** daran **Beteiligten**. In der Literatur wird daher mit beachtlichen Argumenten darum gestritten, ob Dienstgespräche nicht auch generell gegenüber dem Dienstherrn grundsätzlich den Schutz des Fernmeldegeheimnisses genießen. Die Stimmen, die dies befürworten, mehren sich. Doch diese Auseinandersetzung kann hier vernachlässigt werden, denn es wird in Literatur und Rechtsprechung nicht ernsthaft bestritten, dass jedenfalls gegenüber anderen staatlichen Stellen und insbesondere gegenüber der Staatsanwaltschaft jedes Telefonat dem grundrechtlichen Schutz des Fernmeldegeheimnisses unterfällt.

Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts schützt das Fernmeldegeheimnis aus Art. 10 Abs. 1 Grundgesetz (GG) jegliche

Telekommunikation unabhängig von ihrem Inhalt. Davon erfasst sind alle Kommunikationsvorgänge, die sich der Telekommunikationstechnik unter Nutzung einer entsprechenden Anlage bedienen. Art. 10 Abs. 1 GG begründet unter anderem ein **Abwehrrecht gegen** die Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch **den Staat**. Das Gericht sei zitiert: „Der Grundrechtsschutz bezieht sich historisch und aktuell vor allem auf die staatlichen Sicherheitsbehörden" (BVerfGE 85, 386/396).

Will sich eine staatliche Sicherheitsbehörde ohne Zustimmung der Beteiligten Kenntnis von Telefongesprächen oder von Telekommunikationsverbindungsdaten verschaffen, so bedarf es für diesen Grundrechtseingriff einer **speziellen Rechtfertigungsnorm**. Die Eingriffsintensität und das grundrechtliche Gewicht der Unverletzlichkeit des Fernmeldegeheimnisses sind unter anderem die Gründe für die Notwendigkeit spezifischer, normenklarer und insbesondere verhältnismäßiger Regelungen für derartige Grundrechtseingriffe.

Die Strafprozessordnung (StPO) enthält insoweit für die Staatsanwaltschaft **spezielle Befugnisnormen**. Die Auskunft über Telekommunikationsverbindungsdaten ist in den §§ 100g, 100h StPO bereichsspezifisch geregelt und an eine erhöhte Verdachtsschwelle, eine besondere Schwere der Straftat sowie an eine Subsidiaritätsklausel geknüpft und – mit der Ausnahme von Eilfällen – unter den Vorbehalt einer richterlichen Anordnung der Maßnahme gestellt. Liegen diese besonderen Voraussetzungen für den Eingriff in das Fernmeldegeheimnis nicht vor, ist nach einhelliger Auffassung in Literatur und Rechtsprechung ein Rückgriff auf die allgemeine Ermittlungsgeneralklausel aus der StPO ausgeschlossen. Maßnahmen, die gesetzlich gesondert geregelt worden sind, können dann, wenn ihre jeweiligen Voraussetzungen nicht gegeben sind, nicht ersatzweise einfach auf die sehr viel weiter gefasste Ermittlungsgeneralklausel gestützt werden. Die strengen Voraussetzungen für bestimmte Ermittlungshandlungen sind vom Gesetzgeber absichtlich vorgesehen worden und können nicht durch ein beliebiges **„Befugnis-hopping"** durch die Staatsanwaltschaft unterlaufen werden. Auch, und gerade dann, wenn es der Sache nach um eine Maßnahme geht, die in ihrer Eingriffsintensität den gesetzlich besonders geregelten Maßnahmen vergleichbar ist, ist die Durchführung einer solchen Maßnahme dann unzulässig, wenn es an einer speziellen Eingriffsermächtigung fehlt. Anderenfalls würden die bereichsspezifischen Eingriffsregelungen ihre grund-

rechtsschützende Wirkung verlieren. Der grundrechtliche Schutzbereich kann aber nicht den jeweiligen Eingriffsnotwendigkeiten angepasst werden.

Auf den konkreten Fall bezogen bedeutet dies mit anderen Worten: Um die Verbindungsdaten bekommen zu können, hätte die Staatsanwaltschaft – bei Vorliegen der besonderen gesetzlichen Voraussetzungen – eine richterliche Anordnung erwirken müssen. Dies ist nicht geschehen. Wenn also die speziellen Voraussetzungen für die Datenherausgabe nicht vorgelegen haben, hätte die Staatsanwaltschaft ihre Forderung nach Herausgabe der Daten nicht stellen dürfen. Eine Berufung auf die Ermittlungsgeneralklausel ist dafür jedenfalls rechtlich nicht möglich. Damit war das Herausgabeverlangen der Staatsanwaltschaft **unzulässig**.

Die Position der Staatsanwaltschaft, die ihr Vorgehen leider mit Rückendeckung des Justizministeriums für völlig unproblematisch hält, führt – zugespitzt formuliert – in letzter Konsequenz dazu, dass nicht einmal mehr das **Abhören** von dienstlichen Telefonaten noch an die dafür normierten, speziellen strafprozessualen Voraussetzungen und die dafür vorgesehene richterliche Anordnung gebunden wäre. Wenn die spezialgesetzlichen Voraussetzungen nicht gegeben sind, würde dann eben zur Legitimation jeder Ermittlungshandlung gleich welcher grundrechtlichen Eingriffsintensität unzulässigerweise auf die Generalklausel zurückgegriffen werden können. Eine solche Entwicklung darf es nicht geben!

Um zu vermeiden, dass aus einem Einzelfall die Spitze eines Eisbergs mit Folgen auch in ganz anderen Bereichen wird, ist an das Justizministerium die dringliche Bitte zu richten, seine Rechtsauffassung zu revidieren und die Staatsanwaltschaften entsprechend zu informieren.

9.4 Auswertung von Patientenakten durch geschädigte Krankenkassen bei Betrugsvorwurf

Zur Aufklärung von Betrugsvorwürfen gegen einen privaten Pflegedienst hatte eine Staatsanwaltschaft angeordnet, sämtliche Abrechnungsunterlagen mit Patientendaten den betroffenen Krankenkassen zuzuleiten, damit diese als „Sachverständige" die Unterlagen auswerten konnten.

Es bestand der Verdacht, dass Pflegeleistungen bewusst fehlerhaft abgerecht worden waren. Der private Pflegedienst, gegen den ermittelt wurde, ist über diese Maßnahme nicht informiert worden. Ebenso wenig wurden Schweige-

pflichtentbindungserklärungen der betroffenen Patientinnen und Patienten eingeholt.

Die zuständige Staatsanwaltschaft vertrat die Ansicht, dass die geschädigten Krankenkassen als externe **Sachverständige** im Sinne der §§ 72 ff. StPO zulässigerweise in die Ermittlungen einbezogen worden seien, um ihr Erfahrungswissen im Auftrag der Staatsanwaltschaft zu vermitteln. Diese Auffassung ist mehr als problematisch, da die Geschädigten auf diese Weise in eigener Sache den Gang der Ermittlungen beeinflussen konnten.

An dem Vorgehen der Staatsanwaltschaft war zunächst zu kritisieren, dass den Krankenkassen die **gesamten Patientenakten** ohne Vorauswahl übersandt wurden. Hier hätte es einer vorherigen Prüfung bedurft, welche Teile der Patientenakten – etwa hinsichtlich bestimmter verdächtiger Abrechnungszeiträume – den Krankenkassen für die angestrebte Prüfung zwingend zur Verfügung zu stellen waren. Auch wäre es erforderlich gewesen, die Krankenkassen schriftlich darauf hinzuweisen, dass eine eigenständige Nutzung der zur Verfügung gestellten Daten – etwa zur Vorbereitung einer zivilrechtlichen Schadensersatzklage – nicht erfolgen dürfe und das Ergebnis der Überprüfung ausschließlich der auftraggebenden Staatsanwaltschaft zu berichten war. Mündliche Hinweise reichen insoweit nicht aus. Die Krankenkassen hatten hier lediglich einen allgemeinen Hinweis auf die notwendige Wahrung des Schutzes der persönlichen Daten der Patientinnen und Patienten erhalten.

Berechtigte Regressansprüche gegen eine vermeintliche Schädigerin beziehungsweise einen vermeintlichen Schädiger sollen hierbei natürlich nicht ausgeschlossen werden: Den Geschädigten ist es unbenommen, Hinweisen auf unkorrekte Abrechnungen, die in einer strafgerichtlichen Hauptverhandlung öffentlich bekannt werden, im Wege einer Einsicht in die Ermittlungsakten – die freilich separat zu beantragen wäre – nachzugehen. Sachverständige dürfen jedoch personenbezogene Daten, die sie aus der Durchführung ihrer **Sachverständigentätigkeit** zur Kenntnis erhalten, nicht für anderweitige Zwecke nutzen, insbesondere nicht für die Verfolgung eigener Rechtsansprüche.

Die verantwortliche Staatsanwaltschaft hat zugesichert, in künftigen Fällen die mit der Auswertung von Unterlagen betrauten Sachverständigen schriftlich auf diese Anforderungen hinzuweisen und vor der Überlassung der Unterlagen an die Gutachter selbst eine Vorauswahl zu treffen, welche Dokumente für die Begutachtung tatsächlich erforderlich sind.

9.5 Mitteilungen aus Zwangsversteigerungs- und Insolvenzverfahren im Internet durch Justizbehörden – ungewollte Publizitätswirkung?

Immer häufiger nutzen die Justizbehörden für die Veröffentlichung von amtlichen Mitteilungen in Zwangsversteigerungs- und Insolvenzverfahren auch das Internet. Dies bietet zwar neue Möglichkeiten, schafft aber auch erhebliche Risiken. Das zeigt sich insbesondere bei einer öffentlichen Bekanntmachung der schlechten wirtschaftlichen Situation von Bürgerinnen und Bürgern, die von einer Zwangsversteigerung oder Insolvenz betroffen sind.

Die öffentliche Bekanntgabe von **Zwangsversteigerungsdaten** soll einen möglichst großen Interessentenkreis potentieller Erwerberinnen und Erwerber ansprechen, um eine optimale wirtschaftliche Verwertung des zu versteigernden Objekts zu erzielen. Mit der Veröffentlichung von **Insolvenzdaten** im Internet wird potenziellen Gläubigerinnen und Gläubigern die Möglichkeit der raschen Information gegeben, damit sie ihre Forderungen rechtzeitig bei der Insolvenzverwaltung anmelden können – oder aber auch um interessierte Kreise vor insolventen Personen zu warnen.

Zwangsversteigerungsdaten von natürlichen Personen fallen unter das Datenschutzrecht, und zwar auch dann, wenn nicht der Name der Eigentümerin oder des Eigentümers, sondern nur die Anschrift der zu versteigernden Immobilie angegeben wird. Für die Bestimmbarkeit einer Person ist es hierbei ausreichend, wenn eine Interessentin oder ein Interessent durch die Bekanntgabe des Grundstücks und weitere Zusatzinformationen den Namen der Schuldnerin oder des Schuldners herausfinden kann. Eine Veröffentlichung bedarf daher einer gesetzlichen Grundlage oder der Einwilligung der Betroffenen.

Nach § 40 Abs. 2 Zwangsversteigungsgesetz (ZVG) kann die **Bekanntgabe** der **Zwangsversteigerungstermine** – zu der die genauere Bezeichnung des Grundstücks gehört – auch auf andere Weise als durch Anheftung an die Gerichtstafel veröffentlicht werden. Auch wenn es zur Klarstellung wünschenswert wäre, dass der Gesetzgeber für eine Veröffentlichung personenbezogener oder personenbeziehbarer Daten im Internet eine ausdrückliche gesetzliche Regelung schafft, dürfte die entsprechende Internetpräsenz der Justizverwaltung NRW (www.ZVG.nrw.de) mit dem Gesetz noch vereinbar sein.

Eine ausdrückliche Regelung für die Internet-Veröffentlichung von Schuldnerdaten durch die Justiz hat der Gesetzgeber nur für den Bereich der **Insolvenzdaten** in der Insolvenzordnung (InsO) geschaffen: Hier wird das Bundesjustizministerium ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten der Veröffentlichung im Internet zu regeln. Dabei sind insbesondere Löschungsfristen vorzusehen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen

1. unversehrt, vollständig und aktuell bleiben,
2. jederzeit ihrem Ursprung nach zugeordnet werden können und
3. nach dem Stand der Technik durch Dritte nicht kopiert werden können.

Bislang beteiligen sich 14 Bundesländer an der durch Nordrhein-Westfalen redaktionell verantworteten Internet-Präsenz der Insolvenzgerichte (www.insolvenzbekanntmachungen.de).

In der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet wird neben einzelnen Vorschriften zur Datensicherheit und zu Löschungsfristen bestimmt, dass die jeweilige Landesjustizverwaltung Insolvenzdaten im Internet nur veröffentlichen darf, wenn durch geeignete technische und organisatorische Maßnahmen zumindest ein gewisser **Kopierschutz** gewährleistet ist. Hieran fehlt es bislang: Ein Kopierschutz konnte technisch noch nicht realisiert werden; mit einem einfachen Trick können die Daten nach wie vor von den im Internet veröffentlichten Gerichtsbekanntmachungen herauskopiert und beispielsweise für private Listen genutzt werden. Die Anforderungen des Gesetzes und der Verordnung laufen diesbezüglich also zur Zeit leer.

Es ist daher durch informationstechnische Maßnahmen dafür zu sorgen, dass die durch die Justizverwaltung veröffentlichten Insolvenzdaten entweder gar nicht oder nur unter erschwerten Bedingungen im Internet kopiert werden können. Andernfalls wird die Veröffentlichung in der jetzigen Form einzustellen sein.

9.6 Offene Kontodaten und Namenslisten von Gefangenen

Datenschutz gilt auch in Justizvollzugsanstalten – dieser Grundsatz gab den Anlass, auf zwei problematische Verfahrensweisen beim Umgang der Justizvollzugsbehörden mit Gefangenendaten hinzuweisen.

Gegenstand einer Beschwerde war die Übermittlung von **Namenslisten der Gefangenen** an einen anstaltsfremden Friseur, der in der JVA Friseurleistungen erbringt. Hier war die Praxis zu kritisieren, dass Gefangene bei dem Friseur ihren Namen und Ihre Zellennummer in eine Liste eintragen und unterschreiben mussten, um die erhaltenen Friseurleistungen zu quittieren. Um diese Datenübermittlung an eine externe Person zu verhindern, hat die Justizverwaltung veranlasst, dass die Gefangenen nunmehr den Haarschnitt in einer Vormerkliste durch Unterschrift bestätigen, die nicht beim anstaltsfremden Friseur, sondern beim jeweiligen Abteilungsbeamten ausliegt.

Ein weiteres Problem betraf die offene Überbringung von **Kontoauszügen** aus Einzahlungsbelegen der Inhaftierten **ohne verschlossenen Umschlag** durch Beschäftigte des Vollzugsdienstes. Die Beschäftigten der Vollzugsabteilung konnten so den Kontostand der Gefangenen erfahren. Zwar hat die Justizverwaltung die Ansicht vertreten, die Kenntnisnahme sei erforderlich, um etwa Anträge der Gefangenen auf Beschaffung von Gegenständen oder auf Durchführung von Telefongesprächen in Anbetracht ihrer finanziellen Situation sachgerecht beurteilen zu können. Jedoch ist diese Praxis mit datenschutzrechtlichen Anforderungen nicht vereinbar, da eine gesetzliche Grundlage für die Kenntnisnahme sämtlicher den Gefangenen ausgehändigten Kontoauszüge nicht vorhanden ist. Die Beschäftigten der Vollzugsabteilung dürfen sich hiervon nur zur Erfüllung der ihnen obliegenden Aufgaben Kenntnis verschaffen. Die Kenntnis des Kontostandes ist daher nur dann zulässig, wenn die Beschäftigten diese Daten zur Aufgabenerfüllung benötigen, beispielsweise zur Bearbeitung von Anträgen der Gefangenen. Da die Antragsbearbeitung in der Regel wohl nicht von den Beschäftigten des allgemeinen Vollzugsdienst, sondern durch die Verwaltungsabteilung erfolgt, ist die Übermittlung von Kontoauszügen in offenen Umschlägen regelmäßig unzulässig.

Werden die Kontodaten der Gefangenen elektronisch verarbeitet, muss zudem durch eine differenzierte Vergabe von **Zugriffsberechtigungen** sichergestellt sein, dass ein Zugriff sämtlicher Beschäftigter auf die Kontodaten der Gefangenen – etwa mittels Online-Abruf – ausgeschlossen ist. Eine pauschale Zugriffsberechtigung auf Gefangenendaten würde gegen den Grundsatz der Erforderlichkeit verstoßen.

Um zu gewährleisten, dass tatsächlich nur solche Beschäftigte von Kontodaten Kenntnis erhalten, die diese für ihre Aufgabenerfüllung unmittelbar benötigen, wäre die Erarbeitung entsprechender

Verwaltungsvorschriften oder eine Überarbeitung der bestehenden Vollzugsgeschäftsordnung (VGO) sinnvoll. Das Justizministerium NRW hat zugesagt, sich für die Formulierung datenschutzkonformer Regelungen einzusetzen.

10 Soziales

10.1 Das Sozialgeheimnis wahren

Häufiges Anliegen von Bürgerinnen und Bürgern, die Sozialleistungen beantragen, ist immer noch die Frage nach der Zulässigkeit der Anforderung von Kontoauszügen durch Sozialämter als Nachweis der ihnen zur Verfügung stehenden Geldmittel (14. Datenschutzbericht 1999 unter 7.1, S. 99/100). Da in **Kontoauszügen** außer Informationen zu Geldzuflüssen auch solche zu Abbuchungen, also gegebenenfalls zum Ausgabeverhalten der Betroffenen, enthalten sind, müssen diese in der Regel für die Aufgabenerledigung des Sozialamts nicht erforderlichen Angaben durch geeignete Maßnahmen von der Datenerhebung ausgeschlossen bleiben. Dies gilt in gleicher Weise für Nachweise in anderen Leistungsbereichen. Enthält eine Beweisunterlage außer den von einem Sozialleistungsträger erbetenen Informationen auch solche Angaben, die für die Aufgabenerfüllung der Stelle nicht zwingend erforderlich sind, und wünscht die betroffene Person nicht, dass die Stelle hiervon Kenntnis erhält, so kann dieser Konflikt in der Regel durch **Schwärzung** der entsprechenden Angaben gelöst werden.

Ebenso ist der Umfang der Datenerhebung und -speicherung in Akten bei **Hausbesuchen** durch Bedienstete der Sozialämter auf das für die Entscheidung über einen konkreten Antrag der betroffenen Personen zwingend notwendige Maß zu beschränken. Eine Datenerhebung auf Vorrat, etwa um sich ein allgemeines Bild über die Lebenssituation der betroffenen Person machen zu können, ist nicht erforderlich und damit unzulässig. Zudem sind Betroffene vor dem gewünschten Zutritt zur Wohnung durch die Beschäftigten des Sozialamts zu belehren, dass sie den Eintritt in die Wohnung verwehren können und welche Folgen dies für die Leistungsbewilligung haben kann.

Bereits im Jahre 1988 hatte der Kultusminister des Landes Nordrhein-Westfalen in einem Erlass die Notwendigkeit herausgestellt, dass durch geeignete Maßnahmen die Wahrung des Sozialgeheimnisses auch im Bereich der Schulwanderungen und **Klassenfahrten** sicherzustellen ist. Dennoch bestanden Sozialämter in einigen Fällen darauf, Zuschüsse zu Klassenfahrten nicht an betroffene Eltern der Kinder auszuzahlen, sondern ohne deren Einwilligung direkt von der Stadtkasse auf das Konto der begleitenden Lehrperson oder der Schule. Auf diese Weise hätten die Lehrkräfte oder die Schulen rechtswidrig vom Sozialhilfebezug der

Betroffenen Kenntnis erhalten können. Eine solche Offenbarung würde grundsätzlich vermieden, wenn der nachgewiesene Betrag den Eltern zur Verfügung gestellt wird zur Weiterleitung auf das andere Empfängerkonto. Ausnahmen hiervon sind allenfalls dann vertretbar, wenn konkrete Anhaltspunkte aus der Vergangenheit für eine zweckwidrige Verwendung ausgezahlter Sozialhilfeleistungen durch die Eltern vorliegen.

Die Verpflichtung zur Wahrung des Sozialgeheimnisses gebietet es im Übrigen, auch bei **Vorsprachen von Hilfesuchenden** im Sozialamt grundsätzlich dafür Sorge zu tragen, dass Unbefugte keine Kenntnis über Sozialdaten erlangen. Insofern haben Betroffene grundsätzlich einen Anspruch darauf, dass sowohl andere Besucherinnen und Besucher als auch die für die konkrete Bearbeitung ihrer Angelegenheit nicht zuständigen Beschäftigten Hilfegespräche nicht mithören können oder auf sonstige Weise von den personenbezogenen Daten der Betroffenen Kenntnis erlangen. Hilfesuchende sind beispielsweise nicht verpflichtet – wie von einer Bürgerin vorgetragen –, im Wartebereich eines Sozialamts in Gegenwart Dritter den Beschäftigten des Sozialamts ihre personenbezogenen Daten zuzurufen.

In einem anderen Fall beauftragte ein Kreissozialamt ein privates Unternehmen mit der **Zustellung der Dienstpost** an die Bürgerinnen und Bürger. Das Auftreten und das äußere Erscheinungsbild der teilweise jugendlich wirkenden Zusteller hatten dabei zu Missverständnissen und Irritationen bei den Empfängerinnen und Empfängern der Behördenschreiben geführt, die eine Gefährdung des Brief- und Sozialgeheimnisses befürchteten. Diesen Bedenken konnte Rechnung getragen werden, indem das Unternehmen eine Ausstattung der Mitarbeiterinnen und Mitarbeiter mit einheitlicher Dienstkleidung und mit Namensschildern mit Lichtbild zusagte.

Weitere Informationen zu Fragen des Sozialdatenschutzes können auf der Homepage der Landesbeauftragten für Datenschutz und Informationsfreiheit unter www.ldi.nrw.de abgerufen werden.

10.2 Die Grundsicherung im Alter und bei Erwerbsminderung

Die Grundsicherung im Alter und bei Erwerbsminderung soll vor allem die Hauptursache für verschämte Altersarmut beseitigen, den von den Berechtigten befürchteten Rückgriff des Sozialamtes auf die unterhaltspflichtigen Kinder. Des Weiteren soll erwerbsgeminderten Menschen geholfen werden, in Haushaltsgemeinschaft mit Verwandten

oder Verschwägerten leben zu können und dennoch eine materielle Eigenständigkeit zu erlangen.

Die Grundsicherungsstelle ist ebenso wie die Sozialhilfestelle bei der Kommune angesiedelt. In der Praxis der Sozialämter werden diese beiden Aufgaben daher oftmals nicht voneinander getrennt, sondern von denselben Mitarbeiterinnen und Mitarbeitern wahrgenommen. Dabei wird übersehen, dass der zur Darlegung einer Berechtigung auf Leistungen der Grundsicherung im Alter und bei Erwerbsminderung erforderliche Umfang an Daten geringer ist als bei der Hilfe zum Lebensunterhalt. Der Grundsatz der **Zweckbindung** der Daten wird durch diese Organisation unterlaufen. Antragstellende Personen werden zwar nach ihrer Einwilligung in die Übermittlung erforderlicher Daten vom Sozialamt an die Grundsicherungsstelle gefragt, diese „Übermittlung" hat jedoch tatsächlich schon stattgefunden – und zwar die Übermittlung der vollständigen Sozialhilfeakte, unabhängig von der Frage der Erforderlichkeit.

Eine Vereinigung dieser beiden Aufgaben in den kreisfreien Städten und Landkreisen ist nur in einer Form zulässig, die eine gesetzeskonforme Wahrnehmung der Aufgaben ermöglicht. Da nicht sämtliche in den Sozialhilfeakten enthaltenen Daten zur Aufgabenwahrnehmung der Grundsicherung erforderlich sind, ist eine Übermittlung der **vollständigen Sozialhilfeakten** stets ein Verstoß gegen §§ 67a Abs. 1 Satz 1, 67d Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X). Eine zulässige Organisation innerhalb der kreisfreien Städte und Landkreise verbietet daher die Wahrnehmung beider Aufgaben durch ein und dieselbe Person im Bereich der Sachbearbeitung.

Zur **Vermeidung unnötiger Datenerhebungen** kann die Grundsicherungsstelle Sozialdaten ausnahmsweise statt bei den Betroffenen auch bei der Sozialhilfestelle erheben. Den Betroffenen kann angeboten werden, die erforderlichen und bereits erfassten Sozialhilfedaten zu verwenden. Eine solche Vorgehensweise setzt voraus, dass die Grundsicherungsstelle die erforderlichen Daten gegenüber dem Sozialamt und den Betroffenen im Einzelnen darlegt. Der in der Praxis anzutreffende pauschale Hinweis, „dass zur Bearbeitung dieses Antrages die erforderlichen Daten, ..., verwendet werden können" ist jedoch unzureichend. Auch geht aus der Erklärung nicht hervor, dass es sich lediglich um ein Angebot zur Beschleunigung des Verfahrens handelt und die Gewährung von Leistungen davon nicht abhängig ist.

Ab dem 1. Januar 2005 wird dieses Problem an Bedeutung verlieren, da sich die Zuständigkeit für die Hilfe zum Lebensunterhalt in der Mehrzahl der Fälle von der Sozialhilfestelle auf die nach dem Zweiten Buch Sozialgesetzbuch (SGB II) zu gründende Arbeitsgemeinschaft verlagert. Diese gewährt die Hilfe zum Lebensunterhalt für 15- bis 65jährige, erwerbsfähige Hilfebedürftige als **„Grundsicherung für Arbeitsuchende"** in Form des Arbeitslosengeldes II (Alg II). Leistungen nach dem Sozialhilfegesetz sind daneben ausgeschlossen. Die Aufgabenwahrnehmung der „Grundsicherung für Arbeitsuchende" einerseits und der „Grundsicherung im Alter und bei Erwerbsminderung" andererseits wird daher voraussichtlich nicht mehr durch ein und dieselbe Person erfolgen.

Ebenfalls zum 1. Januar 2005 wird das Grundsicherungsgesetz (GSiG) als **„Grundsicherung im Alter und bei Erwerbsminderung"** in das Zwölfte Buch Sozialgesetzbuch (SGB XII) – „Sozialhilfegesetz" eingegliedert. Im Zuge dieser Eingliederung hat der Gesetzgeber durch die Regelungen in den §§ 45 SGB XII und 109a SGB VI klargestellt, dass es allein Aufgabe des Rentenversicherungsträgers ist, die Voraussetzungen der vollen Erwerbsminderung zu prüfen. Eine Kenntnisnahme oder vorherige Anforderung verschiedener medizinischer Unterlagen der antragstellenden Personen durch den Grundsicherungsträger für eigene Zwecke ist nicht erforderlich und somit unzulässig. Der Träger der Grundsicherung ist im Rahmen der Prüfung von Anträgen grundsätzlich nicht befugt, umfassende ärztliche und psychologische Unterlagen anzufordern, einzusehen und gegebenenfalls weiterzugeben. Insoweit dürfte eine Erklärung der Betroffenen ausreichen, dass die entsprechenden ärztlichen Unterlagen direkt dem zuständigen Rentenversicherungsträger übersandt werden.

Zur Feststellung der vollständigen Erwerbsminderung kommt in der Praxis der Grundsicherungsträger bisher ein Vordruck „Ersuchen nach § 5 Abs. 2 GsiG" zum Einsatz, der zur Beifügung von **Befundberichten** und **ärztlichen Gutachten** auffordert. Gängige Praxis ist bisher auch die Unterzeichnung einer „Erklärung über die Entbindung von der Schweigepflicht".

Die Klarstellung der nur kursorischen Prüfungskompetenz des Trägers der Grundsicherung im Alter und bei Erwerbsminderung lässt für die Zukunft erwarten, dass die Leistungsträger ihre Praxis ändern und sowohl von der Anforderung einer Schweigepflichtentbindungserklärung für den Grundsicherungsträger als auch von der Übersendung medizinischer Befunde und Gutachten an den Grundsicherungsträger absehen.

10.3 Datenverarbeitung durch den Medizinischen Dienst der Krankenversicherung

Der Medizinische Dienst der Krankenversicherung (MDK) ist eine unabhängige öffentliche Stelle, die von den gesetzlichen Krankenversicherungen und Pflegeversicherungen eingeschaltet werden muss, wenn es gilt, bestimmte Lebenssachverhalte in medizinischer Hinsicht zu überprüfen und zu begutachten.

Unter Datenschutzgesichtspunkten ist es eine wesentliche Notwendigkeit im Rahmen der Tätigkeit des MDK, dass den Kranken- und Pflegeversicherungen als Ergebnis nur die medizinischen Informationen zugänglich gemacht werden dürfen, die der Gesetzgeber des Sozialgesetzbuchs ausdrücklich erlaubt hat und die im konkreten Fall jeweils zur **Aufgabenerfüllung erforderlich** sind. Insoweit gibt es unterschiedliche Verfahren und Gutachten. Die datenschutzrechtliche Bewertung im konkreten Einzelfall kann durchaus unterschiedlich ausfallen, wenn es sich beispielsweise um ein sozialmedizinisches Gutachten, um ein Gutachten nach Aktenlage zur Frage einer stationären Verweildauer, ein Gutachten zur Frage der Arbeitsunfähigkeit oder auch um eine gutachterliche Bewertung zu gezielten einzelnen Fragen der Kranken- und/oder Pflegeversicherung handelt.

Wichtig ist insoweit, dass unabhängig von den Besonderheiten des jeweiligen Einzelfalles bestimmte datenschutzrechtliche Grundsätze beachtet werden:

- So haben die begutachtenden Ärztinnen und Ärzte eines MDK darauf zu achten, dass bei der Erstellung der Gutachten oder beim Versand der Gutachten die Kranken- oder Pflegekassen überschießende ärztliche Informationen nicht erhalten und deshalb gegebenenfalls Teile der Gutachten ausgeblendet werden. Soweit das gutachterliche Ergebnis unter Nutzung der EDV an die Krankenkassen übermittelt wird, kommt nur eine knappe, dem Datenschutz genügende Zusammenfassung mit den erforderlichen Angaben über den Befund und das Ergebnis der Begutachtung in Betracht. Insbesondere die ausführliche Anamnese und der dokumentierte Befund sind technisch auszublenden.
- Auch bei Vorprüfungen und im Rahmen von Beratungsgesprächen zwischen MDK und Kranken- oder Pflegekasse ist sicherzustellen, dass für den MDK bestimmte medizinische Unterlagen der behandelnden Ärztinnen und Ärzte, die in einem verschlossenen Umschlag mit dem

Vermerk „Zur Vorlage beim MDK" bei der Kranken- oder Pflegekasse vorliegen, von dieser nicht geöffnet werden.

- Keine datenschutzrechtlichen Bedenken bestehen im Ergebnis dagegen, dass die Krankenkasse als Leistungsträger zur Beschleunigung des Begutachtungsverfahrens schon im Vorfeld bei den behandelnden Ärztinnen und Ärzten für die Begutachtung erforderliche Daten und Unterlagen im verschlossenen Umschlag zur Vorlage beim MDK anfordert. Dabei ist zu berücksichtigen, dass die Frage der Erforderlichkeit der Datenerhebung von dem MDK als verantwortliche datenverarbeitende Stelle im Zweifel selbst zu entscheiden ist.

- Auch soweit die betroffene Kranken- oder Pflegekasse aus Vereinfachungsgründen die Rücksendung der für den MDK bestimmten medizinischen Unterlagen übernimmt, kommt eine Übergabe dieser Unterlagen von den Ärztinnen und Ärzten des MDK an die Kranken- oder Pflegekasse ebenfalls nur im verschlossenen Umschlag in Betracht.

- Auch soweit von der jeweils betroffenen Kranken- oder Pflegekasse eine Einladung zu einer Untersuchung bei einer Ärztin oder einem Arzt des MDK ergeht, muss die Einladung so konzipiert sein, dass einladende Stelle der MDK ist und deshalb auch etwaige Hinderungsgründe, den vorgeschlagenen Termin beim MDK wahrzunehmen, nur diesem gegenüber offenbart werden dürfen. Eine Kranken- oder Pflegekasse ist zur Speicherung dieser Daten nicht befugt.

- Zur Wahrung der Datenschutzrechte der betroffenen Versicherten und um etwaige Datenschutzverstöße im Rahmen der Datenverarbeitung nachvollziehen zu können, ist die Datenerhebung und weitere Datenverarbeitung durch den MDK ausreichend zu dokumentieren. So ist beispielsweise bei Verwertung von Fremdunterlagen in einem Gutachten zweifelsfrei deutlich zu machen, welche Quelle benutzt wurde. Andererseits sind Kurzvermerke in den Unterlagen der Krankenkasse, etwa mit dem allgemein gehaltenen Hinweis „Auf Grund der vorliegenden Unterlagen werde (folgendes) ..... festgestellt", nicht zulässig, weil die Richtigkeit des gefundenen Ergebnisses nicht mehr nachprüfbar ist, da die entscheidende Frage, um welche Unterlagen es sich gehandelt hat, in der Zukunft nicht mehr klärbar sein dürfte.

- Um die Datenerhebung und weitere Datenverarbeitung beim MDK datenschutzkonform abwickeln zu können, ist ein für die

begutachtenden Ärztinnen und Ärzte verbindliches Datenschutz- und Datensicherheitskonzept zu erstellen und in Kraft zu setzen. Um Interessenkollisionen zu vermeiden, sollte dabei auch die Frage von „Nebentätigkeiten" der beim MDK beschäftigten Gutachterinnen und Gutachter bei anderen (privaten) Stellen geregelt sein.

Auf Grund der in der Vergangenheit deutlich gewordenen aufgeschlossenen Haltung des MDK gegenüber den Fragen des Datenschutzes und den Datenschutzbelangen der betroffenen Patientinnen und Patienten ist davon auszugehen, dass bezogen auf den Einzelfall auch in Zukunft eine datenschutzkonforme Lösung aufgetretener Probleme möglich sein dürfte.

10.4 Gutachten für die gesetzliche Unfallversicherung

Immer wieder bringen Betroffene Beschwerden vor, dass ihre Datenschutzrechte von den gesetzlichen Unfallversicherungsträgern im Rahmen der Entscheidungsfindung nur sehr mangelhaft beachtet werden.

Überprüfungen haben in einzelnen Fällen erhebliche Unkenntnisse der handelnden Stellen hinsichtlich der gesetzlich geregelten Erfordernisse des Datenschutzes bei Verfahren nach dem Siebten Buch Sozialgesetzbuch (SGB VII) ergeben.

Allein schon die **Erteilung eines Gutachtenauftrags** war mitunter in rechtswidriger Weise erfolgt und bedeutete daher, dass die gesamte weitere Datenverarbeitung auf der Grundlage des rechtswidrig zustande gekommenen Gutachtens ebenfalls rechtswidrig und damit letztlich unzulässig war. Nach § 200 Abs. 2 SGB VII soll vor Erteilung eines Gutachtenauftrags der Unfallversicherungsträger der versicherten Person mehrere Gutachterinnen oder Gutachter zur Auswahl benennen. Danach ist jedes ärztliche Gutachten eines Unfallversicherungsträgers, das in einem Entschädigungsverfahren Verwendung finden soll, vor Erteilung des Auftrags in der Weise vorzubereiten, dass vor dem Hintergrund des normierten Auswahlrechts der betroffenen Person zwingend Gelegenheit gegeben werden muss, sich zu den vorgeschlagenen Gutachterinnen und Gutachtern zu äußern. Eine Verletzung dieser Vorschrift führt unmittelbar zunächst dazu, dass jede Übermittlung von Daten der betroffenen Person an eine Gutachterin oder einen Gutachter unzulässig ist.

Erst mit ihrer **Auswahlentscheidung** stimmen die Betroffenen zu, dass ihre personenbezogenen Sozialdaten an die begutachtende Person übermittelt werden dürfen. Ein ohne eine solche Mitwirkung formulierter Gutachtenauftrag stellt bereits selbst eine unzulässige Datennutzung durch den Unfallversicherungsträger dar. Die in der Übersendung des Auftragschreibens an die Gutachterin oder den Gutachter liegende Datenübermittlung ist darüber hinaus rechtswidrig und unzulässig.

Ein dennoch etwaig entstandenes Gutachten ist ebenfalls rechtswidrig und kann keine Grundlage für einen Bescheid darstellen. Dies bedeutet allerdings nicht zwingend, dass in jedem Fall auch die Entscheidung des Bescheides geändert werden muss. Lediglich in der Begründung kann auf ein solches Gutachten nicht Bezug genommen werden. Entsprechende Textpassagen sind aus dem Bescheid zu entfernen.

Um allerdings eine Auswahlentscheidung nach § 200 Abs. 2 SGB VII überhaupt treffen zu können, ist es notwendig, dass die Betroffenen Zugang zu den entscheidungsrelevanten Informationen und Daten haben. Dies bedingt, dass der **Gutachtenauftrag** vom Inhalt und Umfang bereits abschließend formuliert ist und den Betroffenen im Rahmen des Auswahlverfahrens vorgestellt wird. Nur so kann gegebenenfalls eine betroffene Person überhaupt überprüfen und entscheiden, welche der vorgeschlagenen Gutachterinnen und Gutachter besser oder weniger geeignet ist, die bestehenden Fragen gutachterlich zu bewerten. Dadurch ist gleichzeitig ausgeschlossen, dass nach Erteilung des Gutachtenauftrags der Unfallversicherungsträger **einseitig** den Gutachtenauftrag **verändert**. Hierzu benötigt er stets die Zustimmung der Betroffenen, da für den (neuen) Sachverhalt, der zusätzlich bewertet werden soll, eine Entscheidung der Betroffenen nach § 200 Abs. 2 SGB VII bisher nicht vorliegt.

Weiter sind beispielsweise alle Informationen über eine Gutachterin oder einen Gutachter wesentlich, die die Frage einer beruflichen Eignung bis hin zu einer möglichen **Befangenheit** berühren. Gutachterinnen und Gutachter, die etwa Beschäftigte einer Klinik desselben gesetzlichen Unfallversicherungsträgers sind, sollten wegen bestehender Interessenkollisionen nicht vorgeschlagen werden; zumindest nicht, ohne dass gleichzeitig auf diesen Sachverhalt einer bestehenden Interessenkollision ausdrücklich gegenüber den jeweils Betroffenen hingewiesen wird.

Werden solche Informationen allerdings unterlassen, werden die Betroffenen über wesentliche Eigenschaften der Gutachterin oder des

Gutachters im Unklaren gelassen und können deshalb ihre zustimmende Erklärung nach § 200 Abs. 2 SGB VII anfechten. Dies hätte zur Folge, dass die Erklärung von Anfang an als unwirksam anzusehen ist und somit die gesamte Datenverarbeitung des Begutachtungsverfahrens **ohne Rechtsgrundlage** erfolgt. Ein unter diesen Bedingungen erstelltes Gutachten müsste aus der Akte des Unfallversicherungsträgers entfernt und vernichtet werden. Dies gilt auch für den gesamten Schriftverkehr mit dieser Gutachterin oder diesem Gutachter.

Schließlich ist noch zu beachten, dass bei Erteilung eines Gutachtenauftrags der Unfallversicherungsträger dafür Sorge zu tragen hat, dass die Gutachterin oder der Gutachter seinerseits keine grundlegenden Datenschutzverstöße begeht, etwa **ohne Zustimmung** der Beteiligten die Erstellung des Gutachtens an Dritte **delegiert** oder auch eine Datenerhebung in ihrer oder seiner Person behauptet, die gar nicht stattgefunden hat.

So beklagte sich beispielsweise ein Betroffener, dass er den beauftragten Professor gar nicht gesehen habe, der Professor seinerseits jedoch im Gutachtentext die Erklärung abgab, er habe den Betroffenen gründlich untersucht und alle für die Begutachtung erforderlichen Angaben bei ihm selbst erhoben. Ein auf eine solche **mangelhafte Datenerhebung** aufgebautes Gutachten ist unbrauchbar für die Entscheidungsfindung des Unfallversicherungsträgers. Ein solches Gutachten ist in der Akte des Unfallversicherungsträgers zu sperren und nur noch zur Aufarbeitung dieses fehlerhaften Verhaltens der beteiligten Personen und Stellen zu verwenden, etwa im Rahmen eines Zivilprozesses wegen Schadensersatz, eines Strafprozesses wegen Betruges oder ähnlicher Rechtsverfolgung durch die betroffene Person.

Im Übrigen legt die Formulierung in § 200 Abs. 2 SGB VII „dem Versicherten mehrere Gutachter zur Auswahl benennen" zwar den Schluss nahe, dass Betroffene auch **wiederholt** die Vorschläge **ablehnen** können, bis schließlich irgendwann Übereinstimmung über eine vorgeschlagene Gutachterin oder einen Gutachter gefunden ist. Eine solche Vorgehensweise dürfte allerdings weder der gesetzlichen Mitwirkungspflicht der Betroffenen noch dem übergeordneten Gesichtspunkt der beschleunigten Durchführung des Verwaltungsverfahrens entsprechen.

Deshalb ist davon auszugehen, dass Betroffene sich im Rahmen von § 200 Abs. 2 SGB VII nicht auf eine schlichte Ablehnung des Vorschlags des Unfallversicherungsträgers beschränken dürfen. Vielmehr haben sie

ihrerseits dem Unfallversicherungsträger **Vorschläge** hinsichtlich der begutachtenden Person zu unterbreiten. Soweit danach keine Bedenken hinsichtlich Qualifikation, Befangenheit oder anderer Gesichtspunkte bestehen, dürfte in der Regel einem solchen Vorschlag zu folgen sein. Ziel der gemeinsamen Suche nach § 200 Abs. 2 SGB VII sollte die Erlangung einer **überparteilichen unabhängigen Begutachtung** sein. Deshalb erscheint es auch notwendig, dass, falls der Unfallversicherungsträger den Vorschlag der betroffenen Person hinsichtlich einer Gutachterin oder eines Gutachters ablehnen möchte, dies nur mit einer schlüssigen Begründung erfolgen kann. Diese Begründung sollte für das gegebenenfalls folgende Gerichtsverfahren entsprechend dokumentiert werden.

Von der Begutachtung nach § 200 Abs. 2 SGB VII ist der Datenverarbeitungsvorgang zu trennen, der mit der Einschaltung einer **„beratenden Ärztin"** oder eines **„beratenden Arztes"** durch einen Unfallversicherungsträger verbunden ist. Da die Sachbearbeiterinnen und Sachbearbeiter beim jeweiligen Unfallversicherungsträger in der Regel medizinische Laien sein dürften, liegt es nahe, dass diese Beschäftigten sich im Rahmen der Sachbearbeitung von „beratenden Ärztinnen und Ärzten" die unter Beachtung von § 200 Abs. 2 SGB VII erstellten Gutachten gegebenenfalls im Einzelnen erläutern lassen und mit diesen „beratenden Ärztinnen und Ärzten" die Möglichkeit des weiteren Vorgehens im konkreten Verfahren erörtern. Im **Unterschied** zum Gutachten nach § 200 Abs. 2 SGB VII wird von der weiteren „beratenden" Stimme keine Neutralität verlangt. Sie ist auch nicht erwünscht, da ja das neutral gehaltene Gutachten nach § 200 Abs. 2 SGB VII allein unter dem Blickwinkel der Interessen des Unfallversicherungsträgers überprüft und bewertet werden soll. Letztlich sollen die „beratenden Ärztinnen und Ärzte" nur die Funktion übernehmen, die Ärztinnen und Ärzte hätten, die beim Unfallversicherungsträger fest angestellt wären. Gesichtspunkte der Befangenheit der eine solche Bewertung vornehmenden Person spielen, da es sich um eine Würdigung des Sachverhalts im Interesse des Unfallversicherungsträgers handelt, auch keine Rolle. Eine Einflussnahme des Unfallversicherungsträgers bis hin zu den einzelnen Formulierungen in der gutachterlichen Stellungnahme ist gewollt und beabsichtigt. Solche Stellungnahmen sollten mit dem Hinweis gekennzeichnet werden, dass es sich dabei gerade nicht um ein Gutachten nach § 200 Abs. 2 SGB VII handelt.

Es wäre zu begrüßen, wenn die Verbände der Unfallversicherungsträger sich Transparenz- und Datenschutzleitlinien geben würden, bei deren Berücksichtigung Datenschutzprobleme dann erst gar nicht entstehen dürften.

10.5 Seniorenheime

Immer wieder lässt sich eine Diskrepanz feststellen zwischen dem Anspruch von Pflegeheimen, die Würde und die freie Entfaltung der Persönlichkeit ihrer Bewohnerinnen und Bewohner zu wahren, und der Art und Weise, wie deren personenbezogene Daten erhoben und weiterverarbeitet werden.

Beispielsweise wurden Bewohnerinnen und Bewohner ohne jeden Hinweis auf den Zweck (Planung der Tagesgestaltung) und die Freiwilligkeit einer Mitwirkung aufgefordert, sensible Angaben zu ihrem familiären Hintergrund, ihrer Weltanschauung sowie ihrer sozialen und kulturellen Herkunft zu machen. Die Abfrage umfasste Erlebnisse des Verlustes, der Trennung, des Schmerzes und der Liebe sowie private Wünsche.

Jede Datenerhebung setzt eine umfassende Aufklärung der Betroffenen über die verantwortliche Stelle, über den Zweck und die Erforderlichkeit der Datenerhebung, über die Dauer der Datenspeicherung sowie über die Freiwilligkeit der Angaben voraus.

10.6 Beobachtungsbogen in Kindertagesstätten

Kindertagesstätten wollen zum Zweck einer Qualitätssteigerung ihrer Bildungsarbeit und mit dem weiteren Ziel einer verbesserten Zusammenarbeit mit Grundschulen Beobachtungsbogen einsetzen.

Sowohl Inhalt und Umfang der Beobachtungsbogen als auch die Häufigkeit der Datenerhebungen sowie das sonstige Verfahren bis hin zur Überlassung der ausgefüllten Bogen an dritte Personen und/oder Stellen waren in den verschiedenen **Kindertagesstätten** unterschiedlich. Die datenschutzrechtliche Überprüfung führte durchweg zu dem Ergebnis, dass die Verwendung dieser Bogen zu einem unzulässigen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Kinder und ihrer Personensorgeberechtigten führte. Der Einsatz der Beobachtungsbogen in den Kindertages-

stätten der betroffenen Kommunen wurde daraufhin eingestellt und die Bogen zurückgezogen.

Das seinerzeit zuständige Ministerium für Schule, Jugend und Kinder hat unter Berücksichtigung dieses Prüfergebnisses eine „Vereinbarung zu den Grundsätzen über die Bildungsarbeit der Tageseinrichtungen für Kinder – **Bildungsvereinbarung NRW** –" konzipiert, die im Grundsätzlichen dem Recht auf informationelle Selbstbestimmung der betroffenen Kinder und ihrer Personensorgeberechtigten ausreichend Rechnung trägt. Die Personensorgeberechtigten werden entscheidend in die verschiedenen Phasen der Dokumentation über den Bildungsprozess des einzelnen Kindes mit einbezogen. Wie das jetzt zuständige Gesundheitsministerium weiter mitteilt, sollen Arbeitshilfen für die Erstellung von Dokumentationen über die Beobachtung eines jeden einzelnen Kindes durch die pädagogischen Fachkräfte in den Tageseinrichtungen in einem Projekt bis Ende 2005 entwickelt werden.

Es bleibt zu hoffen, dass es auf diesem Wege gelingt, auch den Inhalt der Dokumentationen im Ergebnis datenschutzkonform zu gestalten.

10.7 „Hartz IV" und der Datenschutz

Am 01.01.2005 ist die Zusammenführung der Sozialhilfe und Arbeitslosenhilfe im Zweiten Buch Sozialgesetzbuch (SGB II) – Grundsicherung für Arbeitsuchende – in Kraft getreten. An deren praktischer Umsetzung bestehen sowohl hinsichtlich der Datenerhebung mit den Antragsvordrucken als auch hinsichtlich der Datenverarbeitung durch die eingesetzte Software erhebliche datenschutzrechtliche Bedenken.

Der Antragsvordruck auf Leistungen zur Sicherung des Lebensunterhaltes erfragt ausführliche Angaben nicht nur zu Einkommens-, Vermögens- und sonstigen Lebensverhältnissen der antragstellenden Person selbst, sondern bezieht auch sämtliche mit ihr in einem Haushalt lebenden Personen ein. Häufige Fragen verunsicherter Betroffener waren: Muss der 60jährige Vater tatsächlich sein Vermögen und Einkommen vollständig offen legen, wenn sein im Haushalt lebender 40jähriger Sohn einen Antrag stellt? Antwort: nein. Können Angaben zur Vermieterin und deren Bankverbindung schon bei Antragstellung erforderlich sein? Antwort: nein. Besteht eine Pflicht zur Angabe der E-Mail-Adresse und Telefonnummer? Antwort: nein. Bestehen Auskunftspflichten über die persönlichen Verhältnisse eines bloßen

Mitbewohners oder einer Untermieterin? Antwort: nein. Auch fehlen klare Hinweise, ohne die angesichts von Fragen zu „sonstigem Vermögen, zum Beispiel Edelmetalle, Antiquitäten, Gemälde" eine vollständige Beantwortung nahezu unmöglich wird: Sollen auch der Ehering und das Stillleben im Esszimmer angegeben werden?

Grundsätzlich ist zur Datenerhebung für das Arbeitslosengeld II anzumerken, dass die verschiedenen Grundsätze, die für die Datenerhebung und Datenverarbeitung bei der Gewährung von Sozialhilfe in Nordrhein-Westfalen gelten, leider nicht übernommen worden sind. Dies gilt auch für Inhalt und Ausgestaltung der vorliegenden Antragsvordrucke der Bundesagentur für Arbeit. An Teilen dieser Vordrucke bestehen erhebliche datenschutzrechtliche Bedenken. Nach Gesprächen zwischen der Bundesagentur für Arbeit und dem Bundesbeauftragten für den Datenschutz, an denen auch die Datenschutzbeauftragten aus Schleswig-Holstein und Nordrhein-Westfalen beteiligt waren, wurde eine entsprechende **Änderung der Formulare** in nicht unwesentlichen Teilen für die Neuauflage 2005 zugesagt.

Insbesondere konnte für die zukünftige Gestaltung der Antragsformulare die Unterscheidung zwischen Mitgliedern der Bedarfsgemeinschaft und den weiteren im Haushalt lebenden Personen erreicht werden. Die jetzige Auflage verlangt noch unterschiedslos umfassende Angaben zum Einkommen und Vermögen aller im Haushalt lebenden Personen, obwohl dieser Personenkreis über den der Bedarfsgemeinschaft hinausgehen kann und nur die Mitglieder der **Bedarfsgemeinschaft** zu derart umfassenden Angaben verpflichtet sind.

Es konnte klargestellt werden, dass sich eine Pflicht zur umfassenden Auskunft über Einkommen und Vermögen der im Haushalt lebenden verwandten oder verschwägerten Personen, die nicht zur Bedarfsgemeinschaft gehören, auch nicht aus der Unterhaltsvermutung des § 9 Abs. 5 SGB II ergibt. Die **Unterhaltsvermutung** kann vielmehr bereits durch gegenteilige Erklärungen der in Haushaltsgemeinschaft lebenden Verwandten oder Verschwägerten **widerlegt werden**.

In der Neuauflage wird auch auf Angaben zur **Vermieterin** oder zum **Vermieter** im Rahmen der Feststellung der angemessenen Kosten für Unterkunft und Heizung verzichtet werden.

In vielen weiteren Punkten sind zwar Verbesserungen in Aussicht gestellt, doch konnten die Bedenken leider nicht vollständig ausgeräumt werden. Sie betreffen beispielsweise folgende Punkte: So besteht die Bundesagentur für

Arbeit hinsichtlich der **Verdienstbescheinigung des Arbeitgebers** unter Berufung auf § 58 Abs. 1 Satz 2 SGB II weiterhin auf der Verwendung ihres nicht neutral gehaltenen Vordruckes. Zur Anerkennung eines Mehrbedarfs für kostenaufwändige Ernährung soll auch die Art der Erkrankung bescheinigt werden, so dass der Sachbearbeitung **Gesundheitsdaten** bekannt werden, wie beispielsweise das Vorliegen einer HIV-Infektion. Des Weiteren geht die Bundesagentur unter Berufung auf die Vertretungsvermutung des § 38 SGB II von einer **informationellen Einheit der Bedarfsgemeinschaft** aus. Durch die Gestaltung der Formulare wird nicht ersichtlich, ob die Mitglieder der Bedarfsgemeinschaft, über die die Antragstellerinnen und Antragsteller umfassende und teilweise sensible Angaben zu machen haben, überhaupt Kenntnis von der Existenz des Antrages und der darin gemachten Angaben haben. Immerhin wird nunmehr seitens der Bundesagentur für Arbeit ausdrücklich darauf hingewiesen, dass jedes Mitglied der Bedarfsgemeinschaft einen eigenen Antrag stellen kann und anderenfalls in das Ausfüllen einbezogen werden soll.

Dieser und weitere Hinweise sind in den nunmehr veröffentlichten **Ausfüllhinweisen der Bundesagentur für Arbeit** zum Antragsvordruck Arbeitslosengeld II enthalten, die im Internet unter www.arbeitsagentur.de abrufbar sind. Mit Hilfe dieser Ausfüllhinweise soll sowohl ein datenschutzkonformes Ausfüllen erreicht als auch Verzögerungen oder Ablehnungen vermieden werden.

Hinsichtlich der **Datenverarbeitungssoftware A2LL**, die in den zuständigen Arbeitsgemeinschaften (ARGE) zur Berechnung der Leistungen zum Einsatz kommen wird, sind immer noch wesentliche Fragen ungeklärt. So mangelt es nach wie vor an einem Zugriffsberechtigungskonzept und einer Protokollierung der Zugriffe. Daher kann jede Sachbearbeiterin und jeder Sachbearbeiter mittels A2LL bundesweit auf die in jeder ARGE und der Bundesagentur für Arbeit gespeicherten Daten zugreifen, ohne dass eine Protokollierung der Zugriffe erfolgt. Bedenklich ist des Weiteren, dass A2LL auch den Zugriff auf die zentrale Personendatenverwaltung (zPDV) der Bundesagentur für Arbeit ermöglicht, mithin die Stammdaten jeder Kundin und jedes Kunden der Bundesagentur abgerufen werden können, unabhängig davon, ob sie oder er auch Leistungen nach dem SGB II erhält oder nicht. Diese **Mängel** wurden durch den Bundesbeauftragten für den Datenschutz **beanstandet**. Eine Abhilfe durch die BA ist jedoch vor April 2005 nicht zu erwarten.

Datenschutzmängel werden aus jetziger Sicht auch weiterhin das Verfahren der Leistungsgewährung nach dem SGB II begleiten; ein für die Betroffenen letztlich unerträglicher Zustand.

11 Gesundheit

11.1 Datenverarbeitung im Gesundheitswesen

Das **Gesundheitsdatenschutzgesetz** Nordrhein-Westfalen (GDSG) vom 22.02.1994, das eine erhebliche Verbesserung des Datenschutzes im Gesundheitswesen mit sich brachte, sollte ursprünglich wieder abgeschafft und einzelne Teile dieses Gesetzes in das bestehende Gesetz über den öffentlichen Gesundheitsdienst Nordrhein-Westfalen (ÖGDG) eingefügt werden. Der Entwurf und die geplante ersatzlose Aufhebung des GDSG begegneten zahlreichen datenschutzrechtlichen Bedenken. Das Vorhaben des Ministeriums wurde aufgegeben.

Im Berichtszeitraum gab es vor allem zur Datenverarbeitung der **Gesundheitsämter** viele Anfragen und Beschwerden. Problematisch ist beispielsweise die Organisationsentscheidung einer Kommune, zur Leitung des Gesundheitsamtes eine Nicht-Medizinerin oder einen Nicht-Mediziner zu bestellen und so eine permanente Datenübermittlung von ärztlichen Mitarbeiterinnen oder Mitarbeitern des Gesundheitsamtes an nicht-ärztliche Vorgesetzte zu implementieren, die nicht im Einklang mit § 203 Strafgesetzbuch – StGB – (Verletzung der ärztlichen Schweigepflicht) stehen dürfte. Die Organisationshoheit einer Kommune umfasst zwar grundsätzlich auch die Kontroll- und Aufsichtsbefugnis. In diesem Rahmen könnte bei Vorliegen bestimmter Voraussetzungen auch die Einsichtnahme der oder des Vorgesetzten in Akten des Gesundheitsamtes, die personenbezogene medizinisch Daten enthalten, erforderlich sein. Diese Akten unterliegen jedoch dem besonderen Schutz der ärztlichen Schweigepflicht. Die **Herausgabe der Akten an Vorgesetzte** ist deshalb nur zulässig, soweit sie zur Erfüllung einer gesetzlichen Pflicht erforderlich ist, eine Rechtsvorschrift sie erlaubt oder die Betroffenen im Einzelfall eingewilligt haben. Grundsätzlich ist die Kenntnisnahme vom Inhalt der Akten des Gesundheitsamtes durch nichtmedizinisches Personal nicht geeignet, die fachliche Kontrolle und Aufsicht hinsichtlich der Behandlung und Untersuchung der Betroffenen auszuüben. Bei anlassbezogenen Beschwerden, aber auch bei allgemeinen Routinekontrollen, die nicht durch die Ärztinnen und Ärzte des Gesundheitsamtes selbst durchgeführt werden können, sind Vorgesetzte daher gehalten, eine externe Ärztin oder einen externen Arzt mit der Begutachtung der entsprechenden Akten zu beauftragen. Die Vorgesetzten dürfen ausschließlich über das Ergebnis der Begutachtung unterrichtet werden.

Durch dieses Vorgehen entsteht keine Kontrolllücke und das Recht der Patientinnen und Patienten auf informationelle Selbstbestimmung ist dennoch ausreichend gewahrt.

Die strenge Verpflichtung zur Wahrung des Arzt-Patienten-Geheimnisses bedingt auch die generelle Pflicht eines jeden Amtes, das mit Gesundheitsdaten in Berührung kommt, zur **Trennung der Aktenführung von medizinischen und nicht-medizinischen Daten**.

Untersuchen Ärztinnen und Ärzte dieselbe Patientin oder denselben Patienten gleichzeitig oder nacheinander aus dem gleichen Anlass, so sind sie untereinander allerdings von der Schweigepflicht befreit. Dies gilt jedoch nur insoweit, als die Kenntnis der Untersuchungsergebnisse der jeweils anderen Ärztinnen und Ärzte für die eigene Untersuchung unabdingbar erforderlich ist. Ansonsten gilt, dass die Ärztinnen und Ärzte des Gesundheitsamtes nur dann Befunde und Gutachten ihrer Patientinnen und Patienten einsehen dürfen, wenn deren **Daten anonymisiert** sind, so dass eine Reidentifizierung verlässlich ausgeschlossen ist.

Den Patientinnen und Patienten ist nach § 9 Abs. 1 GDSG auf Verlangen unentgeltlich **Auskunft** über die im Gesundheitsamt zu ihrer Person gespeicherten Daten sowie über die Personen und Stellen zu erteilen, von denen ihre Daten stammen und an die sie übermittelt wurden. Auf Wunsch ist ihnen Einsicht in die entsprechenden Akten zu gewähren. Das gilt für alle Aufzeichnungen über **objektive physische Befunde** (nachprüfbare Gesundheitstatsachen wie Laborberichte, Röntgenbilder, EKG-Auswertungen) und Berichte über Behandlungsmaßnahmen. Nur soweit eine unverhältnismäßige Beeinträchtigung der Gesundheit der Patientin beziehungsweise des Patienten zu befürchten ist, ist die Ärztin oder der Arzt berechtigt, bestimmte Angaben im Ausnahmefall nicht zugänglich zu machen. **Subjektive Eindrücke** und Aufzeichnungen im Rahmen der Behandlung können nach ärztlichem Ermessen zurückgehalten werden.

Ein Recht auf Auskunft oder Akteneinsicht steht der Patientin oder dem Patienten allerdings nicht zu, soweit **berechtigte** Geheimhaltungsinteressen **Dritter**, deren Daten zusammen mit denen der Patientin beziehungsweise des Patienten aufgezeichnet werden, überwiegen. Ob Geheimhaltungsinteressen Dritter als „berechtigt" anzuerkennen sind, unterliegt der Bewertung und Beurteilung des Gesundheitsamts, dem insoweit ein Beurteilungsspielraum zusteht. Soweit die **Akteneinsicht** gestattet ist, kann die

Patientin oder der Patient Auszüge oder Abschriften selbst fertigen oder sich Ablichtungen gegen Kostenerstattung fertigen lassen.

Die im Gesundheitsamt gespeicherten Patientendaten sind zu **löschen**, wenn ihre Speicherung unzulässig ist, zum Beispiel bei der Speicherung objektiv falscher Daten. Generell sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Davon ist bei patientenbezogenen Daten jedenfalls dann auszugehen, wenn 10 Jahre nach der Aufgabenerfüllung verstrichen sind. Zur ordnungsgemäßen Dokumentation von Verwaltungsverfahren reicht es regelmäßig aus, wenn die Aufzeichnungen **zwei Jahre** nach Abschluss des Verfahrens aufbewahrt werden, es sei denn, es liegen begründete Umstände vor, die eine längere Frist erforderlich machen. Nach Ablauf von zwei Jahren kann im allgemeinen davon ausgegangen werden, dass das Löschungsinteresse der Betroffenen das öffentliche Dokumentationsinteresse überwiegt.

Besondere Umstände für eine längere Aufbewahrungsfrist können beispielsweise in Zukunft zu stellende Leistungsanträge sein, bei denen es notwendig sein kann, wenn die damit im Zusammenhang stehenden früheren Unterlagen noch verfügbar sind. Grundsätzlich bietet sich in einem solchen Fall alternativ zur Datenlöschung eine **Datensperrung** an. Diese Sperrung hat zur Folge, dass die Unterlagen zwar aufbewahrt werden, aber (gesperrt für alle übrigen Verwaltungsvorgänge) nur dann Verwendung finden dürfen, wenn die betroffene Person zuvor in jedem Einzelfall ausdrücklich eingewilligt hat.

In einer Suchthilfestelle haben bei einem Trägerwechsel Personal und Klientel in die Übergabe ihrer Personal- und Patientenakten an den neuen Träger schriftlich einzuwilligen, auch wenn sich an den Arbeits- beziehungsweise Unterbringungsbedingungen sonst nichts verändert. Tritt durch den Trägerwechsel zugleich ein Wechsel in der Kontrolle der Datenverarbeitung auf der Grundlage anderer Datenschutzgesetze ein, ist auch hierauf hinzuweisen.

11.2 Einrichtung eines neuen Krebsregisters

Das Land Nordrhein-Westfalen beabsichtigt, das Modell eines Krebsregisters nach dem Gesundheitsdatenschutzgesetz Nordrhein-Westfalen (GDSG) aufzugeben und ein eigenes Krebsregistergesetz Nordrhein-

Westfalen (KRG) zu schaffen. Damit sollen die Informationsgrundlagen über diese Krankheit ausgeweitet und verbessert werden.

Im Gegensatz zur bisher als Rechtsgrundlage gewählten **Einwilligungslösung** des Gesundheitsdatenschutzgesetzes ist nunmehr im Gesetzentwurf des KRG eine **Verpflichtung** der behandelnden Ärztinnen und Ärzte normiert, jede Patientin und jeden Patienten, die oder der möglicherweise an dieser Krankheit leidet, dem Krebsregister zu melden und die Meldungen bei Erkenntnis- und/oder Behandlungsfortschritt zu wiederholen, zu ergänzen oder zu berichtigen. Selbst bei einer Gesundung werden die Daten nicht gelöscht, sondern sind für den Fall einer Wiederholungs-Erkrankung oder einer Erkrankung an einem anderen Karzinom weiter gespeichert.

Um die Lückenlosigkeit der Erfassung aller in Nordrhein-Westfalen von dieser Krankheit befallenen Personen sicherzustellen, ist die **Meldepflicht** nicht auf die behandelnden Ärztinnen und Ärzte beschränkt, sondern auch auf anderes ärztliches Personal – wie etwa die Labormedizinerinnen und -mediziner – ausgedehnt worden, die Gewebeproben untersuchen. Insoweit werden bewusst „Doppelmeldungen" zu denselben Personen normiert.

Die zu meldenden Daten sollen vor der Aufnahme in das Krebsregister zuverlässig **pseudonymisiert** werden. Das bedeutet, dass die Mitarbeiterinnen und Mitarbeiter und die Nutzerinnen und Nutzer des Krebsregisters keinen Personenbezug der gespeicherten Datensätze herstellen können.

Darüber hinaus ist zu **Forschungszwecken** ein Verfahren implementiert, das unter Einschaltung einer dritten Stelle und der Einholung einer Einwilligung der betroffenen Patientinnen und Patienten durch diese dritte Stelle die Möglichkeit für die Forscherinnen und Forscher eröffnet, mit den Betroffenen in direkten persönlichen Kontakt zu treten.

Nach intensiver Diskussion sowohl des ersten als auch des überarbeiteten Gesetzentwurfs bleibt zu hoffen, dass die gegebenen Anregungen und Vorschläge aufgegriffen werden und damit ein datenschutzkonformes Krebsregister entstehen kann.

11.3 Mammografie-Screening

Mit dem Ziel, die Brustkrebssterblichkeit deutlich zu senken, hat der Bundestag beschlossen, dass die Krankenkassen und die Kassenärztliche Bundesvereinigung ein flächendeckendes und qualitätsgesichertes Screening-Programm nach Europäischen Leitlinien schaffen sollen.

Nun ist für Frauen ab dem 51. bis zum 70. Lebensjahr zur Früherkennung einer Brustkrebserkrankung ein regelmäßiges Mammografie-Screening vorgesehen. Die Teilnahme an dem Programm ist freiwillig. Zunächst sind aber **melderechtliche** und **datenschutzrechtliche** Voraussetzungen im Zusammenhang mit den Einladungen zu klären, die allen Frauen der angesprochenen Altersgruppe zugehen sollen. Das erforderliche Adressenmaterial sollen die Meldeämter an künftige „Zentrale Stellen" liefern, die in Nordrhein-Westfalen bei den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe errichtet werden. Für die Durchführung des Screenings werden regionale Screening-Stellen geschaffen.

Die Datenschutzbeauftragten des Bundes und der Länder haben einvernehmlich festgestellt, dass es nicht ausreicht, nur die melderechtlichen Bestimmungen zu ändern. Auch die **Zuständigkeit** der „Zentralen Stelle" muss gesetzlich begründet werden. Ebenfalls bislang nicht gelöst ist die datenschutzrechtliche Problematik einer weiteren **Übermittlung** der Meldedaten an die Screening-Stellen, die im Gegensatz zu den „Zentralen Stellen" private Stellen sind. Zur Qualitätssicherung soll durch die jeweilige „Zentrale Stelle" zudem ein **Abgleich** der Ergebnisse des Mammografie-Screenings mit den Daten des **Krebsregisters** erfolgen, um Erkenntnisse über Brustkrebserkrankungen trotz regelmäßiger Teilnahme am Screening zu erhalten. Die Datenschutzbeauftragten sind sich auch insoweit einig, dass hierzu die Krebsregistergesetze der Länder erweitert werden müssen.

Die datenschutzrechtlichen Anforderungen gilt es noch umzusetzen.

11.4 Elektronische Patientenakte – das Problem der Verantwortlichkeit

Im Zusammenhang mit den Reformüberlegungen im Gesundheitsbereich werden auch Modelle entworfen, im Rahmen von elektronischen Gesundheitsnetzen unter anderem eine elektronische Patientenakte mit Zugriff der am Netz beteiligten Ärztinnen und Ärzte zu führen, so beispielsweise in dem Projekt „Doctor to Doctor D2D".

Auf einem Server bei der Kassenärztlichen Vereinigung Nordrhein sollen die teilnehmenden Ärztinnen und Ärzte die Möglichkeit haben, eine **„Fallakte"** zu einer Person anzulegen, auf die alle Beteiligten am System Zugriff nehmen können. Alle teilnehmenden Ärztinnen und Ärzte können Behandlungsergebnisse und sonstige Informationen über die jeweilige Person in dieser „Fallakte" ergänzend speichern. Auch wenn für die einzelne

Information die einspeichernden Ärztinnen und Ärzte jeweils die Verantwortung für die Richtigkeit des Inhalts der eingespeicherten Daten und für die Zulässigkeit der Speicherung tragen, so ist – zumindest derzeit noch – offen, welche Person im Sinne des DSG NRW **„verantwortliche Stelle"** für die „Fallakte" insgesamt ist. Die Kassenärztliche Vereinigung Nordrhein kommt dafür jedenfalls nicht in Betracht. Auf ihrem Server müssen die Daten schon auf Grund ihrer besonderen Sensibilität verschlüsselt gespeichert sein. Dadurch wird auch eine Kenntnisnahme des Gesamtinhalts der „Fallakte" durch das an dem Betrieb des Servers beteiligte (nicht medizinische) Personal der Kassenärztlichen Vereinigung Nordrhein ausgeschlossen. Als verantwortliche Stelle im gesetzlichen Sinne kommen aber auch nur Personen in Betracht, die den Inhalt der „Fallakte" vor einem Zugriff dritter Personen, wie beispielsweise im Rahmen eines Ermittlungsverfahrens der Staatsanwaltschaft, schützen können, da sie Geheimnisträger nach § 203 StGB sind.

In Betracht kommt insoweit eine Art „Hausarztmodell", bei dem die **Hausärztin** oder der **Hausarzt** der betroffenen Person die Pflege der „Fallakte" übernimmt. Die Datenschutzrechte der Betroffenen auf Berichtigung, Sperrung und Löschung (sowie gegebenenfalls auf Schadensersatz) wären ihr oder ihm gegenüber geltend zu machen. Das bedeutet für die Hausärztinnen und Hausärzte allerdings, dass sie entsprechend für Datenschutzmängel haften. Mit der Stelle, die den Server betreut, müsste die Hausärztin oder der Hausarzt jeweils einen Vertrag über eine Datenverarbeitung im Auftrag schließen.

Der an diesem Projekt beteiligten Kassenärztlichen Vereinigung Nordrhein sind die aufgezeigten Datenschutzanforderungen bekannt gemacht worden. Welches Datenschutz- und Datensicherheitsmodell im Zusammenhang mit dem Projekt „D2D" tatsächlich umgesetzt werden soll, ist nach dem derzeitigen Erkenntnisstand noch offen.

11.5 Gesundheitskarte

Bei der geplanten Einführung der elektronischen Gesundheitskarte (eGK) zum 01.01.2006 gibt es immer noch mehr offene als gelöste Fragen.

Das Konzept der Karte steht noch nicht fest. So ist bisher nicht entschieden, ob die Daten der Versicherten auf der Karte, auf einem zentralen Server oder auf beiden Medien gespeichert werden. Der Zugriff auf diese Daten

soll allerdings nur möglich sein, wenn zeitgleich eine Ärztin oder ein Arzt, eine Apothekerin oder ein Apotheker oder eine andere in einem Heilberuf tätige Person mit dem gleichfalls elektronischen so genannten **Heilberufsausweis** (HPC) das System bedient. Dadurch sollen die Missbrauchsmöglichkeiten der Karte verringert werden beispielsweise bei Verlust oder Diebstahl.

Das Gesetz schreibt vor, dass als **Pflichtdaten und -funktionalitäten** auf der Karte neben den formellen Versicherungsvertragsdaten, dem Berechtigungsnachweis E 111 (zur Inanspruchnahme von Leistungen im europäischen Ausland) sowie einem Lichtbild und der Unterschrift der Karteninhaberin oder des Karteninhabers auch Angaben zum so genannten elektronischen Rezept (e-Rezept) enthalten sind.

Es gibt aber keinen Zwang, darüber hinaus gehende Angaben auf der Karte zu speichern. Die übrigen gesetzlich vorgesehenen Anwendungen der Karte sind **freiwillige Nutzungsmöglichkeiten** (dazu zählen die elektronische Patientenakte, der elektronische Arztbrief, die Arzneimitteldokumentation, von den Versicherten selbst zur Verfügung gestellte Daten sowie Kostenaufstellungen). Hier ist noch ungeregelt, wie diese technisch zu konzipieren sind, um den Benutzerinnen und Benutzern die größtmögliche Souveränität über ihre eigenen Daten zu gewähren und die Erstellung von Profilen zu vermeiden. Erforderlich sind auch **gestaffelte Zugriffsrechte**. Diese könnten mit PINs und TANs – ähnlich wie beim Online-Banking – geschützt werden. Damit ergibt sich jedoch das Problem, dass diejenigen Bürgerinnen und Bürger, die nicht so vertraut mit technischen Neuerungen sind, mit den neuen Funktionen nicht so umgehen können, dass sie ihr Recht auf informationelle Selbstbestimmung nicht doch aus der Hand geben, weil sie auf die Mithilfe einer dritten Person beim Bedienen der Karte angewiesen sind.

Zur Verwendung von Chipkarten im Gesundheitswesen wurden schon im 13. Datenschutzbericht 1995/96 unter 12.1, S. 88 ff., die grundlegend zu beachtenden **Anforderungen** dargestellt. Auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003 zum Gesundheitsmodernisierungsgesetz (Abdruck im Anhang, Nr. 12) nimmt dazu Stellung. Diese Forderungen haben nichts von ihrer Aktualität verloren.

Der Arbeitskreis „Gesundheit und Soziales" der Datenschutzbeauftragten des Bundes und der Länder hat eine Unterarbeitsgruppe „Gesundheitskarte"

gebildet. Dort werden die grundsätzlich zu beachtenden Kriterien bei der Konzipierung der Gesundheitskarte formuliert und deren Umsetzung kritisch begleitet.

12 Beschäftigtendatenschutz

Das von der Bundesregierung schon für die letzte Legislaturperiode angekündigte und auch jetzt in der Koalitionsvereinbarung verabredete Arbeitnehmerdatenschutzgesetz lässt noch immer auf sich warten (siehe auch 16. Datenschutzbericht 2003 unter 9., S. 99).

Angesichts der stetig wachsenden technischen Kontroll- und **Überwachungsmöglichkeiten** muss klar geregelt werden, welche Daten über Arbeitnehmerinnen und Arbeitnehmer erhoben werden dürfen, wie damit zu verfahren ist und wozu sie genutzt werden dürfen. Bewerberinnen und Bewerber sind gerade bei den heutigen Arbeitsmarktverhältnissen unter Umständen auch besonderen Risiken ausgesetzt, etwa durch unzulässig ausforschende Fragen in Bewerbungsverfahren oder durch das grundsätzlich unzulässige Verlangen eines genetischen Tests.

Daher haben die Datenschutzbeauftragten im Rahmen ihrer an den Bundesgesetzgeber und die Bundesregierung gerichteten Forderungen auch daran appelliert, zügig gesetzliche Regelungen zum **Arbeitnehmerdatenschutz** zu schaffen (Entschließung vom 27./28. März 2003, Abdruck im Anhang Nr. 2). Daher haben die Datenschutzbeauftragten im Rahmen ihrer an den Bundesgesetzgeber und die Bundesregierung gerichteten Forderungen auch daran appelliert, zügig gesetzliche Regelungen zum **Arbeitnehmerdatenschutz** zu schaffen (Entschließung vom 27./28. März 2003, Abdruck im Anhang Nr. 2).

Persönlichkeitsrechte sind im Beschäftigungsverhältnis gerade heute vielfältig bedroht. Das Arbeitnehmerdatenschutzgesetz darf deshalb nicht weiter auf die lange Bank geschoben werden.

13 Wissenschaft

13.1 Studieren über Gebühr

Die Einführung von Studiengebühren für „Langzeitstudierende" hat für erhebliches Aufsehen gesorgt. Auch wenn die Einrichtung und Führung der Studienkonten grundsätzlich nicht zu beanstanden ist, bedarf die konkrete Durchführung der Kontenverwaltung an den einzelnen Hochschulen – wie eine Stichprobe zeigt – zum Teil noch erheblicher datenschutzrechtlicher Nachbesserungen.

Die Einrichtung und Führung der Studienkonten basiert auf den Regelungen des Gesetzes zur Einführung von Studienkonten und zur Erhebung von Hochschulgebühren (**Studienkonten- und -finanzierungsgesetz** – StKFG), auf der Verordnung über die Einrichtung und Führung von Studienkonten mit Regelabbuchung sowie über die Erhebung von Gebühren an den Universitäten, Fachhochschulen und Kunsthochschulen des Landes Nordrhein-Westfalen (RVO-StKFG NW) und auf den dazu ergangenen Verwaltungsvorschriften.

Die **Aufgabe** der Einrichtung und Verwaltung der Konten ist den **Hochschulen** zugewiesen. Für alle Studierenden sind an den Hochschulen Studienkonten mit einem Guthaben eingerichtet worden, das nach Maßgabe einer in jedem Semester fälligen Regelabbuchung verbraucht wird. Welche personenbezogenen Daten der Studierenden zu diesem Zweck in welcher Weise von den Hochschulen verarbeitet werden dürfen und welche Stelle innerhalb der Hochschulen für die Verarbeitung verantwortlich ist, ist in den genannten Vorschriften nicht geregelt; auch gibt es keine konkreten technischen und organisatorischen Vorgaben zur Studienkontenverwaltung.

Das Erheben, das Speichern und das Nutzen der **erforderlichen Studierendendaten** ist nach Maßgabe der allgemeinen Regelung der §§ 12, 13 DSG NRW grundsätzlich zulässig. Dennoch müssen die Hochschulen sicherstellen, dass die Einrichtung und Führung der Konten auch datenschutzgerecht durchgeführt wird und insbesondere ein Missbrauch der Studierendendaten ausgeschlossen ist. Immerhin können im Laufe des Studiums auch besonders sensible Daten (etwa zu Erkrankungen und zu familiären oder sozialen Situationen) anfallen. Insbesondere aus Gründen der Transparenz ist es unbedingt empfehlenswert, bereichsspezifische Regelungen in die **Einschreibungsordnungen** aufzunehmen, in denen Art, Umfang und Verantwortlichkeiten der Verarbeitung der personenbezogenen

Studierendendaten unter Berücksichtigung des Zweckbindungs- sowie des Erforderlichkeitsgrundsatzes klargestellt und festgelegt werden. Die Hochschulen, die zum Zweck der Studienkontenverwaltung in der Regel ein automatisiertes Datenverarbeitungsverfahren einsetzen, haben ein **Verfahrensverzeichnis** zu erstellen (§ 8 Abs. 1 DSG NRW); dieses Verzeichnis ist für die Datenschutzbeauftragten der Hochschulen bestimmt und kann nach Absatz 2 der Norm von jeder Person eingesehen werden. Die Einhaltung der Vorschriften über den Datenschutz haben die Hochschulen ferner gemäß § 10 Abs. 1 DSG NRW durch **technische und organisatorische Maßnahmen** sicherzustellen; welche Maßnahmen zu treffen sind, muss nach § 10 Abs. 3 Satz 1 DSG NRW auf der Grundlage eines **Sicherheitskonzepts** ermittelt werden, zu dessen Bestandteilen auch die **Vorabkontrolle** hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung gehört. Diese Kontrolle ist von der oder dem Datenschutzbeauftragten der Hochschule vor der Entscheidung über den Einsatz oder eine wesentliche Änderung eines automatisierten Verfahrens durchzuführen.

Die Studierenden müssen zwar den mit der gesetzlichen Einführung von Studienkonten und -gebühren verbundenen Eingriff in ihr Recht auf informationelle Selbstbestimmung hinnehmen. Allerdings müssen alle Hochschulen sicherstellen, dass die Einrichtung und Verwaltung dieser Konten auch datenschutzgerecht durchgeführt wird.

13.2 Evaluation der Lehre

An den Hochschulen bewerten inzwischen nicht nur die Lehrenden die Leistungen der Studierenden, sondern die Studierenden beurteilen auch die Lehrenden und die Qualität ihrer Veranstaltungen. Soweit dabei personenbezogene Daten verarbeitet werden, bedarf dies der Regelung in einer Evaluationsordnung der Hochschule.

Das Hochschulgesetz (HG) sieht eine regelmäßige Evaluation von Lehrveranstaltungen und Studiengängen zum Zweck der Qualitätssicherung und -verbesserung vor, an der alle Mitglieder und Angehörigen der Hochschule mitzuwirken verpflichtet sind (§ 6 Abs. 1 HG). Insbesondere die Studierenden sollen zu ihrer Einschätzung befragt werden. Auch eine Veröffentlichung der Bewertungsergebnisse ist vorgeschrieben. Allerdings – und das ist der datenschutzrechtlich entscheidende Punkt – hat die Hochschule das Bewertungsverfahren gemäß § 6 Abs. 3 HG zuvor in einer

Evaluationsordnung festzulegen, die auch Bestimmungen über Art, Umfang und Behandlung der zu erhebenden, zu verarbeitenden und zu veröffentlichenden personenbezogenen Daten der Mitglieder und Angehörigen der Hochschule enthält. Das DSG NRW ist dabei zu beachten.

Was zunächst ganz einfach klingt, erweist sich in der Praxis allerdings oft als schwierig. Viele Hochschulen haben noch gar keine oder aber eine datenschutzrechtlich unzureichende **Evaluationsordnung**, obwohl in den Bewertungsverfahren personenbezogene Daten der Lehrenden und/oder der Lernenden verarbeitet werden (sollen). Ohne eine entsprechende Ordnung ist die Verarbeitung personenbezogener Daten nur mit **Einwilligung** der Betroffenen zulässig.

Häufig wird bereits die Tatsache verkannt, dass im Rahmen der Evaluationen überhaupt **personenbezogene Daten** verarbeitet werden. Sollen sich Studierende etwa mit ihrer Matrikelnummer einloggen, um einen Online-Fragebogen auszufüllen, werden damit zugleich personenbezogene Daten erhoben, auch wenn ihre Namen nicht erfasst werden. Wird jede Veranstaltung einzeln evaluiert, beziehen sich die Aussagen zur Qualität der Veranstaltung notwendigerweise zugleich auch auf die Lehrkraft, so dass alle abgegebenen Bewertungen personenbezogen sind. Vor allem Freitextfelder in Fragebögen eröffnen die Möglichkeit, weitere personenbezogene Daten zu offenbaren.

Auch wenn schon vor Beginn des Bewertungsverfahrens eine Evaluationsordnung erlassen wurde sind die Regelungen zum Umgang mit personenbezogenen Daten im Rahmen der Bewertungsverfahren zumeist **unvollständig** oder sogar **widersprüchlich**. So erwies sich beispielsweise eine Evaluationsordnung – ungewollt – als „Mogelpackung", in der es in einer Vorschrift hieß, die Datenerfassung solle anonym erfolgen, in weiteren Vorschriften aber ausgeführt wurde, welche Daten der Studierenden erhoben und dass die Daten der Lehrenden zum frühestmöglichen Zeitpunkt, jedenfalls aber noch vor der Veröffentlichung anonymisiert würden. Augenfällig war dabei nicht nur der Widerspruch zwischen der vermeintlich anonymen Datenerhebung und den Regelungen zur Verarbeitung von personenbezogenen Daten, sondern es fehlten auch Angaben zur Art der Daten, die von den Lehrenden erhoben werden sollten sowie genauere Regelungen zum Umfang und der Behandlung der erfassten Daten der Lehrenden wie auch der Lernenden. Im Übrigen war auch nicht ersichtlich, warum bei dem konkret geplanten Bewertungsverfahren überhaupt Daten der Studierenden erhoben werden sollten. Dem **Grundsatz der**

Datenvermeidung entsprechend ist auf eine Verarbeitung personenbezogener Daten zu verzichten, wenn sie zum Zweck der Durchführung des Evaluation nicht unbedingt erforderlich ist.

Hochschulen müssen noch vor Beginn eines Bewertungsverfahrens in einer Evaluationsordnung regeln, welche Art von Daten der Lehrenden und – gegebenenfalls – welche Daten der Studierenden im Rahmen des Verfahrens in welchem Umfang, von wem und wie verarbeitet (also erhoben, gespeichert, genutzt, übermittelt, veröffentlicht) und vor allem, wann sie gelöscht werden. Die Datenverarbeitung hat sich dabei insgesamt am Grundsatz der Erforderlichkeit zu orientieren.

13.3 Auskunftei für juristische Staatsprüfungen

Wer kennt sie nicht, die Angst vor Prüfungen? Doch bei allem Verständnis für die Nöte der Prüflinge dürfen zur Bekämpfung der Prüfungsangst nur Mittel eingesetzt werden, die auch den datenschutzrechtlichen Belangen der Prüferinnen und Prüfer hinreichend Rechnung tragen. Das war bei dem Vorhaben eines Dienstleisters, einen Austauschdienst für Protokolle mündlicher juristischer Staatsprüfungen via Internet einzurichten, nicht der Fall.

Wie die Prüfung des konkreten Vorhabens bestätigt, ist nicht alles, was seit langem gängige Praxis ist, deshalb zugleich auch schon datenschutzkonform. Die Geschäftsidee des Austauschdienstes für Protokolle der mündlichen Staatsprüfungen ist durchaus nicht neu: Von ehemaligen Prüflingen gefertigte **Prüfungsprotokolle** werden gesammelt, anderen Prüflingen zur Einsichtnahme zur Verfügung gestellt, und letztere werden zugleich dazu verpflichtet, von ihren mündlichen Prüfungen wiederum entsprechende Protokolle anzufertigen und abzugeben. Diese Protokolle enthalten eine Reihe personenbezogener Daten, und zwar sowohl solche der Prüflinge selbst als auch vor allem solche der Prüferinnen und Prüfer. In dem in Rede stehenden Vorhaben sollten von letzteren nicht nur identifizierende Angaben wie Berufsbezeichnung, Titel und Name erhoben und der sachliche Gegenstand ihrer Prüfungen dargestellt, sondern darüber hinaus umfassende weitere Informationen – etwa vermeintlich festgestellte Charaktereigenschaften sowie ihre Prüfweise – nach der subjektiven Wahrnehmung und mit persönlichen Wertungen der Prüflinge erfasst werden.

Als **gesetzliche Grundlage** für die in dem konkreten Vorhaben geplante geschäftsmäßige Erhebung und Speicherung der Daten zum Zwecke der

Übermittlung an die Prüfungskandidatinnen und -kandidaten kamen nur § 29 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG in Betracht, deren Voraussetzungen indes nicht erfüllt waren.

Es besteht durchaus Grund zu der Annahme, dass die betroffenen Prüferinnen und Prüfer ein **schutzwürdiges Interesse** an dem **Ausschluss** der Erhebung und Speicherung ihrer Daten haben. Zwar mögen die Prüflinge im Hinblick auf die anstehenden mündlichen Examina daran interessiert sein, vorsorglich möglichst viele Informationen über ihre Prüferinnen und Prüfer zu erhalten. Demgegenüber liegt es jedoch im Interesse der letzteren, dass Angaben über ihre persönlichen und sachlichen Verhältnisse nicht bei Dritten erhoben und ungewollt auf einer privaten Website zur Übermittlung an künftige Prüflinge gespeichert werden. Dies gilt erst recht, wenn die Fülle der vorgesehenen Daten berücksichtigt wird, die viele subjektive Wertungen und möglicherweise auch objektiv falsche Aussagen über die Prüferinnen und Prüfer enthalten würden. Die Verarbeitung solcher Daten beeinträchtigt die schutzwürdigen Belange der Betroffenen in besonderer Weise. Die geplante Datensammlung war nach dem besonderen Geschäftszweck gerade darauf angelegt, ein möglichst umfassendes und vielschichtiges Profil der Prüferinnen und Prüfer, ihrer Persönlichkeit sowie ihres Prüfungsverhaltens zu schaffen. Eine solche massive Belastung ihres Persönlichkeitsrechts müssen die Betroffenen nicht hinnehmen.

Auch § 29 Abs. 1 Satz 1 Nr. 2 BDSG schied als Rechtsgrundlage für die geplante Datenverarbeitung aus, da die Gesamtheit aller Informationen, die über die betroffenen Personen erhoben und gespeichert werden sollten, **nicht** aus **allgemein zugänglichen Quellen** entnommen werden konnte.

Mangels gesetzlicher Befugnisnorm ist dieses Vorhaben ohne die wirksamen Einwilligungen der betroffenen Personen – Prüferinnen und Prüfer, Kandidatinnen und Kandidaten – unzulässig. Voraussetzung für eine derartige Einwilligung wäre insbesondere eine vorherige umfassende Aufklärung über die Freiwilligkeit und Widerrufbarkeit der Einwilligung, über Art und Umfang der zu verarbeitenden Daten, über den gesamten Vorgang der geplanten Datenverarbeitung und ihren Zweck sowie über die Risiken der Internetnutzung, die vorgesehenen Sicherheitsmaßnahmen, die Rechte der Betroffenen und dergleichen mehr. Mit der Einholung der Einwilligungen bei den jeweiligen Prüferinnen und Prüfern durch die Auskunftei – als verantwortlicher Stelle – würde zugleich der **Pflicht zur Unterrichtung** über die zu speichernden Daten gemäß § 33 Abs. 1 Satz 2

BDSG nachgekommen und den betroffenen Personen die Möglichkeit zur Korrektur falscher Daten eröffnet.

Die geschäftsmäßige Sammlung und Übermittlung personenbezogener Daten von Prüferinnen und Prüfern sowie Examenskandidatinnen und -kandidaten durch Online-Informationsdienste ist grundsätzlich nur mit wirksamer Einwilligung der betroffenen Personen zulässig.

14 Forschung

14.1 Das Kompetenznetz HIV/AIDS

In Kürze wird das Kompetenznetz HIV/AIDS e.V. an den Start gehen. Nach mehrjähriger Vorplanung hat der bundesweite Forschungsverbund mit Sitz in Nordrhein-Westfalen ein Konzept für den datenschutzgerechten und sicheren Umgang mit sensiblen Daten über die HIV/AIDS-Krankheit in einem vernetzten System erarbeitet.

Bereits im 15. Datenschutzbericht 2001 (unter 13.4, S. 119 ff.) wurde über Planungen in der medizinischen Forschung berichtet, die vorhandene bundesweit zersplitterte Kompetenz durch den Einsatz moderner Datenverarbeitungssysteme zu bündeln und so besser nutzbar zu machen. Dabei wurde eingehend auf die damit verbundenen datenschutzrechtlichen Probleme hingewiesen. Inzwischen sind diese Planungen weit fortgeschritten, und verschiedene Netze haben bereits mit der **praktischen Umsetzung** ihrer Konzepte begonnen. Die Landesbeauftragten für den Datenschutz waren und sind mit der datenschutzrechtlichen Beratung und Prüfung mehrerer dieser hochkomplexen Kompetenznetze befasst.

Da den Forschungsnetzen gleiche Probleme hinsichtlich der Art der Daten, der Struktur der Datenerfassung und der Datenhaltung innewohnen, hat die Telematikplattform Medizinische Forschungsnetze (TMF) inzwischen erfreulicherweise zwei generische **Lösungsmodelle** erarbeitet, die mit dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder abgestimmt sind. Das so genannte Modell A bezieht sich auf die „Bereitstellung von Behandlungs- und Forschungsdaten in klinisch fokussierten Forschungsnetzen", während Modell B die „Pseudonymisierung von Forschungsdaten in wissenschaftlich fokussierten Forschungsnetzen" zum Gegenstand hat. Die Entwicklung dieser Grundmodelle stellt einen Schritt in die richtige Richtung dar, nämlich die Erarbeitung der Datenschutzkonzepte für die Netze einfacher und effizienter zu machen, auch wenn mit den Modellen allein noch nicht alle Probleme gelöst sind. Davon abgesehen, dass jedes Kompetenznetz eigene Besonderheiten aufweist, die auch künftig eine individuelle Prüfung und Beratung erforderlich machen werden, steht die erforderliche Technik für die Umsetzung der Modelle bislang noch nicht umfassend zur Verfügung.

Diese Erfahrung machte das Kompetenznetz HIV/AIDS e.V., nachdem es anhand der TMF-Vorschläge ein – mit einigen Varianten – auf das Modell B

abgestimmtes **Datenschutzkonzept** entwickelt hatte. Da der für die Durchführung dieses Konzepts erforderliche Pseudonymsierungsdienst technisch noch nicht bereitstand und -steht und auch noch nicht abzusehen ist, wann dieser Lösungsansatz zu realisieren sein wird, erstellte das Forschungsteam für die Übergangszeit inzwischen ein eigenes „abgespecktes" Konzept. Nach diesem Übergangsmodell werden die identifizierenden Daten der Teilnehmenden nicht – wie in beiden obengenannten Grundmodellen vorgesehen – an eine externe Datentreuhänderin oder einen -treuhänder übermittelt und dort verwaltet, sondern sie verbleiben ausschließlich in der jeweiligen Behandlungseinrichtung selbst. Die sensiblen Forschungsdatensätze werden in diesen Einrichtungen mit Pseudonymen versehen und nur in dieser **pseudonymisierten Form** in die Datenbank des Netzwerks eingegeben. Die behandelnden Ärztinnen und Ärzte händigen jeder teilnehmenden Person ihr Pseudonym in Papierform aus.

Derzeit werden noch die Patienteninformations- und Einwilligungsschreiben an dieses modifizierte Konzept angepasst. Wie in anderen Forschungsprojekten bedarf es einer umfassenden **Aufklärung** der potentiellen Teilnehmenden über das konkrete Vorhaben sowie insbesondere über den gesamten Prozess der geplanten Datenverarbeitung, die für die Datenverarbeitung verantwortlichen Stellen und Personen, die Freiwilligkeit der Teilnahme und die Rechte der Teilnehmenden (etwa beispielsweise die Möglichkeit des Einwilligungswiderrufs und dessen Folgen sowie das Recht auf Auskunft). Die betroffenen Personen können auf der Grundlage dieser Informationen sodann über ihre Teilnahme an dem Kompetenznetz entscheiden und gegebenenfalls ihre schriftliche Einwilligung in die damit verbundene Datenverarbeitung erklären.

Nach dem derzeitigen Erkenntnisstand begegnen der vorgesehenen Datenverarbeitung im Kompetenznetz HIV/AIDS e.V. keine durchgreifenden Bedenken. Selbstverständlich entscheiden die Betroffenen selbst, ob sie an dem Forschungsvorhaben teilnehmen möchten; ohne ihre wirksame Einwilligung dürfen ihre medizinischen Daten nicht zu Forschungszwecken von und in dem Netz verarbeitet werden.

14.2 Forschungsregister

Ginge es nach dem Wunsch vieler Forscherinnen und Forscher, würden zahlreiche Register eingerichtet, in denen Namen, Anschriften und gegebenenfalls weitere Angaben von ehemaligen Teilnehmenden ihrer

Forschungsprojekte verzeichnet würden. Ohne eine spezielle gesetzliche Grundlage ist die Einrichtung solcher Register jedoch unzulässig.

Das Vorhaben, personenbezogene Daten von ehemaligen Teilnehmenden in Registern zu speichern und anderen Forschenden den Zugang zu diesen Datensammlungen zu ermöglichen, ist in der Regel selbst dann unzulässig, wenn in das Verzeichnis nur Daten solcher Personen aufgenommen werden sollen, die eine entsprechende **Einwilligungserklärung** unterzeichnet haben. Voraussetzung einer wirksamen Einwilligung ist nämlich unter anderem, dass die betroffenen Personen zuvor umfassend und detailliert über das konkrete Ziel und die zu diesem Zweck vorgesehene Datenverarbeitung einschließlich der Speicherdauer der personenbezogenen Daten aufgeklärt wurden. Die Erstellung der Forschungsregister dient jedoch keinem bestimmten und begrenzten Zweck, wie etwa der Durchführung eines konkreten und überschaubaren Forschungsvorhabens, sondern stellt eine **Datenvorratshaltung** von unbestimmter Dauer für noch nicht bestimmte Forschungsvorhaben dar. Mangels Aufklärung könnten die Betroffenen allenfalls unspezifische Generaleinwilligungen geben. Solche Erklärungen sind indes datenschutzrechtlich unwirksam und stellen keine Rechtsgrundlage für die beabsichtigte Datenverarbeitung dar.

Hinzu kommt, dass die **Bedeutung und Trageweite** derartiger Verzeichnisse oftmals von den potentiellen Betroffenen verkannt, aber auch von den Forschenden selbst unzutreffend eingeschätzt wird. Wie brisant die Aufnahme von Daten in ein solches Register sein kann, wird gerade im Bereich der Gesundheitsforschung deutlich: Selbst wenn ausschließlich Name und Adressdaten betroffener Personen verzeichnet würden, würde mit jedem Zugriff auf dieses Krankheitsverzeichnis zugleich auch ein Gesundheitsdatum übermittelt.

Die Erstellung von Forschungsregistern sowie die Aufnahme der Betroffenen in solche Verzeichnisse bedürfen einer spezifischen Rechtsvorschrift, die Zweck, Art und Umfang der Datenverarbeitung, Zugriffsrechte, Verantwortlichkeiten, Datenpflege, Schutzrechte der Betroffenen und dergleichen mehr regelt.

15 Schule

15.1 Die SMS gegen das Schuleschwänzen

„Paul ist nicht zum Unterricht erschienen!" „Pauline hat in der ersten Stunde gefehlt!" So oder ähnlich lauten die Kurzmitteilungen, die manche Eltern auf ihren Mobiltelefonen empfangen können. Mit Handy und SMS soll – nach einer neuen Geschäftsidee – dem Problem des Schuleschwänzens begegnet werden.

Eine Firma bietet derzeit im Testlauf folgendes Verfahren an: Fehlt eine Schülerin oder ein Schüler im Unterricht, meldet die Lehrkraft diese Information an das Schulsekretariat. Hier hat die verantwortliche Person Zugriff auf eine **Datenbank** mit den entsprechenden Angaben des Kindes und der Eltern. Es bedarf nur noch eines Mausklicks, und schon erhalten die Erziehungsberechtigten per SMS eine Benachrichtigung über das Fehlen ihrer Tochter oder ihres Sohns.

Eine Rechtsvorschrift, die diese Datenübermittlung erlauben würde, gibt es nicht. § 18 Schulpflichtgesetz kann nicht als Rechtsgrundlage dienen, da eine sofortige Information der Erziehungsberechtigten über jedes Fernbleiben vom Unterricht über diese Regelung hinausgeht. Auch im Schulverwaltungsgesetz (SchVG) und in der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten findet sich **keine** entsprechende **Übermittlungsbefugnis**. Das Meldeverfahren ist deshalb nur zulässig, wenn die **Erziehungsberechtigten** der minderjährigen Schülerinnen und Schüler zuvor wirksam in einen solchen Datentransfer **eingewilligt** haben. Ist darüber hinaus eine Dokumentation aller Benachrichtigungen in dem Datenverarbeitungssystem der Schule vorgesehen, müssen auch die Minderjährigen ihre Einwilligung in diese Datenverarbeitung erklären, wenn sie gemäß des § 19 Abs. 2 Satz 3 SchVG selbst einwilligungsfähig sind.

Die Entscheidung über den Einsatz eines solchen Meldeverfahrens in der Schule trifft **die Schulleitung** unter Beteiligung der Schulkonferenz. Die Schulleitung ist im Weiteren für den zulässigen Einsatz des **Informationsdienstes** in der Schule **verantwortlich**, auch wenn das System von einem privaten Unternehmen installiert wird. Sie muss deshalb das auf die Schule abgestimmte Konzept prüfen, dokumentieren und in eine Handlungsanweisung an Lehrkräfte und Schulsekretärin oder -sekretär umsetzen. Außerdem muss sie die Vorabkontrolle gemäß § 10 Abs. 3 DSG NRW durchführen

lassen. Sie trägt ferner die Verantwortung für die Aufklärung der Erziehungsberechtigten, Schülerinnen, Schüler und Lehrkräfte und muss schriftliche Einwilligungserklärungen einholen. Die erforderlichen individuellen Einwilligungen können keinesfalls durch den Beschluss der Schulkonferenz ersetzt werden.

Der Einsatz eines elektronischen Informationsverfahrens, bei dem die Erziehungsberechtigten unverzüglich per SMS über jedes Fernbleiben ihrer Kinder vom Unterricht benachrichtigt werden, ist in Schulen nur auf der Grundlage wirksamer Einwilligungen der Erziehungsberechtigten zulässig.

15.2 Einsicht in Abiturunterlagen

Gründe, die eigenen Abiturunterlagen über kurz oder lang noch einmal einsehen zu wollen, gibt es viele. Je nach Zeitablauf kommen dabei unterschiedliche Rechtsgrundlagen für einen Anspruch auf Einsichtnahme in Betracht. Die leider festzustellende ablehnende Haltung vieler Schulleitungen gegen eine solche Einsichtnahme ist nicht datenschutzkonform.

Die Gymnasiastin Anna A. hat soeben die Ergebnisse ihrer Abiturprüfungen erfahren; verwundert über die Benotungen möchte sie die Arbeiten möglichst unverzüglich einsehen. Den Wunsch zur Einsichtnahme teilt sie mit Bernd B., der sein Abitur allerdings bereits vor fünf Jahren abgelegt hat und sich nunmehr voll Stolz an seine damaligen Leistungen erinnern möchte. Carla C. hat bei der 10-Jahres-Feier ihres Abiturjahrgangs die Idee, die Abiturunterlagen nicht nur einzusehen, sondern nach Möglichkeit auch mit nach Hause zu nehmen.

In den genannten Fällen ist wie folgt zu unterscheiden:

Schülerinnen und Schülern eines Gymnasiums oder einer Gesamtschule sowie deren Erziehungsberechtigten ist gemäß § 43 Abs. 4 der Verordnung über den Bildungsgang und die Abiturprüfung in der gymnasialen Oberstufe (APO-GOSt) auf Antrag **Einsicht** in die sie betreffenden Prüfungsunterlagen zu geben, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer **rechtlichen Interessen** erforderlich ist. Die dazu erlassenen Verwaltungsvorschriften stellen unter anderem klar, dass ein rechtliches Interesse gegeben ist, wenn die betroffene Person an der Richtigkeit der Bewertung ihrer Arbeit zweifelt oder wenn sie sich nachträglich von ihrer Leistung und der Ordnungsmäßigkeit ihrer Bewertung überzeugen will.

Außerdem wird darauf hingewiesen, dass die Einsichtnahme auch dadurch erfolgen kann, dass sich die betroffene Person eine **Kopie** der eigenen Prüfungsarbeiten gegen Erstattung der Kosten aushändigen lässt. Anna A., deren Schulverhältnis noch nicht beendet ist, hat also nach § 43 Abs. 4 APO-GOSt einen Anspruch auf Einsichtnahme und Kopie. Hätte sie ein Berufskolleg besucht, stünde ihr ein entsprechender Anspruch gemäß § 28 Abs. 3 der Verordnung über die Ausbildung und Prüfung in den Bildungsgängen des Berufskollegs (APO-BK) zu.

Die genannten Verwaltungsvorschriften führen allerdings, wie verschiedene Beschwerden belegen, bei einigen Schulleitungen zu dem Missverständnis, dass hierin zugleich der Anspruch auf Einsichtnahme erschöpfend geregelt sei. Ein Jahr nach dem Abitur liege die Gewährung der Einsichtnahme nur noch im Ermessen der jeweiligen Schulleitung. Das ist jedoch nicht zutreffend. Da sich § 43 Abs. 4 APO-GOSt nach seinem eindeutigen Wortlaut nur auf die Einsichtnahme von „Schülerinnen und Schülern" bezieht und das Schulverhältnis mit der Aushändigung des Abiturzeugnisses endet (vgl. § 7 Abs. 1 Buchstabe a) der Allgemeinen Schulordnung – ASchO), regelt diese Vorschrift nur einen Teilaspekt des Akteneinsichtsrechts. Mangels bereichsspezifisch abschließender Regelung finden für die Zeit **nach Beendigung des Schulverhältnisses** die allgemeinen Zugangsrechte des DSG NRW Anwendung. Bernd B. hat deshalb einen Anspruch auf Einsichtnahme nach § 18 Abs. 1, Abs. 2 DSG NRW. Auch er kann – gegen Kostenerstattung – Kopien der Unterlagen beanspruchen.

Diese Rechte stehen grundsätzlich ebenfalls Carla C. zu; wenn sie die Arbeiten noch einsehen möchte, sollte sie sich jedoch beeilen. Nach § 9 Abs. 1 Satz 1 Nr. 3 der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten in Verbindung mit § 24 Abs. 2 ASchO sind die Abiturprüfungsunterlagen nämlich nur **zehn Jahre** in den Schulen aufzubewahren und danach zu vernichten. Einen gesetzlichen Anspruch auf **Herausgabe** der Unterlagen gibt es – sehr zum Bedauern von Carla C. – nicht.

Das Recht, die eigenen Abiturarbeiten einzusehen, ist zeitlich nur durch die gesetzliche Aufbewahrungsfrist von zehn Jahren begrenzt. Schülerinnen und Schüler haben ein Recht auf Einsichtnahme nach Maßgabe der einschlägigen Ausbildungs- und Prüfungsordnungen; nach Beendigung des Schulverhältnisses besteht der Anspruch auf Einsicht nach § 18 DSG NRW weiter.

16 Kultur

16.1 Abgabe von Reproduktionen personenbezogenen Archivguts an Gedenkeinrichtungen

Zeitgeschichtliche Dokumentation und Forschung haben einen hohen Stellenwert. Wenn historische Dokumente personenbezogene Daten enthalten, müssen dabei jedoch die Datenschutzbelange der betroffenen Personen gewahrt werden. Sollen – wie geplant – personenbezogene Datenbestände aus dem Landesarchiv auf Mikrofilme reproduziert und an Einrichtungen zur Dokumentation des Holocausts übermittelt werden, bedarf dieser Datentransfer einer gesetzlichen Grundlage.

Seit langem wird über den Antrag beraten, in den Staatsarchiven aufbewahrte personenbezogene Unterlagen – insbesondere Akten über die Verfolgung von nationalsozialistischen Gewaltverbrechen durch die Justizbehörden – zu verfilmen und diese Reproduktionen an die **Gedenkstätte Yad Vashem** in Israel und an das Institut für Zeitgeschichte in München zu übermitteln. Die Unterlagen sollen in den Einrichtungen auf Dauer zur Dokumentation der Zeitgeschichte gesammelt, in einer Datenbank erfasst und darüber hinaus auch wissenschaftlich genutzt werden. Alle Verantwortlichen sind sich einig, dass das Vorhaben von großer Bedeutung ist und unterstützen es.

Das **Archivgesetz Nordrhein-Westfalen** (ArchivG NRW), das den Umgang mit personenbezogenem Archivgut bereichsspezifisch regelt, enthält **keine Rechtsgrundlage** für die geplante Datenübermittlung. Nach § 7 Abs. 1 ArchivG kann nach Ablauf der in Absatz 2 der Norm genannten Sperrfristen Archivgut **nutzen**, wer ein berechtigtes Interesse an der Nutzung glaubhaft macht. Bezieht sich das Archivgut nach seiner Zweckbestimmung oder nach seinem wesentlichen Inhalt auf eine natürliche Person, so darf es frühestens 10 Jahre nach deren Tod genutzt werden; ist der Todestag dem Archiv nicht bekannt, endet die Sperrfrist 90 Jahre nach der Geburt. Bezogen auf die in Rede stehenden Unterlagen ist nicht davon auszugehen, dass die jeweiligen **Sperrfristen** gegenwärtig alle abgelaufen sind. Diese Fristen können ohne die Einwilligungen der Betroffenen unter anderem nur dann verkürzt werden, wenn das Archivgut zu benannten wissenschaftlichen Zwecken, also für konkrete, bereits jetzt feststehende Forschungsvorhaben, genutzt wird. Dies ist hier – jedenfalls in Bezug auf die Gedenkstätte selbst – nicht der Fall. Unabhängig von diesen Sperrfristen ist aber eine **Vervielfältigung** ganzer Archivbestände und die **Übergabe**

dieser Reproduktionen an andere Einrichtungen **zu Dokumentations- und nicht konkretisierten Forschungszwecken** im ArchivG NRW nicht vorgesehen.

Ursprünglich sollte der Datentransfer auf **Verträge** mit den genannten Einrichtungen gestützt werden, in denen der Umgang mit dem personenbezogenen Archivgut geregelt wird. Außerdem sollten in den Verträgen die Sperrfristen für die Nutzung dieses Archivguts verkürzt werden. Verträge als solche reichen allerdings nicht aus, um eine solche Datenübermittlung zu legitimieren. Nach dem Verfassungsgrundsatz des Vorbehalts des Gesetzes bedarf die Verarbeitung von personenbezogenen Daten – ohne die Einwilligung der Betroffenen – vielmehr einer **normenklaren gesetzlichen Grundlage**. In einer solchen Befugnisnorm müssten die wesentlichen Voraussetzungen für die Zulässigkeit der Datenübermittlung festgelegt sein. Die näheren Einzelheiten des Transfers können dann vertraglich geregelt werden.

Erfreulicherweise hat das Kulturministerium inzwischen ausdrücklich zugesagt, dass bei der nächsten Novellierung eine entsprechende Befugnisnorm in das Archivgesetz aufgenommen wird. Justizministerium, Innenministerium und Staatskanzlei haben sich ausdrücklich für die baldige Schaffung einer solchen Rechtsgrundlage ausgesprochen.

Um die vorgesehene Übermittlung von Reproduktionen personenbezogenen Archivguts zu Dokumentations- und Forschungszwecken zu ermöglichen, sollte nunmehr zeitnah eine entsprechende gesetzliche Ermächtigungsgrundlage in das ArchivG NRW eingefügt werden. In dieser Befugnisnorm sind – unter Wahrung der Belange der Betroffenen – insbesondere Zweck, Gegenstand und Umfang der zulässigen Datenübermittlung festzuschreiben.

16.2 Stadtarchiv statt Archiv-GmbH

Seit langem ist ein Trend zur Privatisierung kommunaler Aufgaben zu verzeichnen. Da verwundert nicht, dass nunmehr auch das Archiv eines Kreises in eine GmbH umgewandelt und das Archiv einer Stadt – zusammen mit verschiedenen Kultureinrichtungen – in eine Kultur-GmbH eingebracht werden sollte. Gegen eine Überführung der kommunalen Archive in Gesellschaften privaten Rechts sprechen jedoch durchgreifende Bedenken.

Die kommunalen Archive haben eine besondere datenschutzrechtliche Bedeutung und **Verantwortung**. Gemäß § 10 Abs. 1 Archivgesetz Nordrhein-Westfalen (ArchivG NRW) tragen die Gemeinden und Gemeindeverbände für ihr Archivgut Sorge, indem sie es verwahren, erhalten, erschließen und nutzbar machen. Archivwürdige Unterlagen, die zur Aufgabenerfüllung nicht mehr benötigt werden, sind in das Archiv zu übernehmen. Dies gilt – mit wenigen Ausnahmen – auch für Unterlagen, die personenbezogene Daten enthalten und für solche, die einem Berufsgeheimnis, einem besonderen Amtsgeheimnis oder sonstigen Geheimhaltungsvorschriften unterliegen, also auch für Unterlagen mit besonders sensiblen Gesundheits-, Sozial-, Prozess-, Personal- und Steuerdaten. Alle in den Unterlagen erfassten personenbezogenen Daten werden in den Archiven auf Dauer neuen Zwecken – insbesondere der Dokumentation, der Information und der Forschung – zugeführt. Wer das Archivgut wie nutzen kann, entscheiden die Archivverwaltungen im Rahmen der gesetzlichen Vorgaben. Dabei kommt auch eine Nutzung durch interessierte Dritte in Betracht.

Die Erfüllung der genannten **archivischen Kernaufgaben** ist mit erheblichen Grundrechtseingriffen verbunden. Sowohl durch die Übernahme der personenbezogenen Unterlagen als auch durch ihre Archivierung, Nutzung und die Entscheidung über ihre Nutzung durch Dritte wird in das Grundrecht der betroffenen Personen auf informationelle Selbstbestimmung eingegriffen. Insoweit werden die Gemeinden und Gemeindeverbände im Bereich der kommunalen Archivverwaltungen **hoheitlich** tätig. Die dazu erforderlichen Eingriffsbefugnisse räumt ihnen § 10 ArchivG NRW ein, der mit seinen bereichsspezifischen Datenschutzregelungen zugleich die Voraussetzungen und Grenzen der Zulässigkeit dieses Grundrechtseingriffs festlegt. Nur im Rahmen dieser gesetzlichen Bestimmungen haben die von der Archivierung und Nutzung ihrer Daten betroffenen Personen den Eingriff in ihr Grundrecht hinzunehmen. Das ArchivG NRW sieht nun aber keine Übertragung dieser hoheitlichen Aufgaben und Eingriffsbefugnisse der kommunalen Archivverwaltungen auf eine juristische Person des Privatrechts vor. Eine entsprechende Rechtsgrundlage findet sich auch nicht in anderen Vorschriften, und die fehlende gesetzliche Regelung kann nicht durch einen Unternehmensvertrag ersetzt werden. Deshalb können kommunale Archive nicht so ohne weiteres in juristische Personen des Privatrechts umgewandelt werden.

Die hoheitliche Funktion der kommunalen Archivverwaltungen, personenbezogene Unterlagen zu übernehmen, zu archivieren, zu nutzen und nutzbar zu machen, kann nach geltendem Recht weder auf eine Archiv-GmbH noch auf eine Kultur-GmbH übertragen werden.

16.3 Archivarische Findmittel im Internet

Viele Archive sind zur Optimierung ihrer Dienstleistung bestrebt, dem Wunsch potentieller Nutzerinnen und Nutzern zu entsprechen und die archivarischen Findmittel im Internet zu veröffentlichen. Dabei gibt es nur einen Haken: Soweit diese Findmittel personenbezogene Daten enthalten, fehlt es für deren Veröffentlichung an der erforderlichen Befugnisnorm.

Alle Archive halten – jedenfalls in Papierform – so genannte Findmittel bereit, in denen die archivierten Aktenbestände mit der Archivsignatur und weiteren Ordnungskriterien verzeichnet sind. Die Idee, diese **Findhilfen** auch im **Internet** zu veröffentlichen, ist durchaus überzeugend: Der Historiker aus München soll ebenso wie die Sozialforscherin aus den USA vom jeweiligen Standort aus prüfen können, ob sich die Anreise und weitere Recherche in den jeweiligen Archiven auch lohnt. Zugleich würden die Archive in ihrer schriftlichen Auskunftstätigkeit entlastet.

Die Findmittel enthalten jedoch – zumindest zum Teil – selbst **personenbezogene Daten**, die dem Archivgut entstammen. So fragte beispielsweise ein Archiv an, ob Findmittel zu Akten von Verwaltungsbeamtinnen und -beamten ins Internet gestellt werden dürften, in denen zusammen mit der Archivsignatur die jeweiligen Namen, Vornamen, Geburtsdaten, Berufe und die letzten Dienststellen vermerkt seien. Mit dem Einstellen dieser personenbezogenen Findmittel würden die Personenangaben zugleich an eine unbestimmte Vielzahl von Personen übermittelt. Ein solcher Datentransfer ist ohne Einwilligung der betroffenen Personen nur zulässig, wenn eine **Rechtsvorschrift** ihn erlauben würde. Dies ist bislang nicht der Fall.

Die Verarbeitung personenbezogenen Archivguts ist im Archivgesetz Nordrhein-Westfalen (ArchivG NRW) bereichsspezifisch abschließend geregelt. Dieses Gesetz selbst sieht **keine Veröffentlichungsbefugnis** vor. Insbesondere auch § 1 Abs. 1 Satz 1 ArchivG NRW, nach dem die Erforschung und Veröffentlichung zu den Aufgaben der staatlichen Archive gehört, normiert keine solche Befugnis, sondern enthält lediglich eine Aufgabenzuweisung, so dass diese Vorschrift nicht als Rechtsgrundlage für

die Veröffentlichung personenbezogener Angaben aus Archivgut herangezogen werden kann. Personenbezogene Angaben dürfen vielmehr nur nach Maßgabe des § 7 ArchivG NRW an Dritte übermittelt werden. Dies setzt voraus, dass zum einen die in Abs. 2 normierten **Sperrfristen** einer Nutzung nicht mehr entgegenstehen und zum anderen die dritte Person ein **berechtigtes Interesse** an der Nutzung glaubhaft gemacht hat. Ob diese kumulativ erforderlichen Voraussetzungen vorliegen, hat das Archiv in jedem Einzelfall gesondert zu prüfen. § 7 ArchivG NRW ermächtigt die Archive mithin nicht, personenbezogene Daten aus Archivgut durch eine Internetveröffentlichung an eine unbeschränkte Vielzahl von Personen zu übermitteln, die ihr berechtigtes Interesse nicht zuvor dargelegt haben. Aus denselben Gründen ist aber auch jede andere Veröffentlichung personenbezogener Angaben in Findmitteln nicht zulässig.

Das Vorhaben eines Archivs, aus dem vorhandenen personenbezogenen Archivmaterial Kurzbiographien von Verwaltungsbeamtinnen und -beamten zu erstellen und diese im Internet zu veröffentlichen, muss nach der geltenden Rechtslage ebenfalls unterbleiben. Auch für diese Datenübermittlung fehlt es bislang an der erforderlichen Rechtsgrundlage.

Veröffentlichungen von Archivgut mit personenbezogenen Daten sollten durch eine Vorschrift im Archivgesetz ermöglicht werden. Hier sollte – unter Wahrung der berechtigten Interessen der betroffenen Personen – festgelegt werden, ob und unter welchen Voraussetzungen Archive befugt sind, die Daten zu veröffentlichen. Dabei ist insbesondere auch zu regeln, welche Art von Daten welcher Personengruppen zu welchem Zweck veröffentlicht werden dürfen.

17 Kommunales

17.1 Immer gleich der ganze Kaufvertrag?

Wer ein Grundstück verkauft, hat der Gemeinde den Inhalt des Kaufvertrags mitzuteilen, um dieser die Prüfung eines etwaigen Vorkaufrechts zu ermöglichen. In der Praxis wird diese Pflicht häufig durch die beurkundenden Notarinnen und Notare erledigt. Muss aber hierzu der Gemeinde immer gleich der gesamte Kaufvertrag vorgelegt werden?

Das Grundbuchamt darf die Käuferin oder den Käufer eines Grundstücks erst dann in das Grundbuch eintragen, wenn die Gemeinde bestätigt hat, dass ein Vorkaufsrecht nicht besteht oder nicht ausgeübt wird. In vielen Fällen verlangen Gemeinden neben den erforderlichen Angaben zum Grundstück zumindest auch die Bekanntgabe des Namens und der Adresse der Erwerberin oder des Erwerbers, bevor sie die erforderliche Bescheinigung für das Grundbuchamt ausstellt. Oftmals wird auch die vollständige Vorlage des Kaufvertrages eingefordert. Für eine erste Prüfung, ob ein gemeindliches Vorkaufsrecht besteht, sind aber lediglich **Angaben zum Grundstück** erforderlich. Erst in einer zweiten Stufe, wenn die Gemeinde das Vorliegen eines Vorkaufsrechts feststellt und ein ernsthaftes Interesse an dem Grundstück bekundet hat, ist die Bekanntgabe weiterer Daten und die Vorlage des Kaufvertrages notwendig und zulässig.

Das Justizministerium und das Ministerium für Städtebau und Wohnen, Kultur und Sport des Landes Nordrhein-Westfalen haben sich dieser Rechtsauffassung angeschlossen und in ihren Geschäftsbereichen auf das vorstehend geschilderte zweistufige Mitteilungsverfahren hingewiesen.

17.2 Missbrauch des Fahrzeugregisters

In den Fahrzeugregistern der Zulassungsbehörden sind eine Vielzahl personenbezogener Daten gespeichert. Doch nicht immer ist auch eine Auskunft aus dem Register – etwa zur Ermittlung der Halterin oder des Halters eines Fahrzeugs – zulässig.

Halterauskünfte aus dem Fahrzeugregister dürfen die Zulassungsbehörden zur Verfolgung von **Rechtsansprüchen** nur im Zusammenhang mit Ansprüchen aus dem Straßenverkehr, zur Durchsetzung öffentlich-rechtlicher Ansprüche sowie zur Geltendmachung von übergegangenen Ansprüchen nach

dem Unterhaltsvorschussgesetz oder dem Bundessozialhilfegesetz erteilen (§ 39 Straßenverkehrsgesetz – StVG –).

Ein Rechtsanwalt hatte unter dem Stichwort „Verkehrsunfallsache" eine Halterauskunft beantragt, um das Vorhandensein eines Fahrzeugs zu ermitteln. Tatsächlich diente die erteilte Halterauskunft aber nicht zur Durchsetzung einer Forderung im Zusammenhang mit einem Verkehrsunfall, sondern der Pfändung des Fahrzeugs wegen einer mietrechtlichen Forderung seines Mandanten. Eine derartige Auskunft ist als **Erschleichen personenbezogener Daten** nach § 43 Abs. 2 Nr. 4 BDSG als Ordnungswidrigkeit einzustufen und wurde entsprechend geahndet.

Zusätzlich wurden die Anwaltskammern im Land Nordrhein-Westfalen gebeten, ihre Mitglieder über die Rechtslage zu informieren, um bereits im Vorfeld datenschutzrechtliche Verstöße zu vermeiden. Das Justizministerium wurde ebenfalls unterrichtet.

17.3 Veröffentlichung von Daten der Ratsmitglieder im Internet

Mitunter beschweren sich Ratsmitglieder darüber, dass ihre persönlichen Daten auf den Internetseiten einer Gemeinde veröffentlicht werden. Sie machen geltend, dass ihr Interesse am Schutz der Privatsphäre dem Informationsbedürfnis der Öffentlichkeit vorgehe. Es sei nicht einzusehen, warum beispielsweise Privatanschrift und Privattelefonnummer der Ratsmitglieder weltweit abrufbar sein müssten.

Die Vorschrift des § 43 Abs. 3 Satz 4 Gemeindeordnung des Landes Nordrhein-Westfalen (GO NW)erlaubt allerdings, dass Name, Anschrift, der ausgeübte Beruf sowie andere vergütete und ehrenamtliche Tätigkeiten der Ratsmitglieder veröffentlicht werden können. Über die Einzelheiten der Veröffentlichung entscheidet der Rat beziehungsweise die Bezirksvertretung. Dazu gehört auch die Möglichkeit, eine Veröffentlichung im Internet zu beschließen. Der Wortlaut des § 43 Abs. 3 Satz 4 GO NW enthält keine Beschränkung auf die bisher üblichen Medien wie Amtsblatt oder lokale Presse. Der Sinn und Zweck der Regelung, **Transparenz** für die Bürgerinnen und Bürger zu schaffen, um mögliche Interessenkollisionen bei der Ausübung des kommunalen Mandats offen zu legen, spricht vielmehr dafür, ein Medium zu wählen, dass von möglichst vielen Bürgerinnen und Bürgern wahrgenommen wird. Dies ist schon heute – und zukünftig

vermutlich noch mehr – das Internet, insbesondere die jeweilige Homepage einer Kommune.

Allerdings haben die Kommunen im Rahmen ihrer technischen Möglichkeiten darauf hinzuwirken, dass die veröffentlichten Informationen nicht mithilfe einer Internet-Suchmaschine auswertbar sind. Anderenfalls würde das Ziel des Gesetzgebers, Transparenz zu schaffen, über das erforderliche Maß hinaus überdehnt. Auch erlaubt § 43 Abs. 3 Satz 4 GO NW nicht, dass neben den Privatadressen auch die Privattelefonnummern der Ratsmitglieder veröffentlicht werden. Die Bekanntgabe der privaten Telefonnummer ist deshalb nur mit Einwilligung der Betroffenen zulässig.

Der Rat oder die Bezirksvertretung können beschließen, dass Name, Anschrift, der ausgeübte Beruf sowie andere vergütete und ehrenamtliche Tätigkeiten der Ratsmitglieder im Internet veröffentlicht werden.

18 Ausländerinnen und Ausländer

18.1 Besucherkontrollen in Asylbewerberunterkünften

Wer Personen besuchen möchte, die in Asylbewerberunterkünften wohnen, sieht sich unterschiedlichen Kontrollen ausgesetzt.

Im Wesentlichen ließen sich folgende Verfahrensweisen zur Kontrolle der Besucherinnen und Besucher feststellen:

Eine **Ausweiskontrolle,** die in Ausübung des Hausrechts zur Aufrechterhaltung der Sicherheit und Ordnung in den Unterkünften erfolgt, ist grundsätzlich zulässig. Dies gilt auch für das Führen von **Besucherbüchern oder -listen**, soweit ihr Zweck auf die Kontrolle beschränkt bleibt, ob am Abend alle Besucherinnen und Besucher die Unterkunft wieder verlassen haben. Diese Daten müssen spätestens nach dem Verlassen der Unterkunft wieder gelöscht werden. Dagegen ist die bei einigen Asylbewerberunterkünften festgestellte befristete Aufbewahrung eines **Identitätspapiers** oder das Notieren von **KFZ-Kennzeichen** im Bereich von Asylbewerberunterkünften nicht vom Hausrecht oder bestehenden Rechtsvorschriften gedeckt und deshalb **unzulässig**. Dies gilt schließlich auch für die in einigen Unterkünften praktizierte überflüssige **Weitergabe von Besucherdaten** an andere Stellen wie etwa an das Ordnungs- oder das Sozialamt.

Erfreulicherweise ist das Innenministerium des Landes Nordrhein-Westfalen der datenschutzrechtlichen Empfehlung gefolgt und hat die Betreiberinnen und Betreiber von Asylbewerberunterkünften angewiesen, bei Zugangskontrollen von Besucherinnen und Besuchern nicht datenschutzgerechte Maßnahmen einzustellen.

18.2 Bedenkliche Ausschreibungspraxis im Schengener Informationssystem

Bundesweit koordiniert wurde die Ausschreibungspraxis in der Europäischen Datenbank des Schengener Informationssystems zur Einreiseverweigerung abgeschobener Drittausländerinnen und -ausländer (Nicht-EU-Angehörige) einer datenschutzrechtlichen Prüfung unterzogen.

Auf der Grundlage des Art. 96 Abs. 3 des Schengener Durchführungsübereinkommens (SDÜ) können Ausländerinnen und Ausländer auf Antrag einer Ausländerbehörde im Schengener Informationssystem zum Zweck der Einreiseverweigerung ausgeschrieben werden, wenn sie ausgewiesen, zurückgewiesen oder abgeschoben worden sind und ein Einreiseverbot besteht (ausführliche Informationen über das Schengener Informationssystem enthält der 14. Datenschutzbericht 1999 unter 3.7, S. 66 ff). Spätestens nach 3 Jahren ist nach Art. 112 Abs. 1 SDÜ die **Erforderlichkeit der weiteren Speicherung** zu prüfen und regelmäßig die Löschung der personenbezogenen Daten zu veranlassen. Bereits im 15. Datenschutzbericht 2001 wurde unter 8.2, S. 93 ff, darauf hingewiesen, dass entsprechende Ausschreibungen im Schengener Informationssystem häufig ohne Rechtsgrundlage erfolgen und Löschungsfristen missachtet werden.

Nunmehr wurde auf Veranlassung der Gemeinsamen Kontrollinstanz für Schengen die Ausschreibungspraxis nach Art. 96 SDÜ stichprobenweise kontrolliert. Bei der bundesweit koordinierten datenschutzrechtlichen Prüfung wurden in Nordrhein-Westfalen von 36 Ausländerbehörden die Akten von insgesamt 80 Prüffällen angefordert. In 5 Fällen war eine Ausschreibung lediglich zum Zwecke der **Aufenthaltsermittlung** und somit **ohne Rechtsgrundlage** erfolgt. Hier wurde jeweils die sofortige Löschung der Daten veranlasst. Außerdem wurde deutlich, dass in vielen Fällen keine hinreichende Dokumentation und Kontrolle der Ausschreibungsdauer erfolgt.

Aus dem Prüfungsergebnis ist ersichtlich, dass bisher an der mangelhaften Ausschreibungspraxis nur wenig verbessert wurde.

19 Finanzen

19.1 Gläserne Steuerpflichtige durch das Steueränderungsgesetz

Die Steuergesetzgebung der letzten Zeit ist immer undurchsichtiger geworden. Auch ist kaum aufgefallen, dass durch die vorgenommenen Änderungen auf elektronischem Weg die gläsernen Steuerpflichtigen entstehen werden. Zusätzlich sind Sicherheitslücken bei elektronischen Steuererklärungen bekannt geworden.

So sieht das Steueränderungsgesetz 2003 scheinbar kleine Veränderungen im steuerlichen Verfahren vor, die der elektronischen Erfassung aller Steuerfälle und damit dem Ausbau der Kontrollsysteme zur Vermeidung von Steuerhinterziehung dienen. Weitreichende Folgen kann die nach Erlass einer Rechtsverordnung vorgesehene Einführung einheitlicher steuerlicher Identifikationsmerkmale haben. Künftig erhält jede Person, die in Deutschland wohnt oder ihren gewöhnlichen Aufenthalt hat, ab der Geburt ebenso wie jedes Wirtschaftsunternehmen und jede wirtschaftlich tätige Person eine lebenslang und bundesweit geltende **Identifikationsnummer** (§§ 139 a bis c Abgabenordnung). Diese wird zentral beim **Bundesamt für Finanzen** (BfF) und zusätzlich in den örtlichen Melderegistern gespeichert. Damit sichergestellt wird, dass eine Person nur eine Identifikationsnummer erhält, darf das BfF eine Vielzahl von Daten speichern. (zum Beispiel: Familiennamen, frühere Namen, Vornamen, Tag der Geburt, Anschrift). Vorgesehen ist, dass das BfF diese Daten von den Meldebehörden erhält, die ihrerseits die zugeteilten Identifikationsnummern für die in ihrem Zuständigkeitsbereich gemeldeten Personen in den Meldedatensätzen speichern. Im Gegensatz zur bisherigen getrennten Zuordnung können nun zentral die verschiedenen Steuernummern der unterschiedlichen Besteuerungsverfahren (beispielsweise Erbschafts-, Vermögenssteuer) eindeutig den Steuerpflichtigen zugeordnet werden. Aus rein steuerrechtlicher Sicht mag dies eine verständliche Regelung sein. Aber dadurch entstünde erstmals ein **zentrales Einwohnerregister beim Bundesamt für Finanzen.**

Darüber hinaus stellt die vorgesehene bundesweite Speicherung von Identifikationsnummern zu jeder Person bei den örtlichen Melderegistern eine – gemessen an der Rechtsprechung des Bundesverfassungsgerichts – bedenkliche Regelung dar. Nach seiner gefestigten Rechtsprechung ist eine unbeschränkte Verknüpfungsmöglichkeit von bei den Verwaltungsbehörden vorhandenen Datenbeständen durch ein einheitliches **Personenkennzeichen** als

unzulässig anzusehen (vgl. BVerfGE 65, 1/53 und die Entschließung vom 25./26. März 2004, Abdruck im Anhang, Nr. 18). Eine Registrierung unter einer zentralen Nummer verträgt sich nur dann mit dem Recht auf informationelle Selbstbestimmung, wenn sie an einen eng begrenzten Zweck gebunden ist.

Hier liegt aber das Problem der neuen Regelung, denn die erforderliche strenge Zweckbindung ist in mehrfacher Hinsicht zweifelhaft. Die einheitliche Identifikationsnummer dient dem Aufbau eines zentralen Registers der Gesamtbevölkerung der Bundesrepublik Deutschland. Die Totalerfassung bezieht sich sogar auf Säuglinge, die größten Teils nicht steuerpflichtig sind. Das **Melderegister** ist zugleich aufgrund melderechtlicher Vorschriften unter bestimmten Voraussetzungen zur Auskunft gegenüber anderen Behörden und öffentlichen Stellen verpflichtet. Die dort gespeicherten Daten können sogar online von anderen öffentlichen Stellen abgerufen werden. Zur Zeit ist dem Melderegister noch die Beschränkung auferlegt, die Identifikationsnummer nur an das Bundesamt für Finanzen zu übermitteln. Trotzdem erheben sich ernsthafte Bedenken gegen die generalklauselartige Zweckbindungsregelung, nach der die Finanzbehörden die Identifikationsnummer lediglich erheben und verwenden dürfen, soweit dies „zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist oder eine Rechtsvorschrift die Erhebung und Verwendung der Identifikationsnummer ausdrücklich erlaubt oder anordnet". Die Erhebung und Verwendung der Identifikationsnummer durch andere öffentliche, aber auch nicht öffentliche Stellen soll zwar nur für Datenübermittlungen zwischen ihnen und den Finanzbehörden zugelassen sein (§ 139 b Abs. 2 AO). Allerdings wird allein diese Regelung dazu führen, dass die steuerliche Identifikationsnummer künftig bei einer Vielzahl von Behörden und öffentlichen wie auch nicht öffentlichen Stellen gespeichert sein wird. Dann aber dürfte die Einhaltung der Zweckbindung kaum noch kontrollierbar sein.

Das Gesetz zur Förderung der Steuerehrlichkeit vom 23.12.2003 enthält mit den §§ 93 Abs. 7, 8 und 93 b AO **Regelungen zu Kontenkontrollen**, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maß beschränken. Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung vorgehalten werden müssen. Dabei handelt es sich

um Kontostammdaten wie zum Beispiel Name, Geburtsdatum, Kontonummern. Neben Finanzbehörden sollen nunmehr auch andere Behörden, zum Beispiel die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuerrechts" anknüpft und eigene Ermittlungen dieser Behörde nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, lässt das Gesetz offen. Auch die sonstigen Datenerhebungsvoraussetzungen sind nicht präzisiert. Dem **Transparenzgebot** widerspricht es im Übrigen, dass Betroffene von Abfragen, die zu keinem Ergebnis geführt haben, nichts erfahren sollen. Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss diese staatliche Kontenkontrolle auf den Prüfstand. Sie haben den Gesetzgeber daher aufgefordert, die diesbezüglichen Vorschriften der Abgabenordnung mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten (Entschließung vom 26. November 2004, Abdruck im Anhang, Nr. 24).

Mit einem gewissen Sicherheitsrisiko sollen Gewerbetreibende ab dem 01.01.2005 ihrer Verpflichtung nachkommen, die **Umsatzsteuer- und Lohnsteuer-Anmeldungen** nur noch auf elektronischem Weg an das zuständige Finanzamt zu übermitteln. Der Fiskus stellt hierfür kostenlos die Software in dem Verfahren **ELSTER** „**El**ektronische **Steuererklärung**" zur Verfügung. Mit diesem Verfahren wird bisher allerdings keine Authentifizierung angeboten, die die sichere Identifizierung der Steuerpflichtigen erlaubt, so dass missbräuchliche Antragstellungen durch Dritte möglich sind. Mittelfristig soll aber ein Authentifizierungsverfahren eingerichtet werden. Es bleibt abzuwarten, ob hiermit Manipulationen unmöglich werden.

- **Die bundesweit geltende steuerliche Identifikationsnummer darf nicht zu einem verfassungsrechtlich unzulässigen Personenkennzeichen werden. Ist die Identifikationsnummer mit einem so weitgesteckten Verbreitungsgrad erst einmal eingeführt, dürfte der Schritt, sie auch in anderen Verwaltungsbereichen als allgemeine Personenkennziffer nutzbar zu machen, nicht mehr weit sein. Es muss daher noch gründlicher geprüft werden, wie eine strikte Eingrenzung einer künftigen steuerlichen Identifikationsnummer auf den Steuerbereich erreicht werden kann.**

- **Die Regelungen zu Kontenkontrollen gemäß §§ 93 Abs. 7, 8 und 93 b AO müssen gesetzlich nachgebessert werden. Der Gesetzgeber bleibt**

aufgefordert, für normenklare, dem Transparenzgebot entsprechende Datenschutzvorschriften zu sorgen.

- In dem elektronischen Verfahren der Umsatz- und Lohnsteueranmeldungen muss die Datensicherheit gewährleistet sein. Das Verfahren darf nur zum Einsatz gelangen, sofern geeignete Authentifizierungsverfahren vorhanden sind.

19.2 Das Recht der Steuerpflichtigen auf Akteneinsicht – nur im Ermessen der Finanzbehörden?

Die Steuerpflichtigen werden zwar immer gläserner, ein Informationsrecht über die zu ihrer eigenen Person gespeicherten Daten wird ihnen von den Finanzämtern jedoch nach wie vor oft verwehrt.

Trotz der grundlegenden Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung lehnt die Finanzverwaltung den grundsätzlich bestehenden Anspruch der Steuerpflichtigen auf Einsichtnahme in die über sie geführten **Steuerakten** immer noch in vielen Fällen ab. Während das Auskunfts- und Akteneinsichtsrecht in anderen Bereichen öffentlicher Verwaltung – wenn auch in unterschiedlichem Umfang – besteht, liegt in Besteuerungsverfahren die begehrte Einsichtnahme in die eigene Steuerakte im Ermessen der Finanzbehörden – ein verfassungsrechtlich unhaltbarer Zustand.

Im Rahmen einer datenschutzgerechten Novellierung der Abgabenordnung, wie sie wiederholt und zuletzt in der Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 (Abdruck im Anhang, Nr. 2) gefordert wurde, sollte ein **Auskunfts- und Akteneinsichtsrecht** bereichsspezifisch geregelt werden, damit es nicht bei einer bloßen Ermessensentscheidung bleibt. Ein erster vom Bundesfinanzministerium verfasster Novellierungsvorschlag enthält noch Unklarheiten, die in der Praxis zu unterschiedlichen Auslegungen führen werden. Insbesondere wird nur ein Anspruch auf Auskunft über die zur Person der oder des Auskunftssuchenden gespeicherten Daten gewährt. Danach wäre keine Auskunft zu erteilen über wichtige Angaben wie Herkunft, Empfängerinnen und Empfänger der Daten sowie den Zweck der Speicherung. Außerdem soll die Finanzbehörde über die Form der Auskunftserteilung – ob durch Einsicht in Unterlagen, schriftliche Auskunft oder Übersendung von Kopien – wiederum nach ihrem Ermessen entscheiden. Besser wäre es, wenn die Finanzbehörde nur dann eine andere

als die gewünschte Form der Auskunft wählen dürfte, wenn hierfür ein wichtiger Grund vorläge.

Das Recht auf Auskunft und Akteneinsicht im Steuerverfahren muss daher als gerichtlich voll nachprüfbarer Rechtsanspruch ausgebildet sein.

20 Statistik

20.1 Mikrozensus

Anfragen von Bürgerinnen und Bürgern zu den jährlich wiederkehrenden repräsentativen Befragungen nach dem Mikrozensusgesetz lassen erkennen, dass Betroffene nicht immer vollständig über die Rechtsgrundlagen dieser Erhebungen informiert sind.

Die Mikrozensuserhebungen über die Bevölkerung, den Arbeitsmarkt und die Wohnsituation von Haushalten werden in den Jahren 2005 bis 2012 auf Grund der **Neufassung des Mikrozensusgesetzes** (MZG) vom 24.06.2004 (BGBl. I S. 1350) durchgeführt. Sie erfolgen auch weiterhin durch Befragungen von Bürgerinnen und Bürgern in Haushalten. Diese werden auf der Grundlage von Auswahlbezirken ausgewählt, die ihrerseits durch mathematische Zufallsverfahren bestimmt werden. Die bisher regelmäßig einmal jährlich durchgeführten Erhebungen werden künftig gleichmäßig über die Kalenderwochen verteilt. Diese Neuerung soll zu deutlich aktuelleren Ergebnissen als bisher führen. Für die von der Erhebung betroffenen Personen bedeutet dies jedoch keine Veränderung in der Häufigkeit der Befragung.

Um Bürgerinnen und Bürgern das Ausfüllen der Erhebungsvordrucke zu erleichtern, werden vom Landesamt für Datenverarbeitung und Statistik (LDS) **Erhebungsbeauftragte** eingesetzt. Diese sind ebenso wie die mit der Auswertung der Mikrozensus-Erhebungen betrauten Beschäftigten des LDS nach dem Bundesstatistikgesetz zur Verschwiegenheit verpflichtet. Es wird darauf geachtet, dass die Erhebungsbeauftragten nicht in unmittelbarer Nähe des eigenen Wohnortes eingesetzt werden. Sollte ihre Hilfe nicht in Anspruch genommen werden, kann ein Erhebungsbogen auch selbst ausgefüllt und dem LDS im verschlossenen Umschlag übersandt werden.

Häufig wird gefragt, ob die Teilnahme an der Mikrozensusbefragung verbindlich ist und welche Rechtsfolge eine eventuelle Nichtteilnahme nach sich ziehen kann. Ebenso wie bisher besteht auch künftig eine grundsätzliche **Auskunftspflicht**. Lediglich einzelne Auskünfte über bestimmte Erhebungs- und Hilfsmerkmale sind freiwillig. Eine Verletzung der Auskunftspflicht stellt allerdings keine Ordnungswidrigkeit dar, so dass sie nicht mit einem Bußgeld geahndet werden kann.

Informationen zu Erhebungen nach dem Mikrozensusgesetz werden demnächst auf der Homepage erscheinen (www.ldi.nrw.de).

20.2 Forschungsdatenzentrum der Statistischen Landesämter

Die Statistischen Landesämter beabsichtigen eine Projektzusammenarbeit durch die Einrichtung eines so genannten Forschungsdatenzentrums, wobei jedes Landesamt einen regionalen Standort bilden soll, der die in den einzelnen Bundesländern erhobenen Statistikdaten eines Fachbereichs zentralisiert bereithält.

Ziel dieses Projekts, das auf einer Empfehlung der vom Bundesministerium für Bildung und Forschung eingesetzten Kommission zur Verbesserung der informationellen Infrastruktur zwischen **Wissenschaft** und **Statistik** beruht, ist, der Wissenschaft Statistikdaten vereinfacht zugänglich zu machen.

Die Statistischen Landesämter sind bisher nur zur Bereitstellung der von ihnen in ihrem **regionalen Zuständigkeitsbereich** erhobenen Statistikdaten befugt. Hochschulen oder sonstige Einrichtungen, die mit der Aufgabe unabhängiger wissenschaftlicher Forschung betraut sind, konnten diese Daten daher immer nur bei den einzelnen Statistischen Landesämtern getrennt abfragen, was sich als sehr zeitintensiv erwies.

Neben der zentralisierten Bereitstellung sollten die Statistikdaten ursprünglich außerdem in **nicht-anonymisierter** Form durch die Einrichtung von so genannten Gastarbeitsplätzen für Wissenschaftlerinnen und Wissenschaftler bei den Statistischen Landesämtern zur Verfügung gestellt werden. Das Bundesstatistikgesetz und die entsprechenden Landesstatistikgesetze sehen jedoch ausschließlich die Bereitstellung von **faktisch-anonymisierten** Statistikdaten vor, die nur mit einem unverhältnismäßig großen Aufwand personenbezogen zugeordnet werden können. Auf die von Datenschutzbeauftragten geäußerten Bedenken, dass mit der Preisgabe der personenbezogenen Daten der Befragten ein unverhältnismäßiger Eingriff in ihr Recht auf informationelle Selbstbestimmung verbunden sei, der auch nicht unter Berufung auf das Grundrecht der Freiheit von Wissenschaft und Forschung gerechtfertigt werden könne, haben die Statistischen Landesämter von diesem Vorhaben Abstand genommen.

Da aber auch die Übermittlung der Statistikdaten an die jeweils fachlich zuständige Regionalstelle eine grundlegende Veränderung der in den Statistikgesetzen geregelten Aufgabenzuständigkeiten der Statistischen Landesämter bedeutet, bedarf es hierfür einer normenklaren, bisher nicht vorhandenen **Rechtsgrundlage**.

Im Hinblick auf den von der Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik aufgezeigten notwendigen Änderungsbedarf lassen sich die datenschutzrechtlichen Bedenken allenfalls für die Dauer einer regional und zeitlich eingeschränkten Testphase zurückstellen. Dabei sollte ebenfalls ein Modell getestet werden, bei dem eine zentrale Datenspeicherung auf Vorrat bei einem Statistischen Landesamt nicht erforderlich ist, sondern die Daten nur im Einzelfall für ein konkretes Forschungsvorhaben zur Verfügung gestellt werden.

21 Internationaler Datenverkehr

International agierenden Unternehmen, die personenbezogene Daten an Stellen außerhalb des Europäischen Wirtschaftsraumes in so genannte Drittstaaten übermitteln wollen, stehen verschiedene Handlungsalternativen zur Verfügung. Die Einzelheiten einer zulässigen Datenübermittlung in Drittstaaten sind ausführlich im 16. Datenschutzbericht 2003 dargestellt.

Zu ergänzen ist, dass die Europäische Kommission in der Zwischenzeit weitere **Angemessenheitsentscheidungen** getroffen hat und zwar für Argentinien sowie für die Kanalinseln Guernsey und Isle of Man, so dass Datenübermittlungen an Stellen in diesen Ländern unter den selben Voraussetzungen möglich sind wie an eine vergleichbare Stelle im Inland. Die Kommissionsentscheidungen sind im Internet unter www.europa.eu.int zu finden.

Durch den **Beitritt** der Staaten Estland, Litauen, Malta, Polen, Slowakei, Slowenien, Tschechien, Ungarn und Zypern **zur Europäischen Union** am 01. Mai 2004 sind gemäß § 4b Abs. 1 Nr. 1 BDSG Übermittlungen von personenbezogenen Daten an Stellen in diesen Staaten datenschutzrechtlich im Wesentlichen den Datenübermittlungen im Inland gleichgestellt.

Ein bei internationalen Konzernen zunehmend beliebtes Instrument, um bei Datenübermittlungen in Drittstaaten Garantien für die Persönlichkeitsrechte der Betroffenen abzugeben, sind **verbindliche Unternehmensregelungen**. Nach Daimler Chrysler und der Musterunternehmensreglung des Gesamtverbandes der Deutschen Versicherungswirtschaft haben inzwischen die Telekom und der Konzern General Electric Regelungen vorgelegt, die die deutschen Datenschutzaufsichtsbehörden als geeignete Grundlage für Datenübermittlungen in Drittstaaten ansehen. Das Verfahren zur Begutachtung der Unternehmensregelung von General Electric wurde von der LDI koordiniert, da ein Schwerpunkt der Geschäftstätigkeit des Konzerns in Nordrhein-Westfalen liegt. Bisher konnten 16 Genehmigungen gemäß § 4c Abs. 2 BDSG für in Nordrhein-Westfalen ansässige Unternehmen des General Electric Konzerns erteilt werden, die personenbezogene Daten auf der Basis der Unternehmensregelung an Stellen in den USA übermitteln.

Für Konzerne dürfte von großem Interesse sein, dass das in Deutschland bewährte Koordinierungsverfahren der Aufsichtsbehörden für die daten-

schutzrechtliche Bewertung von verbindlichen Unternehmensregelungen nun auch auf europäischer Ebene Schule zu machen scheint. Die Datenschutzkontrollstellen in den Staaten der Europäischen Union bemühen sich um eine **koordinierte Prüfung von Unternehmensregelungen**. Konzerne, die in mehreren europäischen Staaten tätig sind und Drittstaatenübermittlungen auf eine Konzerndatenschutzregelung stützen wollen, sollten sich wegen der Anerkennung der Regelung durch alle oder mehrere EU-Mitgliedstaaten mit der Datenschutzbehörde am europäischen Hauptsitz ihres Konzerns in Verbindung setzen. Soweit es keinen Hauptsitz gibt, sollte die Behörde in dem Staat angesprochen werden, wo der Schwerpunkt der Geschäftstätigkeit des Konzerns liegt.

22 Behördliche und betriebliche Datenschutzbeauftragte

22.1 Datenschutzbeauftragte bei öffentlichen Stellen

Die Datenschutzbeauftragten aus den verschiedenen Bereichen der nordrhein-westfälischen Verwaltungen sind aktiv und haben vielfältige Probleme vor Ort zu lösen. Eine Fragestellung war dabei von ganz grundsätzlicher Bedeutung: Was ist der Unterschied zwischen einem Abrufverfahren und einer Verbunddatei?

Die Verantwortlichen in den Verwaltungen wollen zunehmend die einmal in ihrer Institution vorhandenen Daten zur Erfüllung unterschiedlicher Aufgaben nutzen. Das datenschutzrechtliche Gebot der **Trennung** von Datenbeständen aus **verschiedenen Aufgabenbereichen** muss gleichwohl beachtet werden. Für das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger ist die Gewährleistung eines angemessenen Schutzes der personenbezogenen Daten bei der Mehrfachnutzung von Datenbeständen von besonderer Bedeutung. Das DSG NRW eröffnet mit der Verbunddatei in § 4a und dem automatisierten Abrufverfahren in § 9 zwei verschiedene Wege, die der Verwaltung die Nutzung eines Datenbestandes zur Erfüllung verschiedener Aufgabenstellungen ermöglichen. In der Verwaltungspraxis stellt sich dabei immer wieder die Frage nach dem Verhältnis dieser beiden Vorschriften zueinander.

Das **automatisierte Abrufverfahren nach § 9 DSG NRW** bezieht sich auf Sachverhalte, in denen es eine verantwortliche Stelle gibt, die einen Datenbestand pflegt. Die weiteren beteiligten Stellen sind befugt, zur Erfüllung ihrer Aufgaben unter bestimmten Voraussetzungen für eigene Zwecke Daten durch Abruf zu erheben. Sie arbeiten ansonsten jedoch nicht unmittelbar mit oder in der Datenbank, aus der der Abruf möglich ist. Aus der Sicht der den Datenbestand pflegenden Stelle stellt der Abruf grundsätzlich eine Übermittlung an die abrufende Stelle dar. Die übermittelnde Stelle hat aber aufgrund der Funktionsweise eines Abrufverfahrens nicht die Möglichkeit, im Einzelfall eine Missbrauchskontrolle durchzuführen wie sie nach § 14 Abs. 2 DSG NRW vorgesehen ist. Das Fehlen der Missbrauchskontrolle im Abrufverfahren bedeutet ein erhöhtes Gefährdungspotential für die Persönlichkeitsrechte der Betroffenen. Deshalb verlangt § 9 DSG NRW klare gesetzliche Regelungen für die Einrichtung von Abrufverfahren.

Demgegenüber sind **Verbunddateien nach § 4a DSG NRW** solche Dateien, in denen mehrere öffentliche Stellen gemeinsam Daten in einer Weise verarbeiten, die über den bloßen Abruf hinausgeht. Dies wird dadurch deutlich, dass das Gesetz die Festlegung einer verantwortlichen Stelle vorschreibt. Das ist bei einem Abrufverfahren nicht erforderlich, weil eine klare Zuordnung der den Datenbestand pflegenden Stelle möglich ist. Charakteristisch für eine Verbunddatei ist, dass sie die datenschutzrechtlichen Berechtigungen abbildet, die im Verhältnis der beteiligten Stellen untereinander bestehen. Jede beteiligte Stelle kann nur auf die Daten und in dem Umfang zugreifen wie dies auch außerhalb des automatisierten Verfahrens möglich wäre. Ist etwa die regelmäßige Übermittlung bestimmter Datensätze gesetzlich erlaubt oder vorgeschrieben, können die entsprechenden Datensätze mehreren Stellen gemeinsam zur Verfügung stehen. Ist hingegen eine Stelle nur im Einzelfall, also beim Vorliegen besonderer Voraussetzungen, befugt, von der anderen Stelle Daten zu erfragen, kann dieser Stelle auch nicht der generelle Zugriff auf alle Daten der anderen Stelle eingeräumt werden, weil ansonsten § 14 Abs. 2 DSG NRW im Verfahren nicht abgebildet würde. Vielmehr kann dann eine elektronische Datenabfrage im Einzelfall nur zugelassen werden, wenn es einen Verfahrensschritt gibt, in dem diejenige Stelle, die über die Daten verfügt, den Zugriff auf den einzelnen Datensatz willentlich autorisiert.

Denkbar ist etwa die Einrichtung eines Verbundverfahrens, in dem verschiedene Fachabteilungen einer Behörde arbeiten. So ist es zum Beispiel in der Verwaltungspraxis nicht unüblich, ein Verbundverfahren einzurichten zwischen der Kasse einer öffentlichen Stelle und den Fachabteilungen, die Auszahlungen veranlassen oder deren Tätigkeit zu Einnahmen führt. Hierbei ist zu beachten, dass die **Zweckbindungsgrundsätze** des § 13 DSG NRW im Verfahren abgebildet werden müssen.

Verbunddatei und automatisiertem Abrufverfahren ist gemeinsam, dass vor der Inbetriebnahme der Verfahren gemäß § 10 DSG NRW ein **Sicherheitskonzept** erstellt und eine **Vorabkontrolle** durchgeführt werden muss.

Verbunddateien müssen so aufgebaut sein, dass die Datenverarbeitungsbefugnisse der beteiligten Stellen exakt abgebildet sind. Automatisierte Abrufverfahren bedürfen einer gesetzlichen Grundlage, weil eine Missbrauchskontrolle im Sinne des § 14 Abs. 2 DSG NRW in Abrufverfahren fehlt und diese Verfahren damit ein erhöhtes Gefährdungspotential für die betroffenen Personen darstellen.

22.2 Betriebliche Datenschutzbeauftragte

§ 4f BDSG schreibt vor, dass private Stellen, in denen mehr als vier Beschäftigte personenbezogene Daten automatisiert verarbeiten, betriebliche Datenschutzbeauftragte bestellen müssen. Diese Verpflichtung bereitet kleineren Unternehmen oder Stellen manchmal praktische Schwierigkeiten.

Das System der betrieblichen Datenschutzbeauftragten hat in Deutschland eine lange Tradition. Dennoch erhielten im Frühjahr/Sommer 2004 viele – vornehmlich kleine – Unternehmen und Daten verarbeitende Stellen Post, in der auf die vermeintlich neue Verpflichtung zur Bestellung von betrieblichen Datenschutzbeauftragten gemäß § 4f BDSG hingewiesen wurde. Geworben wurde häufig für Datenschutzschulungen und es wurden Angebote für die Tätigkeit als externe Datenschutzbeauftragte gemacht. Auch wenn manche dieser Schreiben in unseriöser Weise eine gesetzliche Neuerung vortäuschten, haben sie offenbar viele Stellen wach gerüttelt, die sich ihrer Verpflichtung zur **Bestellung** einer oder eines Datenschutzbeauftragten bisher nicht bewusst waren. Die Anfragen zur Bestellungspflicht stiegen sprunghaft an.

Zu Tage trat aber auch, dass gerade kleine Unternehmen, die die Voraussetzung des § 4f BDSG – mehr als vier Beschäftigte verarbeiten Daten automatisiert – nur knapp überschreiten, Schwierigkeiten mit der Bestellungspflicht haben. Grundsätzlich ist die Möglichkeit der Bestellung externer Beauftragter gerade für diese Unternehmen oft eine praktikable Lösung, da sie häufig selbst nicht über Personal verfügen, das die für Datenschutzbeauftragte erforderliche fachliche Eignung hat. Hier kann eine externe Person, die mehrere ähnlich strukturierte Unternehmen betreut, kostengünstiger und fachlich qualifizierter arbeiten. Besondere Schwierigkeiten haben insbesondere Anwaltskanzleien, Apotheken, Steuerberatungsbüros, Ärzte und Ärztinnen. Diese Stellen sind vielfach nicht nur relativ klein, sondern sie unterliegen einer **beruflichen Schweigepflicht** und können deshalb nicht ohne weiteres externe Datenschutzbeauftragte bestellen. Aber auch diese Stellen können zu praktikablen Lösungen kommen, wenn sie etwa eine externe Datenschutzbeauftragte oder einen externen Datenschutzbeauftragten wählen und zugleich intern eine Person bei Datenschutzkontrollen im Einzelfall einsetzen. Das interne Personal ist regelmäßig auch an die Schweigepflicht gebunden und kann die Unterlagen einsehen, zu denen die oder der Datenschutzbeauftragte keinen Zugang erhalten kann.

Keinesfalls aber sind solche beruflichen Schweigepflichten unterliegende Stellen wegen ihrer Besonderheiten von der Pflicht zur Bestellung von Datenschutzbeauftragten oder gar von der Anwendung des BDSG insgesamt ausgenommen. Der Düsseldorfer Kreis hat sich mit einem Gutachten der **Bundesrechtsanwaltskammer** auseinandergesetzt, das für Anwaltskanzleien eine Ausnahme von den Regelungen des BDSG annimmt.

Diese Auffassung der Kammer ist nicht mit der Europäischen Datenschutzrichtlinie vereinbar, die keine Ausnahmen von der Anwendung ihrer grundsätzlichen Datenschutzprinzipien für Anwaltskanzleien oder eine der anderen oben erwähnten Berufsgruppen zulässt. Die Datenschutzprinzipien der Richtlinie sind durch das BDSG in innerstaatliches Recht umgewandelt. Der Düsseldorfer Kreis wird sich über diese Rechtsfrage mit der Bundesrechtsanwaltskammer auseinandersetzen.

23 Informationsfreiheit

23.1 Keine Flucht aus der Informationspflicht ins Privatrecht ermöglichen

Vor allem Kommunen erfüllen ihre Aufgaben auch in privatrechtlichen Rechtsformen. Die hierzu geschaffenen privatrechtlichen Organisationen verstehen sich nicht als öffentliche Stellen. Die Anwendbarkeit des Informationsfreiheitsgesetzes IFG NRW ist umstritten – eine unbefriedigende Rechtslage.

Grundsätzlich sind alle öffentlichen Stellen in Nordrhein-Westfalen verpflichtet, den Bürgerinnen und Bürgern Zugang zu den bei der jeweiligen Stelle vorhandenen Informationen zu gewähren. Hierzu gehören ohne Einschränkung auch öffentliche Unternehmen, die sich wirtschaftlich betätigen (zum Beispiel der Bau- und Liegenschaftsbetrieb NRW), weil sie öffentlich-rechtlich organisiert sind. Die Erfüllung öffentlicher Aufgaben wird jedoch vermehrt aus der Verwaltung **ausgegliedert** und durch rechtlich verselbständigte, privatwirtschaftlich organisierte Unternehmen wahrgenommen. Diese Unternehmen sind juristische Personen des privaten Rechts; daran ändert sich auch nichts, wenn sie ganz oder mehrheitlich einer Gemeinde oder einem Gemeindeverband gehören. Nach dem Wortlaut des Gesetzes ist nicht klar, ob sie trotzdem als öffentliche Stellen im Sinne des IFG NRW anzusehen sind.

Eine Auskunftspflicht juristischer Personen des Privatrechts besteht nach dem IFG NRW nur, soweit diese öffentlich-rechtliche Aufgaben wahrnehmen. Öffentlich-rechtliche Aufgaben sind solche, die der öffentlichen Verwaltung **gesetzlich zugewiesen** sind. Hierzu zählt auch der Verkauf öffentlicher Grundstücke durch eine privatrechtliche Verwertungsgesellschaft. Gleich, ob sie als privatrechtliche Gesellschaft einer Gemeinde oder in privater Trägerschaft fungiert, sie erfüllt nach wie vor eine öffentlich-rechtliche Aufgabe der Verwaltung, weil der Verkauf von Grundstücken der Gemeinde nach § 90 Gemeindeordnung zu den kommunalen Aufgaben zählt.

Soweit es jedoch einer öffentlich-rechtlichen Körperschaft frei steht, ob sie eine Aufgabe durch ihre Verwaltung oder – ausgelagert – in privatrechtlicher Organisationsform erfüllt, ist die Aufgabenwahrnehmung nicht mehr öffentlich-rechtlicher Natur. Solche Aufgaben gehören im Wesentlichen dem Bereich der freiwilligen Selbstverwaltung oder der **Daseinsvorsorge** an, wie etwa die Stromversorgung. Beispielsweise ist eine Kommune ge-

setzlich nicht verpflichtet, ein Hallenbad zu errichten und zu unterhalten, sondern dies gehört zur freiwilligen Selbstverwaltung. Sie kann das Bad daher durch ihre Verwaltung errichten und betreiben. Sie kann diese Aufgabe jedoch auch abgeben und durch eine Bädergesellschaft weiterführen lassen. Wenn die öffentliche Hand an dem Unternehmen beteiligt ist, maßgeblich dessen Entscheidungen beeinflusst und die Geschäftsergebnisse mitverantwortet, sollte der freie Zugang zu Informationen grundsätzlich gegeben sein.

Allerdings ist **streitig**, ob eine solche städtische GmbH auskunftspflichtig ist. Zum Teil wird in der Literatur hierzu die Meinung vertreten, dass es sich immer noch um eine öffentlich-rechtliche Aufgabenwahrnehmung handele, wenn sie gemeinwohlerheblich und vom Verwaltungsträger durch eigene Initiative zur öffentlichen Aufgabe gemacht worden sei. Ob er dazu einen Eigenbetrieb gründe oder sich einer Organisation in privatrechtlicher Form bediene, die er mehrheitlich beherrsche, könne keinen Unterschied machen. Danach wäre eine Auskunftspflicht anzunehmen. Die Gegenmeinung verneint eine Auskunftspflicht mit dem Argument, dass insoweit keine öffentlich-rechtliche Aufgabe wahrgenommen werde.

Der Streit über die Auslegung des § 2 Abs. 4 IFG NRW ist insbesondere deshalb misslich, weil häufig gerade jene öffentlichen Bereiche privatisiert werden, die über ein besonders großes Finanzvolumen verfügen – etwa die Energieversorgung oder Verkehrsbetriebe. Nach Sinn und Zweck des IFG NRW soll Transparenz insbesondere beim Umgang mit Steuermitteln gefördert werden. Diese Zielsetzung wird aber unterlaufen, wenn öffentliche Stellen sich ihrer **Informationspflicht** dadurch entziehen könnten, dass sie ihre Aufgabenwahrnehmung privatisieren. Dementsprechend haben die Informationsbeauftragten Deutschlands im Rahmen einer Entschließung vom 16. Dezember 2003 (Abdruck im Anhang Nr. II) gefordert, die Geltungsbereiche der Informationsfreiheitsgesetze auf alle Unterlagen, die im Zusammenhang mit der Tätigkeit von Staat und Verwaltung stehen, zu erstrecken – unabhängig von der Frage, ob öffentliche Aufgaben durch die öffentliche Hand selbst oder durch von ihr beherrschte private Unternehmen wahrgenommen werden.

Wegen der nach wie vor bestehenden Auslegungsschwierigkeiten ist eine gesetzlich klare Einbeziehung auch der privatrechtlichen Unternehmen mit Beteiligung öffentlicher Verwaltungsträger in den Anwendungsbereich des IFG NRW wünschenswert.

23.2 Bereichsspezifische Zugangsregelungen

23.2.1 Wann ist eine Zugangsregelung eine Zugangsregelung?

Häufig wird informationssuchenden Personen gleich zu Beginn die Vorrangregelung in § 4 Abs. 2 IFG NRW zu Unrecht als Stolperstein in den Weg gelegt. Hier sind oft langwierige Klärungsprozesse erforderlich.

So wehren sich pauschal die Finanzbehörden, die Industrie- und Handelskammern, die Deichverbände und zum Teil die Bauverwaltung dagegen, Informationen zugänglich zu machen. Es heißt dann immer, es gäbe eine bereichspezifische Regelung, die **Vorrang** vor dem IFG NRW hätte. Die dafür genannten Gründe lauten: Die Abgabenordnung sehe ein Zugangsrecht absichtlich nicht vor, das Bundesgesetz über die Industrie- und Handelskammern schließe die Anwendung der landesrechtlichen Informationsfreiheit aus. Gleiches wollten die Deichverbände aus dem Bundesgesetz über Wasser- und Bodenverbände lesen und die Bauverwaltung aus Teilen des Baugesetzbuches des Bundes.

Wann tatsächlich eine bereichsspezifische Zugangsregelung gegeben ist, die dem allgemeinen Informationszugang nach dem IFG NRW als verdrängende Spezialregelung vorgeht, bestimmt sich danach, ob beide Normen denselben **Regelungsgegenstand** haben und die bereichsspezifische Norm insoweit eine **abschließende** Regelung trifft. Ob eine identische Regelungsmaterie vorliegt, muss daran geprüft werden, ob sich beide Gesetze an denselben Adressatenkreis wenden und welcher Schutzzweck dabei verfolgt wird. Liegen diese Voraussetzungen vor, ist in einem weiteren Schritt zu prüfen, ob die bereichsspezifisch getroffene Regelung wirklich abschließend ist oder noch Raum für einen allgemeinen Informationszugang lässt.

Nach diesen Prüfmaßstäben können sich weder die Finanzverwaltungen und die Industrie- und Handelskammern noch die Deichverbände und Teile der Bauverwaltung generell darauf berufen, keine Informationen herausgeben zu müssen. Es bedarf immer einer **gründlichen Prüfung** der jeweils in Betracht zu ziehenden Norm, unabhängig davon, ob es sich um Bundes- oder Landesrecht handelt. Erst wenn tatsächlich eine bereichsspezifische Bestimmung den Informationszugang so wie er dem Grundgedanken des IFG NRW entspricht, in abschließender Form regelt, kann von dem Vorrang dieser Bestimmung ausgegangen werden.

Am Beispiel des behaupteten Ausschluss des IFG NRW durch das Baugesetzbuch lässt sich diese Prüfung demonstrieren. Die dort normierten Zugangsregeln etwa über die Offenlegung von beabsichtigter Bauleitplanung dienen in erster Linie der Ermittlung der bei Aufstellung und Beschlussfassung abzuwägenden **öffentlichen und privaten Belange**. Außerdem soll die öffentliche Auslegung eine Unterrichtung der Öffentlichkeit über voraussichtliche Auswirkungen eines Bauleitplanes ermöglichen und den Anstoß zur Äußerung potentiell durch die Planung betroffener Personen geben. Damit differieren schon Regelungsgegenstand, Adressatenkreis und Regelungszweck gegenüber dem allgemeinen Informationszugang. Außerdem schließen die Transparenzregeln einen individuellen Informationszugang nicht aus.

Das Finanzministerium sperrt sich leider nach wie vor dagegen, das IFG NRW zu akzeptieren. Das Wirtschaftsministerium entzieht sich einer eigenen Beurteilung, ob das IFG NRW auf die Industrie- und Handelskammern Anwendung findet. Demgegenüber hat das Innenministerium dafür gesorgt, dass die Deichverbände seine Anwendung grundsätzlich nicht mehr in Frage stellen. Es wäre schön, wenn das Ministerium für Stadtentwicklung und Wohnen den Baubehörden ebenfalls **Hinweise** für eine gründliche Prüfung bei der Anwendung des Baugesetzbuches geben würde.

Gründlichere Prüfungen des Verhältnisses vom IFG NRW zu anderen Gesetzen sind wünschenswert. Vorzugswürdig wäre allerdings eine gesetzliche Klarstellung.

23.2.2 Die Gemeindeordnung geht dem IFG NRW nicht vor

Wünsche nach Einsichtnahme in Unterlagen nichtöffentlicher Ratssitzungen wurden überwiegend pauschal mit der Begründung abgelehnt, dem Informationszugang stünden speziellere Veröffentlichungsregelungen der Gemeindeordnung (GO NW) entgegen.

Zunächst kann der Anwendbarkeit des IFG NRW nicht entgegen gehalten werden, dass Beratung und Beschlussfassung durch den Rat oder die Ausschüsse keine Verwaltungstätigkeiten im Sinne des IFG NRW seien. Zum einen sind diese Organe vom Anwendungsbereich des IFG NRW nicht ausdrücklich ausgenommen, zum anderen fällt der Erlass von Satzungen unter die klassische öffentlich-rechtliche Handlungsform einer Kommune. Seine Anwendung ist weiterhin selbst dann nicht ausgeschlossen, wenn ein spezielles Informationszugangsrecht geregelt ist. Konkurrenzfragen müssen

vielmehr in jedem konkreten Einzelfall durch eine an **Sinn und Zweck der bereichsspezifischen Vorschrift** orientierten Auslegung geklärt werden. Das IFG NRW tritt nur dann hinter anderen gesetzlichen Informationsrechten im Sinne einer verdrängenden Spezialität zurück, wenn die konkurrierenden Vorschriften identische Regelungsmaterien haben. Daran fehlt es beispielsweise, wenn sich die Normen an unterschiedliche Adressaten richten oder unterschiedliche Zielsetzungen verfolgen. Dies trifft auf die speziellen Zugangsregeln der GO NW zu.

Die Regelung der Gemeindeordnung zur Öffentlichkeit von Ratssitzungen lässt ein allgemeines Informationszugangsrecht unberührt, sie trifft lediglich die allgemeine Bestimmung, wann Ratssitzungen öffentlich und wann sie nichtöffentlich durchgeführt werden sollen. Auch die allgemeine Pflicht des Rates, wesentliche Inhalte der Ratsbeschlüsse öffentlich zu machen, stellt lediglich eine allgemeine **Bekanntmachungspflicht** des Rates und keine Zugangsregelung dar. Die genannten Vorschriften richten sich also an andere Adressatinnen und Adressaten und haben zudem eine andere Zielrichtung als das IFG NRW.

Darüber hinaus spricht eine historische Betrachtung dafür, dass das neue Zugangsrecht des **IFG NRW neben** den Regelungen der **GO NW** anwendbar ist. Die Regelungen der GO NW haben im Hinblick auf die Öffentlichkeit von Ratssitzungen nur den Grundgedanken des IFG NRW – Transparenz der öffentlichen Verwaltung – vorweg genommen und stellen eine Mindestanforderung dar, die heute durch das IFG NRW ergänzt wird. Anhaltspunkte, nach denen der Gesetzgeber mit den oben genannten Vorschriften den Zugang zu Ratsunterlagen abschließend regeln und daneben keine allgemeinen Zugangsrechte zulassen wollte, sind nicht erkennbar. Vor allem stehen der Anwendbarkeit des IFG NRW nicht die Vorschriften der GO NW über die Verschwiegenheit entgegen, da die Pflicht zur Amtsverschwiegenheit im Rahmen des IFG NRW entfällt und somit ein Verstoß gemäß §§ 30, 29 Abs. 2 GO NW nicht in Betracht kommen kann.

Die Tatsache, dass eine Ratssitzung oder ein Teil von ihr nichtöffentlich stattgefunden hat, steht noch nicht automatisch gegen die Anwendung des IFG NRW, weil seine gesetzlichen Ablehnungsgründe einen ausreichenden Schutz für die berechtigte Geheimhaltung der in dieser Sitzung verhandelten Themen und Unterlagen bieten. Es ist daher in jedem Einzelfall zu prüfen, ob im Hinblick auf die jeweils begehrten Informationen einer der Verweigerungsgründe gegeben ist. Erfolgt die **Nichtöffentlichkeit der**

Ratssitzungen aufgrund der Erörterung von persönlichen oder wirtschaftlichen Verhältnissen oder fachlichen Qualifikationen Dritter, könnte etwa ein Verweigerungsgrund nach §§ 8 oder 9 IFG NRW in Betracht kommen. Im Hinblick auf den Schutz von **Protokollen vertraulicher Beratungen** nach **§ 7 Abs. 1 IFG NRW** ist insoweit zu berücksichtigen, dass nach dieser Vorschrift lediglich der Inhalt der vertraulichen Beratung, nicht aber das Beratungsergebnis – wie etwa der verhandelte Grundstückskaufvertrag – schützenswert ist.

Der Informationsanspruch wird durch die Gemeindeordnung nicht ausgeschlossen. Weder die kommunalverfassungsrechtliche Stellung der Gemeindeorgane Rat und Ausschüsse noch spezielle Zugangsregelungen stehen einer Anwendung des IFG NRW entgegen.

23.2.3 Vorrang des Verwaltungsverfahrensgesetzes, aber ohne Sperrwirkung

Will eine informationssuchende Person, die nicht Beteiligte in einem Verwaltungsverfahren ist, Einsicht in die Verfahrensakte nehmen, wird ihr oft entgegen gehalten, dass nach § 29 Verwaltungsverfahrensgesetz (VwVfG) kein Zugang zur Akte gewährt werden könne, weil sie nicht Beteiligte des Verfahrens sei. Zugleich wird versucht, ihr den Informationszugang nach dem IFG NRW zu verweigern, weil nach der Auffassung einiger öffentlicher Stellen § 29 VwVfG als speziellere Zugangsregelung die Anwendung des IFG NRW ausschließe.

Diese unzutreffende Auffassung beruht auf der Annahme, dass schon dann, wenn es in einem Rechtsgebiet eine **besondere Zugangsregelung** gibt, nur nach dieser verfahren werden dürfe. Eine solche automatische Ausschlusswirkung haftet aber nicht von vornherein jeder besonderen Zugangsregelung an. Wenn die besondere Regelung den gleichen Sachverhalt erfasst und mit einer anderen Rechtsfolge bewertet, tritt die allgemeine Regelung zwar zunächst zurück. Wird nach der besonderen Regelung kein Zugang gewährt, weil die Voraussetzungen nicht erfüllt sind, findet aber grundsätzlich wieder die allgemeine Zugangsregelung Anwendung. Ein Ausschluss kann nur dann angenommen werden, wenn nach Sinn und Zweck des bereichsspezifischen Gesetzes die Anwendung sonstiger Zugangsmöglichkeiten ausgeschlossen sein soll.

Bei der Zugangsregelung des VwVfG handelt es sich um eine Ausnahmeregelung gegenüber dem früher geltenden Amtsgeheimnis, das wegen der

Gewährung rechtlichen Gehörs ausnahmsweise durchbrochen wurde. Es galt nämlich der Grundsatz, die Verwaltung arbeite geheim und gewähre nur ausnahmsweise einen Informationszugang. Mit dem **Informationsfreiheitsgesetz** wurde dieser Grundsatz gerade umgekehrt. Die Verwaltung arbeitet grundsätzlich öffentlich, nur in den vom Gesetzgeber festgelegten Ausnahmefällen bleibt der Informationszugang verwehrt. Informationen der Verwaltung sind jetzt öffentlich zugänglich, ganz gleich ob sie Gegenstand eines noch laufenden oder eines abgeschlossenen Verfahrens sind, und auch unabhängig davon, ob sie Gegenstand eines allgemeinen oder speziellen Interesses sind. Der Einwand, § 29 VwVfG sei die speziellere Regelung im Verhältnis zum IFG NRW, wäre richtig, wenn alle vom verfahrensrechtlichen Akteneinsichtsrecht umfassten Fälle zugleich das Zugangsrecht nach dem IFG NRW erfüllten. Das ist aber gerade nicht der Fall. Beide Vorschriften sind nebeneinander anzuwenden.

Selbst wenn der Spezialität der verfahrensrechtlichen Zugangsregelung gefolgt würde, könnte daraus allein noch **kein Ausschluss** des informationsrechtlichen Zugangsrechtes hergeleitet werden, weil ein solcher nach Sinn und Zweck des VwVfG nicht gewollt ist. Das Akteneinsichtsrecht nach § 29 VwVfG ist sowohl Ausfluss des Rechtsstaatsprinzips als auch des Rechts auf informationelle Selbstbestimmung. Es dient nicht nur der Verwirklichung rechtlichen Gehörs für die durch die spätere Verwaltungsentscheidung betroffene Person und der Fairness im Verfahren, sondern darüber hinaus der Mitwirkung der Beteiligten an der Wahrheitsfindung der Behörde. Die Regelung nimmt damit – allerdings noch in unzulänglicher Weise – schon das voraus, was in stärkerem Maße den gesetzgeberischen Willen beim IFG NRW bestimmte, nämlich die Akteneinsicht als notwendigen Bestandteil der öffentlichen Kontrolle staatlichen Handelns anzuerkennen. Die oft behauptete Systemwidrigkeit des informationsrechtlichen Zugangsrechtes im Verfahrensrecht besteht somit nicht.

Für das Verhältnis des allgemeinen Rechts auf Akteneinsicht nach dem **Umweltinformationsgesetz** zum Verwaltungsverfahrensgesetz ist übrigens unstreitig, dass bei gleicher Konstellation das allgemeine und freie Zugangrecht auch für alle Verfahrensbeteiligten besteht, ohne dass dort eine Systemwidrigkeit behauptet wird.

Dass das Verwaltungsverfahrensgesetz keine Sperrwirkung gegenüber dem IFG NRW entfaltet, bedarf einer Klarstellung im Gesetz oder zumindest in einer Verwaltungsvorschrift.

23.3 Ungeahnter Zuwachs an vermeintlichen Geschäftsgeheimnissen

23.3.1 Wer hat die Amtskette gespendet?

Die neue Amtskette eines Bürgermeisters erregte gewisses öffentliches Aufsehen. Woher sie denn sei und wer sie denn bezahlt habe, wurde gefragt – zunächst vergeblich.

Die Stadt verweigerte die Antwort unter Berufung darauf, dass es sich dabei um Geschäftsgeheimnisse handele. Das **Geschäftsgeheimnis** der spendenden Unternehmen bestehe darin, dass sie bei Bekanntgabe der Namen von weiteren Spendenanfragen belästigt werden könnten. Der Stadt und damit auch der Allgemeinheit drohe zudem ein wirtschaftlicher Schaden, da bei Offenlegung der Vorgänge die Spendenbereitschaft der Unternehmen nachlassen könnte.

Den Begriff des „Geschäftsgeheimnisses" erfüllen solche Umstände gerade nicht. Ein Geschäftsgeheimnis im Sinne des § 8 IFG NRW setzt nämlich voraus, dass die gewünschten Informationen den Gegenstand eines **berechtigten wirtschaftlichen Interesses** eines Unternehmens bilden. Das Geheimgehaltene muss danach für die Wettbewerbsfähigkeit Bedeutung haben. Maßgeblich ist in diesem Sinne daher, inwieweit mögliche Konkurrenzunternehmen tatsächlich einen wirtschaftlichen Nutzen aus der Offenlegung der entsprechenden Informationen ziehen können. So kann ein schutzwürdiges wirtschaftliches Interesse etwa im Hinblick auf die Gewinn- und Ertragslage des Unternehmens, Marktstrategien oder die Absicht, eine bestimmte Ware oder Dienstleistung auf den Markt zu bringen, gegeben sein. Die Zuteilung oder Entgegennahme einer Spende stellt jedoch keine solche Tätigkeit im wettbewerbsrechtlichen Sinne dar. Es handelt sich hierbei nicht um das Erlangen eines wirtschaftlichen Vorteils im Rahmen des Wettbewerbs, sondern um die bloße Entgegennahme einer rein zufälligen Zuwendung von dritter Seite ohne rechtlichen Grund. Die Spende für die Amtskette war weder für die spendenden Unternehmen noch für die Stadt ein Geschäftsgeheimnis.

Darüber hinaus war der Informationszugang in diesem Fall aber auch wegen des **überwiegenden Interesses der Allgemeinheit** an der Bekanntgabe der Spendernamen nach § 8 Satz 3 IFG NRW zu gewähren. Das überwiegende Interesse der Allgemeinheit ergab sich einerseits daraus, dass die Beschaffung der Amtskette seit geraumer Zeit in der lokalen Presse

Gegenstand von Berichterstattung und Leserbriefen war. Hinzu kam, dass bei Spenden – als Leistungen ohne Gegenleistung – der Eindruck entstehen konnte, dass eventuell doch auf eine andere Weise eine Gegenleistung erbracht worden sein könnte. Dieser mögliche Zweifel an der Rechtmäßigkeit des Verwaltungshandelns begründete ein Interesse der Allgemeinheit an der Offenlegung der Informationen, das gegenüber einer eventuellen finanziellen Einbuße durch den Ausfall potenzieller Spenden überwog.

Die Stadt blieb so hartnäckig bei ihrer unzutreffenden Auffassung, dass es erst einer förmlichen Beanstandung und einer verwaltungsgerichtlichen Entscheidung bedurfte, um den Informationsanspruch durchzusetzen (VG Düsseldorf, Urteil vom 09. Juli 2004, Az: 26 K 4163/03).

23.3.2 Und noch einmal: angebliche Geschäftsgeheimnisse

Gegenstand der gewünschten Akteneinsicht war ein Vertrag, der zwischen der Stadtverwaltung und einer privaten Eventagentur geschlossen wurde. Inhalt des Vertrags war die Überlassung einer öffentlichen Marktfläche zur Veranstaltung eines werktäglichen Spezialitätenmarktes.

Die Stadt lehnte den Informationsantrag mit der Begründung ab, dem Zugang stehe der Schutz von **Geschäftsgeheimnissen** der Eventagentur entgegen. Durch eine Bekanntgabe der Zahlungsverpflichtungen der Agentur könnte diese bei ihren Vertragsverhandlungen mit den Marktstandbetreibern geschwächt sein. Zudem sei bei gleichzeitiger Kenntnis der Beträge, die die Standbetreiber an die Agentur zahlen müssten, ein Rückschluss auf die Gewinn- und Verlustrechnung der Eventagentur möglich.

Diese Argumentation vermag jedoch nicht zu überzeugen, denn der Schutz von Geschäftsgeheimnissen nach dem IFG NRW setzt ein **berechtigtes wirtschaftliches Interesse** an der Geheimhaltung der begehrten Informationen voraus. Bei Verträgen zwischen Kommunen und Privaten, die bereits geschlossenen sind, ist zu berücksichtigen, dass eine Offenlegung von Entgelt- oder Haftungsregelungen eher nicht durch ein schützenswertes wirtschaftliches Interesse des Unternehmens auszuschließen ist. Bei den Zahlungsverpflichtungen der Eventagentur handelt es sich nämlich um Sondernutzungs- und Verwaltungsgebühren für die Überlassung einer öffentlichen Fläche. Solche Gebühren müssen grundsätzlich einer

öffentlichen Nutzungsordnung entnommen werden können. Somit ist die Verwaltung im Umgang mit finanziellen Haushaltsmitteln stärker als eine Privatperson an objektive Kriterien gegenüber den Entscheidungsgremien der Stadt gebunden. Zudem ist nach Vertragsschluss kein Wettbewerbsnachteil zu mitbietenden Konkurrenten mehr zu befürchten. Schon aus diesem Grund kann insoweit kein berechtigtes wirtschaftliches Interesse an einer Geheimhaltung im Sinne des IFG NRW gegeben sein.

Unabhängig davon sprach vieles dafür, dass die Allgemeinheit ein überwiegendes Interesse an der Gewährung des Informationszugangs hatte. Zum einen unterliegt ein Geschäftsgeheimnis, das im Zusammenhang mit der Wahrnehmung öffentlicher Aufgaben steht, grundsätzlich einer stärkeren Sozial- und Gemeinwohlausrichtung als private Geheimnisse (siehe hierzu 16. Datenschutzbericht 2003 unter 22.5.3, S. 194 ff). Zum anderen ergab sich das überwiegende Interesse der Allgemeinheit bereits daraus, dass die Nutzung des öffentlichen Platzes für den neuen Spezialitätenmarkt wegen rückständiger Forderungen der Stadt Gegenstand der Berichterstattung in der lokalen Presse war. Dieses Interesse der Allgemeinheit wog höher als das Interesse der Eventagentur, die Zahlungsverpflichtungen nicht bekannt zu geben, um bei der Gestaltung der von den Vertragspartnerinnen und -partnern zu zahlenden Nutzungsentgelte freier zu sein. Der dadurch zu berücksichtigende wirtschaftliche Schaden für die Eventagentur wäre daher nur bei überhöhten Entgelten ernstlich in Betracht zu ziehen.

Zwar hat die Stadt inzwischen auf Empfehlung der LDI die Vertragsunterlagen in Kopie zur Verfügung gestellt, die für die Nutzung der öffentlichen Fläche anfallenden Gebühren wurden jedoch geschwärzt. Im Hinblick auf die oben stehende Argumentation muss die Angelegenheit daher erneut gegenüber der Stadt aufgegriffen werden, damit der betreffende Vertragsteil ohne die Schwärzungen zugänglich gemacht wird.

23.3.3 Grundstückskaufverträge sind keine Geschäftsgeheimnisse

Informationsanträge über die Veräußerungen von Gemeindegrundstücken werden häufig pauschal mit der Begründung abgelehnt, der Einsichtnahme stünden bei Verträgen mit natürlichen Personen der Schutz personenbezogener Daten oder bei Verträgen mit juristischen Personen des Privatrechts Betriebs- und Geschäftsgeheimnisse entgegen.

Im Hinblick auf den **Schutz personenbezogener Daten** versäumen die Gemeinden häufiger, vor einer Ablehnung zunächst die abgestufte Prüfung im Sinne des §§ 9 Abs. 1, 10 Abs. 1 IFG NRW vorzunehmen (siehe hierzu 16. Datenschutzbericht 2003 unter 22.5.5, S. 198). Danach kann der Zugang etwa zu gewähren sein, wenn ein rechtliches Interesse an der Kenntnis des Vertragsinhalts geltend gemacht wird und überwiegende schutzwürdige Belange der Käuferin oder des Käufers nicht entgegenstehen. Hierfür reicht allerdings ein allgemeines Kaufinteresse nicht aus. Die informationssuchende Person muss vielmehr im Hinblick auf den Vertragsinhalt ein subjektives Recht geltend machen. Dies könnte etwa ein Vorkaufsrecht oder ein anderes dingliches Recht an dem Grundstück sein. Sofern keine der Ausnahmen von dem Schutz personenbezogener Daten nach § 9 Abs. 1 Buchstaben a) – e) IFG NRW in Betracht kommt, muss die öffentliche Stelle in einem zweiten Schritt prüfen, ob der Zugang jedenfalls teilweise nach Abtrennen oder Schwärzen der sensiblen Angaben zu gewähren ist. Insoweit könnten etwa die Personalien der Vertragspartei zu schwärzen sein. Ist die Identität der Käuferin oder des Käufers allerdings bereits bekannt, können alle weiteren Vertragsinhalte auf sie oder ihn bezogen werden und sind mithin zu schützen. Erst wenn ein Abtrennen oder Schwärzen der sensiblen Daten nicht möglich ist, muss die Einwilligung der betroffenen Person eingeholt werden.

Bei Grundstückskaufverträgen mit privaten Unternehmen kann ein Informationszugang nicht pauschal mit dem Hinweis auf ein **Betriebs- oder Geschäftsgeheimnis** abgelehnt werden. Für eine begründete Ablehnung reicht es nicht aus, dass vertraglich Vertraulichkeit vereinbart ist oder im Vertrag Informationen enthalten sind, die nach dem Willen des Unternehmens geheim gehalten werden sollen. Entscheidend ist vielmehr, dass ein objektiv berechtigtes wirtschaftliches Interesse an der Geheimhaltung gegeben ist. Maßgeblich kann dabei etwa der Umstand sein, inwieweit mögliche Konkurrenz einen wirtschaftlichen Nutzen aus der Offenlegung der begehrten Informationen ziehen kann. Nach erfolgtem Vertragsschluss ist dies allerdings kaum denkbar.

Zwar können Betriebs- oder Geschäftsgeheimnisse grundsätzlich auch bei einer öffentlichen Stelle gegeben sein, allerdings nicht in gleichem Schutzumfang wie bei privaten Unternehmen. Betriebs- oder Geschäftsgeheimnisse können sich keinesfalls auf den Bereich der Wahrnehmung öffentlicher Aufgaben erstrecken. Sie können also nur durch eine Tätigkeit entstehen, die sich außerhalb der öffentlichen Aufgabenerfüllung oder gelegentlich der

Aufgabenwahrnehmung ergibt, beispielsweise durch die Entwicklung einer Software, die eine automatisierte Bearbeitung von Verwaltungsverfahren oder Planungs- und Entscheidungsprozesse ermöglicht. In diesem Bereich soll die öffentliche Stelle – hinsichtlich des von einer konkurrierenden Person gewünschten Informationszuganges – genauso geschützt sein wie ein privates Unternehmen.

Bei Abschluss eines Grundstückskaufvertrages handeln die Gemeinden in Erfüllung öffentlicher Aufgaben, so dass sie diesbezüglich kein Betriebs- oder Geschäftsgeheimnis geltend machen können. Die Stadt ist beim Verkauf eines öffentlichen Grundstücks keine privaten Rechtspersonen vergleichbare Partnerin. Es liegt vielmehr im Allgemeininteresse, die Umstände eines solchen Grundstücksverkaufes in Erfahrung bringen zu können.

23.3.4 Cross-Border-Leasing-Geschäfte – top secret?

Die in der öffentlichen Diskussion umstrittenen Cross-Border-Leasing-Geschäfte sind auch Gegenstand von Informationsanträgen nach dem IFG NRW. Bei diesen Geschäften haben US-Unternehmen öffentliche Anlagen wie Messehallen, Stadtwerke oder Abwassernetze von deutschen Kommunen geleast. Die Rechtslage in den USA hatte bis vor einiger Zeit Steuersparmodelle möglich gemacht, wenn ausländische Immobilien geleast wurden. Dadurch, dass die Kommunen die Anlagen aufgrund des Steuerschlupflochs wiederum zu einem günstigeren Preis von den US-Unternehmen zurückleasen konnten, haben die Geschäfte den Kommunen einen Barwertvorteil gebracht.

In verschiedenen Kommunen wurden Anträge auf Informationszugang zu den Namen der beteiligten Unternehmen und den Vertragsunterlagen mit der Begründung abgelehnt, die Kommunen hätten sich vertraglich verpflichtet, die in den Unterlagen enthaltenen Informationen nicht an Dritte weiterzugeben. Dem ist jedoch entgegenzuhalten, dass eine gesetzliche Verpflichtung der öffentlichen Stelle nach dem IFG NRW nicht vertraglich abbedungen werden kann. Vielmehr sind die im Rahmen des allgemeinen Informationszuganges in Betracht kommenden Verweigerungsgründe abschließend im IFG NRW festgelegt. Eine vertragliche **Vertraulichkeitsvereinbarung** ist von diesen Ausnahmetatbeständen nicht umfasst.

Die Kommunen müssen deshalb im Einzelfall den Anforderungen des IFG NRW entsprechend darlegen, inwieweit dem Informationszugang etwa der

Schutz von Betriebs- oder Geschäftsgeheimnissen der betroffenen US-Unternehmen und Finanzdienstleister nach **§ 8 IFG NRW** entgegensteht (siehe hierzu 16. Datenschutzbericht 2003 unter 22.5.3, S. 194). Fraglich ist insoweit, ob allein schon die Namen der Vertragspartnerinnen und -partner bereits ein Geschäftsgeheimnis darstellen und an ihrer Geheimhaltung ein **berechtigtes wirtschaftliches Interesse** besteht. Die Offenbarung der Information, welche US-Unternehmen und Finanzdienstleister mit welcher Stadt eine Cross-Border-Leasing-Geschäftsverbindung eingegangen sind, kann für sich gesehen noch keine nachteiligen Konsequenzen für die Wettbewerbsfähigkeit der Unternehmen nach sich ziehen. Allein aufgrund dieser Information können mögliche Konkurrentinnen und Konkurrenten keinen wirtschaftlichen Nutzen gewinnen, weil das Vertragswerk bereits abgeschlossen ist. Die Kommunen befürchten zwar, dass bei Bekanntgabe der Namen diese Unternehmen sowohl in den USA als auch in Deutschland in der öffentlichen Diskussion „an den Pranger gestellt" und deshalb deren Geschäfte beeinträchtigt werden könnten. Diese befürchteten Auswirkungen beruhen aber auf einer subjektiven Bewertung und Einschätzung durch Teile der Öffentlichkeit in Deutschland und den USA im Zusammenhang mit der Rechtslage und den Risiken von Cross-Border-Leasing-Geschäften. Eine öffentliche Meinungsbildung wird durch den Schutzzweck des IFG NRW nicht verhindert.

Unabhängig von der Frage, ob überhaupt ein Geschäftsgeheimnis vorliegt, spricht vieles dafür, dass die Allgemeinheit in diesen Fällen ein **überwiegendes Interesse** an der Gewährung des Informationszugangs nach **§ 8 Satz 3 IFG NRW** hat (siehe hierzu auch 16. Datenschutzbericht 2003 unter 22.5.3, S. 196). Dies gilt hier in besonderem Maße, wenn Gegenstand der Vertragswerke nicht nur Straßenbahnen, Schienennetze und Messehallen sind, sondern zum Beispiel auch das Abwassernetz, also Anlagen, die nach dem Abwassergesetz Teil der öffentlich-rechtlichen Aufgabenwahrnehmung im Rahmen der Abwasserentsorgung sind. Wegen einer Vertragsbindung für etwa 30 bis 99 Jahre und wegen der Bedeutung der zugrundeliegenden Aufgaben können mit den Verträgen erhebliche Risiken für die Kommunen verbunden sein. Damit besteht auch an der Bekanntgabe von Vertragsinhalten – also auch soweit sie Geschäftsgeheimnisse enthalten – etwa den Haftungsregelungen bei Pflichtverletzungen ein öffentliches Interesse. Auch im Hinblick auf die Einflussmöglichkeiten und Mitwirkungsrechte der Beteiligten sowie deren Konkursrisiko besteht ein Interesse der Allgemeinheit an der Bekanntgabe der Firmennamen und weiterer Informationen aus den Verträgen. Dieses Interesse der

Allgemeinheit dürfte in der Regel höher wiegen als das Geheimhaltungsinteresse des US-Unternehmens oder der Kreditinstitute.

Die Cross-Border-Leasing-Verträge sind grundsätzlich der Öffentlichkeit zugänglich. Sollten dennoch einzelne Teile der begehrten Vertragsunterlagen nach dem IFG NRW zu schützen sein, müssten die informationspflichtigen Stellen der Antragsstellerin oder dem Antragsteller jedenfalls einen eingeschränkten Informationszugang nach Abtrennen oder Schwärzen der sensiblen Daten gewähren oder Auskunft erteilen.

23.4 Mehr Licht! Beispiele aus verschiedenen Verwaltungsbereichen

23.4.1 Starke Nachfrage nach Bauangelegenheiten

Sehr oft wird die Einsichtnahme in Bauakten gewünscht. Dies betrifft eigene oder fremde Baugenehmigungsverfahren ebenso wie Bauplanungsunterlagen.

Bei Informationsanträgen zu Bauunterlagen werden hin und wieder Bedenken im Hinblick auf den Schutz personenbezogener Daten geäußert. Möglichen datenschutzrechtlichen Problemen trägt § 9 IFG NRW allerdings in vollem Umfang Rechnung (siehe dazu 16. Datenschutzbericht unter 22.5.5. S. 197 ff.). Abgesehen davon geht es aber auch um andere Fragen. So stehen in manchen Fällen dem Informationszugang, soweit es die **Anfertigung von Kopien** für die informationssuchende Person anlangt, Urheberrechte Dritter entgegen. Hierzu können etwa die Urheberrechte einer oder eines Sachverständigen im Hinblick auf ein im Rahmen eines Genehmigungsverfahrens erstellten Gutachtens zählen oder die Rechte der beauftragten Architektin an den von ihr erstellten Bauplänen.

Nach § 5 Abs. 1 Satz 5 IFG NRW darf eine andere als die von der informationssuchenden Person begehrte Art des Informationszugangs von der öffentlichen Stelle nur bestimmt werden, wenn hierfür ein wichtiger Grund vorliegt. Die Beachtung von Urheberrechten kann im Hinblick auf die Herausgabe von Kopien einen solchen wichtigen Grund darstellen. Das Urheberrecht schützt vor unerlaubter Verwertung oder Nutzung der erstellten Werke. So ist gemäß § 16 Urhebergesetz die Vervielfältigung eines geschützten Werkes und Herausgabe an Dritte der Urheberin oder dem Urheber vorbehalten. Dabei ist allerdings zu differenzieren, ob eine öffentliche Stelle die Nutzungs- und Verwertungsrechte an der in Auftrag

gegebenen Arbeit – beispielsweise an einem Gutachten oder einem Planentwurf – erworben hat oder ob diese Rechte weiterhin der Erstellerin oder dem Ersteller des Werkes zustehen und sie oder er unter Umständen in eine Herausgabe der Informationen eingewilligt hat. Urheberrechtlich unbedenklich ist dagegen in jedem Fall die bloße Einsichtnahme in ein geschütztes Werk.

Der Schutz von Urheberrechten ist ein wichtiger Grund, dem bei der Herausgabe von Kopien Rechnung getragen werden muss. Gegebenenfalls bleibt dann nur die Einsichtnahme als zulässiger Informationszugang.

23.4.2 Umfangreiche Aktenbestände sind kein Ablehnungsgrund

Da die Bauunterlagen für eine Dosenfabrik und Lagerhalle etwa 40 DIN A 4 Aktenordner ausmachten und im Hinblick auf das Vorliegen möglicher Betriebs- und Geschäftsgeheimnisse durchgesehen werden mussten, wollte die Stadtverwaltung einen Informationsantrag ursprünglich ablehnen.

Der Verwaltungsaufwand, der aufgrund einer Akteneinsicht entstehen kann, stellt jedoch grundsätzlich keinen gesetzlichen Verweigerungsgrund dar. Sofern größere Aktenbestände sorgfältig auf das Vorliegen von Verweigerungsgründen geprüft und sensible Daten unter Umständen abgetrennt oder geschwärzt werden müssen, kann für die begehrte Akteneinsicht allenfalls eine Gebühr erhoben werden. Allerdings würde auch hier unter Beachtung des landesrechtlichen Trennungsgebotes zu berücksichtigen sein, dass die Baugenehmigungsbehörde schon beim Anlegen der Genehmigungsakte verpflichtet war, die dem Betriebs- oder Geschäftsgeheimnis unterliegenden Informationen zu kennzeichnen und gegebenenfalls abgesondert in der Akte abzuheften.

Dem Trennungsgebot ist frühzeitig Rechnung zu tragen. So sollten Informationen, die bei einer späteren Einsichtnahme wegen eines gesetzlichen Verweigerungsgrundes nicht zugänglich sein dürfen, bereits zum Zeitpunkt der Aktenanlage getrennt und in einen eigenen Vorgang geheftet werden, während eine Kopie mit den geschwärzten Daten zur Verfahrensakte genommen wird. Damit entfällt der Verwaltungsaufwand bei der Prüfung eines späteren Informationsantrages.

23.4.3 Was steht eigentlich in den Berechnungsgrundlagen für Abfall- und Straßengebühren?

Die Berechnungsgrundlagen für die Gebühren der Abfallbeseitigung und Straßenreinigung waren von Interesse.

Die Stadt lehnte den Informationszugang pauschal mit der Begründung ab, dass die entsprechenden Aufgabenbereiche durch zwei privatrechtliche Entsorgungsgesellschaften wahrgenommen würden und das IFG NRW daher nicht zur Anwendung käme. Dies war nicht zutreffend, denn die Stadt hatte übersehen, dass es sich bei der Müll- und Abwasserentsorgung nach § 5 Landesabfallgesetz und § 53 Landesabwassergesetz um **öffentlich-rechtliche Aufgaben** handelt, die sie auf die Entsorgungsgesellschaften übertragen hatte. Damit ist das IFG NRW auch auf private Entsorgungsgesellschaften anzuwenden.

Wenig serviceorientiert war zudem, dass die Stadt ihrer **Beratungspflicht** aus dem Grundsatz des bürgerfreundlichen Verhaltens im Sinne des § 25 Verwaltungsverfahrensgesetz Nordrhein-Westfalen nicht nachgekommen ist (siehe hierzu 16. Datenschutzbericht 2003 unter 22.4, S. 189). Die Stadt hätte den Antragsteller darüber aufklären müssen, dass sich die Berechnungsgrundlagen aus den nach gesellschaftsrechtlichen Regelungen zu erstellenden Planungsrechnungen und Betriebsabrechnungen ergaben, die allein bei den Entsorgungsgesellschaften vorlagen und daher auch nur dort zur Verfügung gestellt werden konnten. Andererseits waren für den Antragsteller aber auch die Kostenanmeldungen und Kostenabrechnungen interessant, die die Gesellschaften nach den Verträgen mit der Stadtverwaltung zur Begründung der Mittelanmeldung der Stadt vorlegen mussten. Diese Unterlagen waren bei der Stadt selbst vorhanden und konnten auch dort eingesehen werden. Danach stand dem Antragsteller in diesem Fall grundsätzlich ein Informationsanspruch sowohl gegenüber der Stadt als auch gegenüber den beiden Entsorgungsgesellschaften zu.

Trotz der ausdrücklichen Empfehlung weigert sich die Stadt weiterhin, die begehrten Berechnungsgrundlagen zur Verfügung zu stellen. Sollte die Verwaltung nicht positiv reagieren, wird das Verhalten der Stadt zu beanstanden sein.

23.5 Aktive Informationspolitik im Rat leider vorerst gescheitert

In einer Kommune hatte die oppositionelle Ratsfraktion den Entwurf einer Geschäftsordnung des Rates vorbereitet, der in besonderem Maße die Zielsetzungen des IFG NRW unterstützten sollte. In Rahmen dieses Entwurfs sollten zum Beispiel die Unterlagen öffentlicher Sitzungen mit Beschlussvorlagen, Begründung und Abstimmungsergebnis der Öffentlichkeit über das Ratsinformationssystem online verfügbar gemacht werden.

Neben den im IFG NRW normierten allgemeinen Zugangsrechten schreibt § 12 IFG NRW den öffentlichen Stellen nach der Gesetzesbegründung eine **aktive Informationspolitik** vor. Im Zeitalter des Internet, in dem jede Behörde sich bemüht, ihre gesetzlichen Aufgaben serviceorientiert für die Bürgerinnen und Bürger auch über die neuen Medien umzusetzen, ist eine entsprechende Veröffentlichung daher wünschenswert. Eine aktivere Nutzung des Internet für die Vermittlung von Informationen, die ansonsten in jedem Einzelfall herausgegeben werden müssen, kann zudem zu einer Reduzierung der Zahl von Informationsanträgen führen und damit eine Arbeitserleichterung für die öffentliche Verwaltung darstellen.

Nach dem Entwurf der Geschäftsordnung sollen Unterlagen auch aus **nichtöffentlichen Sitzungen** ausdrücklich nach Maßgabe des IFG NRW zugänglich sein. Leider wurde die Änderung der Geschäftsordnung im Rat abgelehnt.

Die Beratung, die für den Entwurf der Geschäftsordnung geleistet wurde, war hoffentlich nicht dauerhaft vergebens. Zur Nachahmung empfohlen findet eine aktive Informationspolitik vielleicht in anderen Kommunen mehr Befürwortung.

23.6 Gebührenvorauszahlung: Informationen gegen Vorkasse ist nicht im Sinne des IFG NRW

Der Anspruch auf Informationszugang stößt nicht in jeder Behörde auf Gegenliebe. Kann das Informationsbegehren nicht durch die im Gesetz vorgesehenen Ausschlussgründe abgelehnt werden, versucht es die informationspflichtige Stelle auch schon mal mit der Gebührenfalle.

Das IFG NRW gewährt den Informationszugang grundsätzlich voraussetzungslos. Das bedeutet, dass die Gewährung des Informationszugangs nicht

von Bedingungen – insbesondere nicht von der Vorauszahlung einer Gebühr – abhängig gemacht werden darf. Durch eine Gebührenforderung vor Informationsgewährung würde eine unzulässige Hürde geschaffen, welche die Informationssuchenden möglicherweise von der Wahrnehmung ihrer Informationsrechte abhalten könnte. Zwar wird die Vorauszahlung auf § 16 Gebührengesetz des Landes Nordrhein-Westfalen (GebG NRW) gestützt, wonach die Vornahme einer Amtshandlung von einer Vorschusszahlung abhängig gemacht werden kann. Für Amtshandlungen nach dem IFG NRW widerspricht diese Regelung jedoch der gesetzgeberischen Intention, der informationssuchenden Person einen voraussetzungslosen Informationszugang zu gewähren. Das der Verwaltung bei der Anwendung des § 16 GebG NRW eingeräumte Ermessen („kann ... abhängig gemacht werden") ist deshalb entsprechend einer sich am Willen des IFG NRW-Gesetzgebers orientierenden Auslegung grundsätzlich auf Null reduziert, so dass von der eingeräumten Befugnis zu vorheriger Gebührenerhebung im Falle von Amtshandlungen nach dem IFG NRW **kein Gebrauch** gemacht werden sollte.

Zu beanstanden ist auch die in Einzelfällen festgestellte Methode, die informationssuchende Person durch die schlichte Ankündigung des vorgesehenen Gebührenrahmens (10 € bis 1.000 €) von der Wahrnehmung ihres Informationszugangsrechtes abzuschrecken. Eine Gebühr nach § 11 IFG NRW darf aber überhaupt nur erhoben werden, wenn mit der erteilten Auskunft oder der gewährten Akteneinsicht ein **erheblicher** Vorbereitungs- oder Verwaltungsaufwand verbunden ist. Selbst wenn ein erheblicher Aufwand zur Gebührenerhebung berechtigt, muss der geforderte Betrag von der Behörde nachvollziehbar und in angemessener Höhe festgesetzt werden. Durch die Gebühr soll lediglich der durch die Informationsgewährung unmittelbar zusätzlich entstandene Verwaltungsaufwand ausgeglichen werden. Nicht erstattungsfähig sind insbesondere diejenigen Aufwendungen, die einem Verwaltungsträger dadurch entstehen, dass er auf Grund einer Anfrage die Anwendbarkeit des IFG NRW zu prüfen hatte. Obwohl diese Aufwendungen unmittelbar auf die Anfrage zurückzuführen sind, obliegt es einer Behörde von Amts wegen, sich im Rahmen ihres Verwaltungshandelns des jeweils anwendbaren Rechts zu vergewissern. Solche Bemühungen können den Bürgerinnen und Bürgern nicht entgeltlich angelastet werden. Das gleiche gilt für Arbeitsaufwendungen, die entstehen, wenn dem landesrechtlichen **Trennungsgebot** nicht von vornherein Rechnung getragen wurde. Das wird immer dann der Fall sein, wenn die Akte nicht so angelegt wurde, dass die dem IFG NRW unterfallenden Informationen ohne

unverhältnismäßigen Aufwand abgetrennt werden können. Die Trennung spielt vor allem in Genehmigungs- und Planfeststellungsverfahren eine Rolle, weil hier von Anfang an in Antragsunterlagen etwa Geschäfts- oder Betriebsgeheimnisse besonders gekennzeichnet und abgesondert von den übrigen Unterlagen abgeheftet werden können.

In der Mehrzahl aller Fälle wird im Übrigen – wenn überhaupt – nur eine Gebühr im unteren Bereich des Gebührenrahmens in Betracht kommen. Nichts spricht dagegen, die voraussichtliche Höhe einer zu erwartenden Gebühr den Informationssuchenden vor Gewährung des gewählten Informationszuganges mitzuteilen, damit diese sich darauf einstellen oder möglicherweise eine andere Art des Informationszuganges wählen können.

Auch eine mittelbare Beeinträchtigung der Wahrnehmung des Rechts auf Informationszugang ist unzulässig. Die Gewährung des Informationszugangs darf deshalb nicht von der Vorabzahlung einer Gebühr abhängig gemacht werden. Ebenso hat der Versuch zu unterbleiben, Informationssuchende durch die Angabe der denkbar höchsten Gebühr abzuschrecken.

23.7 Neuerungen im Recht auf Zugang zu Umweltinformationen

Seit bald zwei Jahren wartet die EG-Richtlinie über den Zugang der Öffentlichkeit zu Umweltinformationen (Richtlinie 2003/4/EG vom 28.01.2003) auf ihre Umsetzung in nationales Recht. Im Februar 2005 läuft die Frist zur Umsetzung ab.

Kurz vor dem Fristende ist das bundesrechtliche Umweltinformationsgesetz (UIG) geändert worden und am 14. Februar 2005 in Kraft getreten. Der Anwendungsbereich umfasst – im Gegensatz zum früheren UIG – nur informationspflichtige Stellen des Bundes. Das bedeutet, dass die Länder eigene Umweltinformationsgesetze schaffen müssen. Auch Nordrhein-Westfalen ist damit in der Pflicht, ein Landesgesetz zu erarbeiten. Da es außerdem zu den Ländern mit eigenen Informationsfreiheitsgesetzen gehört, sollten sinnvollerweise Überlegungen zur **Angleichung beider Gesetze** angestellt werden. Es dürfte den Bürgerinnen und Bürgern kaum verständlich sein, wenn die Zugangsrechte unterschiedlich ausfallen. Deshalb wird es notwendig sein, den höheren Standard bei der Ausgestaltung des Zugangsrechtes der EG-Richtlinie soweit wie möglich auf das IFG NRW zu übertragen. Die dafür in Betracht zu ziehenden Verbesserungen in der Umweltinformationsrichtlinie umfassen vor allem folgende Punkte:

- bei Privatisierung öffentlicher Aufgaben (im Umweltbereich) gilt das Informationszugangsrecht auch gegenüber privaten Unternehmen;
- ein Informationsantrag darf zum Schutz behördlicher oder privater Interessen nur abgelehnt werden, wenn die Abwägung entgegenstehender Interessen ein überwiegendes Geheimhaltungsinteresse ergibt;
- öffentliche Stellen wie private Unternehmen werden verpflichtet, (Umwelt-)Informationen von sich aus – auch im Internet – zu veröffentlichen.

Im Interesse der Bürgerinnen und Bürger könnten die Informationsrechte auch in einem Gesetz zusammengefasst werden (so auch die Entschließung der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands vom 02. Juni 2004, abgedruckt im Anhang Nr. III). Leider haben sich die zuständigen Ministerien zu der ihnen übersandten Entschließung noch nicht geäußert.

Anhang

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

65. Konferenz am 27./28. März 2003

1. TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und Kontrollinfrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance" (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hardware und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten beziehungsweise das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulationssicheren und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüffunktionen und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,
- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,
- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,
- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,
- der Zugang zum Internet und E-Mail-Verkehr durch Softwarerestriktionen behindert würde,
- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,
- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und
- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informationstechnik und Kommunikationstechnik auf, Hardware und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,
- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und
- die Nutzung von Hardware und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personen-

bezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

2. Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

- Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.
- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgabengrenzen und Befugnisgrenzen missbraucht werden.
- Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
- Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in" statt „opt out").

Technischer Datenschutz

Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den Systemschutz und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

Förderung von datenschutzgerechter Technik

Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von E-Mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (zum Beispiel Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungsdaten und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungsdaten und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung

der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts zum Beispiel bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

Stärkung des Schutzes von Gesundheitsdaten

Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten zum Beispiel zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung" einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis. Geprüft

werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, zum Beispiel in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

Datenschutz und Gentechnik

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen – dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes" vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt

Datenschutz im Steuerrecht

Im bisherigen Steuerrecht und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichtsrecht und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismä-

ßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und Vorratsspeicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informationsrechte und Auskunftsrechte zuzuerkennen.

Arbeitnehmerdatenschutz

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

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

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie

vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

Stellung des Bundesdatenschutzbeauftragten

Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

Verbesserung der Informationsrechte

Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

3. Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9802 Anordnungen, waren es im Jahr 2001 bereits 19896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen

die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Abs. 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

4. Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur" der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur" gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.01.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen" eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen" bietet im Gegensatz zur „qualifizierten elektronischen Signatur" und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung" keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen" hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen" vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen. Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.
- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.
- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechtsverkehr und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005" als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,
- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,
- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,
- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und gegebenenfalls Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung" staatlich zu fördern.

- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,
- e-Government-Projekte und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,
- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern.
- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

5. Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10-Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefonüberwachung, Wohnraumüberwachung oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

6. Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungsdaten und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens unter anderem vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungsdaten und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrundelegen,

- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungsdaten und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnoseangaben und Behandlungsangaben zum Beispiel zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden. Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grundsätzlich selbst zu entscheiden,

   - ob sie überhaupt verwendet wird,
   - welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
   - welche Daten zu löschen sind und wann das zu geschehen hat,
   - ob sie im Einzelfall vorgelegt wird und
   - welche Daten im Einzelfall ausgelesen werden sollen.
   - Sicherzustellen ist weiterhin

- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen" vom 3. Mai 2002, wonach „der Patient Herr seiner Daten" sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

1. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski", „raucht", „trinkt zwei Biere pro Tag"), diese überwachen und so zur „Gesundheitspolizei" werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

2. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

7. Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hardware und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen

Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)" entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen.

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt.

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und IT-Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln beziehungsweise vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

1. Die Schutzprofile mit dem Titel „BISS – Benutzerbestimmbare Informationsflusskontrolle" – haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

2. Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

Entschließungen zwischen den Konferenzen

8. Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation (28. April 2003)

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vergleiche dazu Entschließung der 65. Konferenz vom 28.03.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (zum Beispiel Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie zum Beispiel PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.03.2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass zum Beispiel der Erwerb eines „vertragslosen" Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinnlosen und nutzlosen Datenhalden führen. So sind erfahrungsgemäß zum Bei-

spiel die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

9. Neuordnung der Rundfunkfinanzierung (30. April 2003)

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind . Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.

Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.

Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

10. Bei der Erweiterung der DNA-Analyse Augenmaß bewahren (16. Juli 2003)

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g Strafprozessordnung (StPO) für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (so genannter genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr – wie vom geltenden Recht gefordert – in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,
- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch

das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht-codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (zum Beispiel kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

11. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum automatischen Software-Update (7. August 2003)

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von Systemsoftware und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei – oftmals vom Nutzer unbemerkt oder zumindest nicht transparent – Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.
- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.
- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das – unbemerkte – Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

66. Konferenz am 25./26. September 2003

12. Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartalsübergreifenden und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein

tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.

- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (zum Beispiel mit Data-Warehouse-Systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungsdaten und Leistungsdaten unzulässig ist, und dass
- die Krankenkassen die Daten nur für Abrechnungszwecke und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

13. Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b Strafprozessordnung (StPO) und anderer verdeckter Ermittlungsmaßnahmen" vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 Prozent erhöht (1996: 2149; 2001: 3868) hat,
- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2494 um das Sechsfache auf 15741 gestiegen ist,
- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3730 auf 9122 fast verdreifacht hat,
- in 21 Prozent der Anordnungen zwischen 1000 und 5000 Gespräche, in acht Prozent der Anordnungen mehr als 5000 Gespräche abgehört worden sind,
- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von circa zwei Prozent auf circa 14 Prozent angestiegen ist,
- die Beschlüsse in circa dreiviertel aller Fälle das gesetzliche Maximum von drei Monaten umfassen, dreiviertel aller Maßnahmen tatsächlich aber nur bis zu zwei Monaten andauern,
- lediglich 24 Prozent der Beschlüsse substanziell begründet werden,
- es nur in 17 Prozent der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,
- 73 Prozent der betroffenen Anschlussinhaberinnen und Anschlussinhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (zum Beispiel Beweisverwertungsverbote).
- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und Ermittlungsrichter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.
- Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100 a StPO muss reduziert werden.
- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.
- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Gesprächsteilnehmerinnen und Gesprächsteilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.
- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.
- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.
- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.
- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (zum Beispiel IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Entschließungen zwischen den Konferenzen

14. Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes (21. November 2003)

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

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

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

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen

Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

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

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

15. Übermittlung von Flugpassagierdaten an die US-Behörden (13. Februar 2004)

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

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zollbehörden und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden zum Beispiel Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotelreservierungen und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen. Die US-Zollbehörden wollen alle Reservierungsdaten mindestens dreieinhalb Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere acht Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensicht-

lich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

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

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

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Artikel 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet (http://www.europa.eu.int). Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zur Zeit praktiziert wird, muss ausgeschlossen werden.

67. Konferenz am 25./26. März 2004

16. Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechtspolitischen und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

17. Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden – anders als insbesondere den behandelnden Ärztinnen und Ärzten – nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und Datenverarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 Strafgesetzbuch (StGB) die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a Strafprozessordnung (StPO) für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

18. Personennummern

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

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

19. Automatische Kfz-Kennzeichenerfassung durch die Polizei

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

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

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

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

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

20. Die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004 schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Entschließung zu Radio-Frequency Identification vom 20. November 2003 (Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Techno-

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

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

- sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;
- wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;
- dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und
- soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.
- Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

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

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

68. Konferenz am 28./29. Oktober 2004

21. Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

22. Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff" in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung" und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens" offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

23. Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Entschließung zwischen den Konferenzen

24. Staatliche Kontenkontrolle muss auf den Prüfstand! (26. November 2004)

Das „Gesetz zur Förderung der Steuerehrlichkeit" vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z.B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes" anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen" verwendet (neben den Begriffen „Einkommen" und „Einkünfte" etwa auch „Wohnung", „Kindergeld", „Arbeitnehmer"), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z.B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch

auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

Entschließungen der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)

I. Gleiche Transparenz in Verwaltung und Archiven (26. Mai 2003)

Seit 1998 sind in Brandenburg, Berlin, Schleswig-Holstein und Nordrhein-Westfalen Informationsfreiheitsgesetze entstanden, die den Bürgerinnen und Bürgern einen voraussetzungslosen Zugang zu behördlichen Informationen ermöglichen. Während fast alle europäischen Länder mittlerweile über solche Regelungen verfügen, steht ein Informationsfreiheitsgesetz des Bundes nach wie vor aus.

Die Idee, amtliche Informationen für alle zugänglich zu machen, ist jedoch älter als die Informationsfreiheitsgesetze der vier deutschen Bundesländer. Auch in Deutschland gelten sowohl auf der Bundesebene als auch in den einzelnen Ländern bereits seit langem Archivgesetze, die Interessierten einen allgemeinen Zugang zu Informationen eröffnen. Sie können daher als Vorläufer der Informationsfreiheitsgesetze betrachtet werden.

Ein entscheidender Unterschied zu den Informationsfreiheitsgesetzen besteht jedoch darin, dass die Offenlegung von in den Archiven befindlichen Unterlagen an strenge Fristen gebunden und beispielsweise nach dem Bundesarchivgesetz in der Regel erst nach dreißig Jahren möglich ist. Nur in Einzelfällen kann von diesen Fristen abgewichen werden. Teilweise wird die Offenlegung des Archivguts sogar von einem berechtigten Interesse der Antrag stellenden Person abhängig gemacht. Archivierte Akten sind dadurch faktisch nur noch für die historische Forschung interessant.

Diese archivrechtlichen Einschränkungen sind mit den Prinzipien der Informationsfreiheitsgesetze nicht in Einklang zu bringen. Sie würden zu dem geradezu absurden Ergebnis führen, dass frei zugängliche Akten nach Abgabe an ein Archiv plötzlich geheim gehalten werden. Dieser Widerspruch kann auch nicht dadurch gelöst werden, dass – wie dies teilweise gehandhabt wird – zuvor eingesehene Unterlagen bei Übergabe an das Archiv entsprechend gekennzeichnet werden und folglich nicht mehr den Geheimhaltungsfristen unterliegen. Diese Verfahrensweise macht den Zugang zu Dokumenten vom Zufall einer zuvor stattgefundenen Akteneinsicht abhängig. Aktuelle Informationen der Verwaltung, die zunächst allgemein zugänglich sind, werden so paradoxerweise mit der Übernahme durch das Archiv langjährig verschlossen, nur um sie nach Ablauf dieser Fristen wieder der Öffentlichkeit zugänglich zu machen.

Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland fordert daher die Gesetzgeber auf, den Informationszugang in archivrechtlichen Regelungen nach den

Maßstäben der Informationsfreiheit zu gestalten: Einschränkungen des Informationsanspruchs sind dann nur aufgrund eines überwiegenden privaten oder öffentlichen Geheimhaltungsinteresse möglich.

Die Änderung bestehender Archivgesetze kann aber nur ein erster Schritt sein. Eine eindeutige, verständliche und widerspruchsfreie Regelung von Informationsrechten wird nur gelingen, wenn Archivgesetze, Informationsfreiheitsgesetze und Datenschutzgesetze in einem einheitlichen Informationsgesetzbuch zusammengeführt werden.

II. Ausweitung der Informationsfreiheit statt Flucht ins Privatrecht (16. Dezember 2003)

Auf ihrer Tagung in Kiel am 16. Dezember 2003 forderten die Informationsfreiheitsbeauftragten Deutschlands:

Die zunehmende Privatisierung öffentlicher Aufgaben darf nicht zu einer Umgehung der Informationsfreiheitsgesetze führen. Im Gegenteil: Bürgerinnen und Bürger müssen gerade in Zeiten knapper werdender öffentlicher Mittel und der damit einhergehenden Verlagerung von Aufgaben in den privaten Bereich die Möglichkeit haben, Entscheidungen nachzuvollziehen und zu kontrollieren. Solche Kontrollmöglichkeiten der Öffentlichkeit auf der Grundlage der geltenden Informationsfreiheitsgesetze bestehen im Prinzip nur gegenüber öffentlichen Stellen.

Derzeit ist ein Zugang zu Informationen nicht mehr möglich, sobald Aufgaben formell aus der Verwaltung ausgegliedert und fortan privatwirtschaftlich organisiert werden. Dies gilt auch, wenn der Staat an dem Unternehmen beteiligt ist, maßgeblich dessen Entscheidungen beeinflusst und etwaige negative Geschäftsergebnisse die öffentlichen Haushalte belasten. Erfahrungsgemäß werden vor allem jene öffentlichen Bereiche privatisiert, die über ein besonders großes Finanzvolumen verfügen (zum Beispiel Liegenschaftsverwaltung, Energieversorgung, Verkehrsbetriebe, Wirtschaftsförderung). Hier ist besondere Transparenz hinsichtlich der Verwendung öffentlicher Steuermittel geboten. Soll dies erreicht und damit auch eine stärkere Akzeptanz behördlicher und politischer Entscheidungen ermöglicht werden, darf die Anwendung der Informationsfreiheitsgesetze nicht von der Rechtsform abhängen, in der öffentliche Aufgaben erledigt werden.

Darum fordern die Informationsfreiheitsbeauftragten Deutschlands:

Die Informationsfreiheitsgesetze müssen generell für Unterlagen gelten, die im Zusammenhang mit der Tätigkeit von Staat und Verwaltung stehen. Dabei darf es nicht darauf ankommen, ob die Aufgaben durch Behörden oder durch Private, an denen die öffentliche Hand mehrheitlich beteiligt ist, wahrgenommen werden. Ebenso wenig kommt es auf die Rechtsform an, in der jeweils gehandelt wird. Nur wenn sich das Recht auf Informa-

tionszugang auch auf die privatrechtlich organisierte Wahrnehmung öffentlicher Aufgaben erstreckt, können Bürgerinnen und Bürger sowie interessierte Verbände von ihrem Recht auf politische Mitgestaltung Gebrauch machen. Die Informationsfreiheitsgesetze stellen einen wichtigen Baustein unseres demokratischen Gemeinwesens dar. Sie sind ein Instrument für alle, die sich aus erster Hand Informationen über staatliches Handeln beschaffen und aktiv an der politischen Willensbildung mitwirken möchten. Damit stärken die Informationsfreiheitsgesetze die Demokratie.

Dass Gesetze, die öffentliche Stellen binden, auch für Private in öffentlicher Trägerschaft gelten, ist keineswegs neu. Beispielsweise erstreckt sich der Anwendungsbereich einer Reihe von Datenschutzgesetzen der Länder auch auf Vereinigungen des Privatrechts, bei denen die Anteilsmehrheit in der Hand des Staates liegt. Auch das Bundesdatenschutzgesetz und das Umweltinformationsgesetz des Bundes enthalten Bestimmungen zur Bindung solcher Unternehmen. Diesen Regelungen liegt eine einheitliche Motivation zu Grunde: die Rechte der Bürgerinnen und Bürger dürfen nicht von der Rechtsformwahl der öffentlichen Hand abhängen.

Der Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten Deutschlands gehören die Informationsfreiheitsbeauftragten der Länder an, in denen Informationsfreiheitsgesetze in Kraft sind.

III. Verbesserter Zugang zu den Umweltinformationen durch die neue Richtlinie der Europäischen Union (02. Juni 2004)

Das bundesdeutsche Umweltinformationsgesetz beruht auf der europäischen Umweltinformationsrichtlinie, die im vergangenen Jahr neu gefasst und wesentlich erweitert worden ist. Deshalb sind die Mitgliedstaaten der Europäischen Union verpflichtet, ihre Umweltinformationsgesetze entsprechend zu ändern.

Die Informationsbeauftragten der Länder Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein stellen fest, dass die Frist zur Umsetzung der Umweltinformationsrichtlinie bereits im Februar 2005 ausläuft. Sie fordern die Gesetzgeber auf, die Verbesserungen der europäischen Richtlinie unverzüglich in nationales Recht umzusetzen. Unter anderem verdienen folgende Punkte eine besondere Aufmerksamkeit:

Der Begriff der „Informationen über die Umwelt" ist weiter gefasst als bisher. Nunmehr sind neben Informationen zu Wechselwirkungen von gentechnisch veränderten Organismen zur Umwelt auch Angaben zum Zustand der menschlichen Gesundheit und Sicherheit, zu Belastungen der Nahrungskette und zu umweltbedingten Beeinträchtigungen bei Bauwerken offen zu legen.

Werden im Umweltbereich öffentliche Aufgaben privatisiert, so gilt das Recht auf Zugang zu Umweltinformationen auch gegenüber privaten Unternehmen.

Ein Antrag auf Zugang zu Umweltinformationen darf zum Schutz behördlicher oder privater Interessen nur noch abgelehnt werden, wenn die Abwägung entgegen stehender Interessen ein überwiegendes Geheimhaltungsinteresse ergibt.

Öffentliche Stellen wie private Unternehmen, die öffentliche Umweltaufgaben wahrnehmen, werden verpflichtet, Umweltinformationen von sich aus - auch im Internet - zu veröffentlichen.

Das Ziel des Umweltinformationsgesetzes - also die Verbesserung der Umwelt durch das Engagement der Bürgerinnen und Bürger - kann umso effektiver erreicht werden, je transparenter das Verwaltungshandeln ist. Die europarechtlich vorgegebenen Verbesserungen tragen zu mehr Transparenz bei. Bund und Länder sollten daher nicht weiter zögern, ihren Verpflichtungen nachzukommen und den Umweltinformationszugang auch in Deutschland zu stärken. Personen, die bei Bundesbehörden oder Landesbehörden, für die noch kein allgemeines Informationszugangsrecht gilt, Verwaltungsakten einsehen möchten, sind darauf besonders angewiesen.

Soweit die Umweltinformationsrichtlinie nicht allein durch ein Bundesumweltinformationsgesetz, sondern auch auf Länderebene umgesetzt werden sollte, regen die Informationsbeauftragten an, eine Zusammenführung von Umweltinformationsgesetz und allgemeinem Informationsfreiheitsgesetz in Erwägung zu ziehen. Für die Bürgerinnen und Bürger könnten Unsicherheiten vermieden werden, wenn ihre Informationsrechte in nur einem Gesetz bestimmt wären.

IV. Kommerzielle Nutzung öffentlicher Informationen – keine Nachteile für Bürgerinnen und Bürger! (02. Juni 2004)

Das Europäische Parlament und der Europäische Rat haben am 17. November 2003 eine Richtlinie verabschiedet, mit der ein Rahmen für die Weiterverwendung von Informationen des öffentlichen Sektors festgelegt wird. Durch transparente und für alle Mitgliedsstaaten gleiche Regelungen soll die Aufbereitung solcher Informationen durch private Unternehmen erleichtert sowie die Erstellung grenzübergreifender Produkte ermöglicht werden. Die Richtlinie soll das wirtschaftliche Potenzial der Informationsgesellschaft unter gleichen Wettbewerbsbedingungen fördern. Die europäischen Vorgaben sind spätestens bis zum 1. Juli 2005 in nationales Recht umzusetzen.

Die Richtlinie betrifft ausschließlich Informationen, die aufgrund der bestehenden Rechtslage in den Mitgliedsstaaten bereits zugänglich sind, und legt einen Gebührenrahmen für deren Weiterverwendung fest. Während die Informationsfreiheitsgesetze nur

eine begrenzte Kostenerhebung vorsehen, um die Bürgerinnen und Bürger nicht von der Antragstellung abzuhalten, können für die kommerzielle Nutzung von Informationen auf der Grundlage der Richtlinie jedoch höhere Gebühren erhoben werden. Sogar eine Gewinnspanne für die Verwaltung ist vorgesehen. Dies bedeutet, dass öffentliche Stellen, die beabsichtigen, für die kommerzielle Verwendung ihrer Informationen höhere Kosten als bisher zu verlangen, erst einmal erfragen müssen, zu welchem Zweck der Informationszugang überhaupt beantragt wird. Wesentliches Merkmal der Informationsfreiheitsgesetze ist jedoch, dass niemand begründen muss, wozu sie oder er die Informationen verwenden möchte.

Die Informationsbeauftragten der Länder Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein fordern, dass bei der Umsetzung der Richtlinie nicht nur die Vorteile der Kommerzialisierung, sondern auch die Belange der Bürgerinnen und Bürger berücksichtigt werden:

Die Nutzung der Informationsfreiheit für private Zwecke darf nicht eingeschränkt werden. Bürgerinnen und Bürger, die bei öffentlichen Stellen den Zugang zu Informationen beantragen, müssen dieses Recht nach wie vor ohne Begründung ihres Antrages ausüben können.

Die Höhe der für den Informationszugang erhobenen Gebühren darf nach wie vor nicht von einer Antragsstellung abschrecken. Das Bürgerrecht auf Informationsfreiheit darf nicht durch die Hintertür der Kostenerhebung ausgehöhlt werden.

Auf Bundesebene muss endlich das im Koalitionsvertrag der Regierungsparteien vereinbarte Informationsfreiheitsgesetz verabschiedet werden. Nur auf dessen Grundlage ist es für alle Bürgerinnen und Bürger möglich, im gemeinsamen europäischen Binnenmarkt an den gesellschaftlichen und wirtschaftlichen Vorteilen der Informationsgesellschaft teilzuhaben.

Da die Bundesrepublik Deutschland in der Europäischen Union eines der Schlusslichter in der Informationsgesetzgebung ist, sollte der Gesetzgeber diesen europarechtlichen Impuls aufgreifen und auch auf Bundesebene einen freien Zugang zu Informationen schaffen. Bislang besteht das Recht auf Akteneinsicht nur in Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein sowie bundesweit in Bezug auf Umweltinformationen.

V. Öffentlichkeit der Sitzungen von Entscheidungsgremien (22. November 2004)

Die Forderung nach einer gesetzlichen Regelung der Informationsfreiheit wird bisher in Deutschland nur mit dem Recht auf Zugang zu Informationen in Verbindung gebracht, die bei den Behörden in Form von Akten, elektronisch gespeicherten Daten oder anderer

Datenträger vorhanden sind. Von ebenso großer Bedeutung für die Transparenz staatlicher Entscheidungsfindung ist jedoch die Möglichkeit der Teilnahme an den Sitzungen von Gremien, die in einer Vielzahl öffentlicher Stellen mit erheblichen Entscheidungsbefugnissen ausgestattet sind.

Die Öffentlichkeit von Gerichtsverhandlungen ist eine der frühen Errungenschaften des Rechtsstaates. Obwohl auch Plenarsitzungen von Parlamenten von jeher öffentlich stattfinden, tagen in vielen Ländern aber die Landtagsausschüsse in der Regel nach wie vor nichtöffentlich. Dies ist auch auf der kommunalen Ebene der Fall. Bei anderen öffentlichen Stellen, deren Entscheidungen durch demokratische Mitwirkungsgremien legitimiert werden, wie z.B. Bildungs-, Sozial- oder Versorgungseinrichtungen, sind nichtöffentliche Sitzungen die Regel.

Transparenz staatlichen Verhaltens erfordert aber im Gegenteil, dass auch die Entscheidungsfindung staatlicher Gremien grundsätzlich in der Öffentlichkeit stattfindet. Dies schließt nicht aus, dass für bestimmte Bereiche (z.B. Personalentscheidungen oder Verschlusssachen) oder von Fall zu Fall (z.B. wenn der Schutz personenbezogener Daten dies erfordert) die Öffentlichkeit ausgeschlossen wird.

In den USA wurde in der Folge der Gesetzgebung zur Informationsfreiheit im Rahmen der „Government in the Sunshine Acts" sowohl auf der Ebene des Bundes als auch der Einzelstaaten festgelegt, dass der Meinungsaustausch in behördlichen Kollegialsitzungen im Lichte der Öffentlichkeit durchzuführen ist. Ort, Zeitpunkt und Gegenstand der Sitzungen sind vor dem Termin öffentlich bekannt zu machen. Der Ausschluss der Öffentlichkeit ist zu begründen. Nichtöffentliche Sitzungen sind zu protokollieren, damit der Inhalt von Sitzungen, bei denen die Öffentlichkeit widerrechtlich ausgeschlossen wurde, nachvollziehbar bleibt.

Die Arbeitsgemeinschaft der Informationsbeauftragten der Länder Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein fordern, dass der Grundsatz der Öffentlichkeit von Sitzungen für alle Gremien eingeführt wird. Diese stellen ihre Verantwortung gegenüber dem Gemeinwohl vor allem dadurch unter Beweis, dass Bürgerinnen und Bürgern Zugang zu den Sitzungen von staatlichen Gremien erhalten. Der Ausschluss der Öffentlichkeit ist nur für bestimmte und abschließend zu regelnde Tatbestände zuzulassen.

Stichwortverzeichnis

Abgabenordnung 143
Abonnentendaten 53
Abrechnungsdaten 53
Abrufverfahren 153
Adressdatei 51
Adresshandel 28
Akteneinsicht 113, 132, 146, 163, 174
Allgemeinen Schulordnung 132
Amtsgeheimnis 135
Angemessenheits-entscheidungen 151
anonyme Nutzungs-möglichkeiten 16
Anrufmanagementsysteme 10
APIS (Arbeitsdatei PIOS-Innere Sicherheit) 82
Arbeitnehmer-datenschutzgesetz 120
Arbeitsverhältnis 46
Archivgesetz 133
Archivgut 133, 135, 136
Aufbewahrung 83
Aufbewahrungsfrist 132
Auftragsdatenverarbeitung 53, 65
Ausfallrisiko 58, 60
Auskunftei 56, 58, 124
Auskunftsdaten 33
Auskunftspflicht 148, 158
Auskunftsrecht 60
Ausweiskontrolle 141
Authentifizierungsverfahren 146
automatisierte Einzelentscheidung 66
Barcode 50
Bauunterlagen 170
Bedarfsgemeinschaft 109
Bekanntmachungspflicht 161
Beobachtung 43, 77
Beobachtungsbogen 107
berechtigtes Interesse 39, 57, 137
berufliche Schweigepflicht 155
Berufsgeheimnis 135
Besucherdaten 141
betriebliche Datenschutzbeauftragte 48, 155
Betriebsgeheimnisse 175
Betriebssystem 17
Bildaufnahmen 42
Bildaufzeichnung 79
Bildübertragung 76
BIOS 17
Blacklists 34
Blockierungsmechanismen 8
Bluetooth 18
Bonität 55, 60
Bonitätsauskunft 58, 59, 64
Bonitätsbewertung 60
Bonitätsdaten 56, 57
Bonitätsprüfung 66
Call-Center 51
Chipkartensystemen 7
Computerviren 12
Credit-Scoring 66
Data Mining 9
Data Warehouse 9
Datenabfrage 154
Datenlöschung 114
Datenschutzbeauftragte 153
Datenschutzkontrollstellen 152
Datenschutzleitlinien 107
Datenschutzniveau 71

Datensicherheit 94
Datensicherheitskonzept 103
Datensicherungsbänder 24
Datensparsamkeit 16, 28
Datenspeicherungen 11
Datensperrung 114
Datenvermeidung 28, 44, 124
Datenvorratshaltung 129
Dienstverhältnis 89
Direktwerbung 34
Diskriminierungsverbot 63
DNA 87
DNA-Analysen 2
Düsseldorfer Kreis 156
Einverständniserklärungen 84
Einwilligung 33, 37, 52, 53, 57, 65, 97, 99, 123, 125, 128, 130, 134, 140
Einwilligungserklärung 129
Einwilligungslösung 115
elektronische Patientenakte 118
elektronisches Informationsverfahren 131
elektronisches Rezept 118
ELSTER „Elektronische Steuererklärung 145
Erforderlichkeit 99, 142
Erhebungsbeauftragte 148
Ermittlungsgeneralklausel 90
Evaluationsordnung 123
Fahrzeugregister 138
Familienstammbaum 35
Fernmeldegeheimnis 10, 31, 89
Festplatte 24
Filmaufnahmen 84
Fingerabdrücke 5, 87
Firewire 17
Forschungsdaten 127
Funkchips 3
Funk-Schnittstellen 18
Funktionsübertragung 65
gebrauchte PCs 23
Gebührenerhebung 174
Gedenkstätte Yad Vashem 133
Geheimhaltungsinteresse 113, 170, 176
Geheimhaltungsvorschriften 135
Gemeindeordnung 139, 160
genetischer Fingerabdruck 87
Gesamtkonzept 78
Geschäftsgeheimnis 6, 164, 167, 169
geschlossene Benutzungsgruppe 12
Gesetz gegen den unlauteren Wettbewerb 33
Gesundheitsdaten 27, 110
Gesundheitsdatenschutzgesetz 114
Gesundheitskarte 117
großer Lauschangriff 5, 86
Grundschutzhandbuch 19
Grundsicherung 98
Hackerangriffe 12
Halterauskünfte 138
Hartz IV 108
Hausrecht 41
heimliche Vaterschaftstests 2
Hinweisschilder 46, 47
Hochschulgesetz 122
Homebanking 26
Homepage 35
Identifikationsmerkmale 143
Identifikationsnummer 143, 145
Identifizierung 33
Identifizierungsmerkmale 4
Identitätsdaten 70
Informationsanspruch 165, 172
Informationsantrag 165
Informationsfreiheitsgesetz 163
Informationspflicht 158
Informationspolitik 173

Informationszugang 159, 168, 172, 173, 175
Informationszugangsrecht 160, 176
Insolvenzdaten 38, 93
Insolvenzordnung 38
Integrität 13
Interessenabwägung 45, 54
Interessenkollisionen 104
Internationaler Datenverkehr 151
Internetprotokoll 30
Internetveröffentlichung 137
Inverssuche 29
IT-Strukturanalyse 20
Kaufkraftbewertung 56
Kaufkraftdaten 55
Kennzeichnungspflichten 5
Kernbereich privater Lebensgestaltung 86
Kommunikationsdaten 31
Kontenkontrollen 144
Kontenzugriffs 4
Kontoauszüge 95
Konzerndatenschutzregelung 152
Kopierschutz 94
Körperzellen 87
Krebsregistergesetz 114
Kreditfabriken 64
Kriminalakten 83
Kunsturhebergesetz 42
Landesarchiv 133
Lesezugriffe 69
Löschfunktionen 23, 25
Löschprogamm 24
Löschung 11, 23, 83, 117
Löschungsfristen 94, 142
Löschungspflichten 83
Medienprivileg 39
Mehrfachnutzung 153
Melderegister 144
Melderegisterauskunft 32
mikro-geografische Daten 62
Mindestspeicherdauer 72
Missbrauchskontrolle 153
Mobilfunkgeräte 25
Notrufnummer 79
Nutzungsprofile 15
Nutzungszwang 8
Online-Umfragen 36
Online-Updates 12
Ordnungswidrigkeiten 57, 139
Organisationsmangel 68
Passagierdaten 71
Passagierdatenbanken 70
Passagierdatenübermittlung 72
passenger name record 70
Patientenakten 27, 92, 114
Patientendaten 91, 114
Payback-Karten 49
Personalausweisnummer 28
Personenbeziehbarkeit 56
Personenkennzeichen 4, 143, 145
Personenkennziffer 145
Persönlichkeitsrecht 42, 45, 47
Polizeigesetz 76
Portallösung 32
Prangerwirkung 37
prepaid-Handys 29
Pressefreiheit 39
Privatgespräche 88
Privatsphäre 139
Protokollierung 68
Prüfungsakten 27
Prüfungsprotokolle 124
Pseudonymisierung 115, 127
Push-Lösung 72
Rasterfahndung 76, 79, 80
Ratsmitglieder 139
Recht am eigenen Bild 42, 84, 85
rechtliche Interessen 131
Regelungszweck 160
RFID-Chips 7, 49

richterliche Anordnung 5, 91
richterlichen Entscheidung 87
Risikoanalyse 12
Rundfunkänderungs-
staatsvertrag 28
Rundfunkfinanzierung 28
Sachverständige 91
Schätzdaten 59
Schengener Informations-
system 141
Schlüsselverwaltung 22
Schnittstellen 17, 20
SCHUFA 57, 66
Schulverwaltungsgesetz 130
Schutzbedarfsermittlung 20
Schutzprofile 13
schutzwürdige Interessen 47, 54,
125
Schutzzweck 159
Schwärzung 97
Schweigepflicht 100, 112, 113
Schweigepflichtentbindungs-
erklärungen 92
Score-Wert 60
Scoring 3, 60
sensitive Daten 62
Sicherheitsfunktionen 15
Sicherheitskonzept 12, 16, 19, 22,
122, 154
Sicherheitsmaßnahmen 21, 24
Sicherheitsniveaus 23
Sicherheitsrisiken 16
Sozialdaten 99
Sozialgeheimnis 97
Sozialhilfebezug 97
sozio-demografische Daten 62
Spam-Abwehr 34
Spamfilter 34
Speichelprobe 2
Speicherdauer 41, 76
Speicherkapazität 16
Speichermedien 16, 18, 25
Sperrfristen 133, 137
Sperrung 117
Statistikdaten 149
Steuerakten 146
Steuerehrlichkeit 4
Studiengebühren 121
Studierendendaten 121
TCP = Trusted Computing
Platform 14
Technikfolgenabschätzung 9
Teledienstedatenschutzgesetz 32
Telefonauskunft 30
Telefonwerbung 33, 51
Telekommunikationsdienste 10
Telekommunikationsgesetz 89
Telekommunikations-
überwachung 30
TPM = Trusted Platform
Modul 14
Transaktionsdaten 26
Transparenz 13, 15, 62, 63, 72,
139, 161
Transparenzgebot 145, 146
Trennungsgebot 171, 174
Übermittlungsbefugnis 130
Übertragungstechniken 18
Überwachungskameras 45, 77
Überwachungsmaßnahmen 30
überwiegendes Interesse 169
UMTS 30
Umweltinformationsgesetz 163,
175
unerwünschte Werbung 33
Unterhaltsvermutung 109
Unternehmensregelungen 152
Unverhältnismäßigkeit 40
Urhebergesetz 170
Urheberrechte 170
verantwortliche Stelle 65, 117

verbindliche Unternehmensregelungen 151
Verbindungsdaten 88, 91
Verbunddatei 153
Verdachtsschöpfungsmethode 79, 81
Verdrängungseffekt 77
Verfassungsschutzbericht 75
Verfügbarkeit 15
Verhaltensprofile 4
Verhältnismäßigkeit 28, 81
Verhältnismäßigkeitsgrundsatz 78
Verkehrsdaten 12
Verknüpfung 50
Veröffentlichung 75
Veröffentlichungsbefugnis 136
Verschwiegenheit 148
Vertrauenswürdigkeit 14
Vertraulichkeit 12, 13, 15, 33, 167
Vertraulichkeitsvereinbarung 168
Verweigerungsgründe 168
Videoaufzeichnung 77
Videobeobachtung 78
Videokameras 43
Videoüberwachung 40, 43, 45, 46, 76
Voice over IP 9
Vorabkontrolle 48, 122, 130, 154
Vorkaufsrecht 138
Vorratsdatenspeicherung 3, 31, 32
Wartungstätigkeiten 15
WebCam 43
Werbeadressaten 51
Werbezwecke 52
Werturteile 37
Wettbewerbsfähigkeit 169
wirtschaftliches Interesse 165
W-LAN 18
Zentraldatei 4
zentrales Einwohnerregister 143
Zugangskontrollsysteme 22
Zugangsrecht 163
Zugangsregelung 159, 161
Zugriffsberechtigungen 95
Zugriffsberechtigungskonzept 110
Zugriffskontrolle 39
Zugriffsrechte 118
Zurechenbarkeit 13
Zustimmung 105
Zwangsidentifizierung 28
Zwangsversteigerungsdaten 93
Zweckbestimmung 53
Zweckbindung 99, 144
Zweckbindungsgrundsätze 154
Zwecke, persönliche und familiäre 35
Zwischenspeicherung 11

Datum: .....

Absender/in:

.....
(Vorname, Name)

.....
(ggf. Behörde)

.....
(Straße, Hausnummer)

.....
(PLZ, Ort)

Landesbeauftragte
für Datenschutz und Informations-
freiheit Nordrhein-Westfalen
Reichsstraße 43

40217 Düsseldorf

Betr.: Informationsmaterial

Hiermit bitte ich um Übersendung folgender Broschüren:

_____ Aufkleber zum Adressenhandel

_____ Datenscheckheft

_____ Datenschutzrecht des Landes NRW

_____ den neuesten Datenschutzbericht

_____ den ..... Datenschutzbericht

_____ Datenschutzgerechtes eGovernment

_____ Faltblatt Achtung Kamera – Videoüberwachung
durch private Stellen

_____ Faltblatt Adressenhandel und unerwünschte Werbung
Faltblatt Datenschutz ... ist Ihnen egal?

_____ Faltblatt Datenschutz im Verein

_____ Faltblatt Handels- und Wirtschaftsauskunfteien

_____ Handys - Komfort nicht ohne Risiko

_____ Faltblatt zum Informationsfreiheitsgesetz NRW: informieren – einmischen – mitreden – Tipps und Informationen für Aufgeweckte

_____ Orientierungshilfe Behördliche Datenschutzbeauftragte

_____ Orientierungshilfe Schulen ans Netz

_____ Orientierungshilfe Datenschutz und Datensicherheit beim Betrieb von IT-Systemen

_____ Orientierungshilfe Datenverarbeitung im Auftrag

_____ Orientierungshilfe Telefax

_____ Orientierungshilfe Unterlagenvernichtung

_____ Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

_____ Serviceorientierte Verwaltung „Vom Bürgerbüro zum Internet"

_____ Tagungsband: Sommersymposium Informationsfreiheit

Mit freundlichen Grüßen

Notizen

Notizen

Notizen

Notizen

N W.

http://www.ldi.nrw.de