Achtzehnter Datenschutz- und Informationsfreiheitsbericht

der

Landesbeauftragten für Datenschutz

und Informationsfreiheit

Nordrhein-Westfalen

Bettina Sokol

für die Zeit vom 1. Januar 2005

bis zum 31. Dezember 2006

Herausgeberin:

Landesbeauftragte für Datenschutz
und Informationsfreiheit
Nordrhein-Westfalen
Bettina Sokol
Kavalleriestraße 2–4

40213 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.

ISSN: 0179-2431
Düsseldorf 2007

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorbemerkung

Auch nach einem Jahr hat es sich noch nicht überall herumgesprochen: Die Dienststelle ist innerhalb Düsseldorfs umgezogen und hat ihren Sitz jetzt in der Kavalleriestraße 2-4. Der Wechsel in ein anderes Gebäude war notwendig geworden, nachdem die "frühere Heimat" der Dienststelle – eine Landesliegenschaft – verkauft worden war.

Kontinuität wurde gleichwohl in etlichen Bereichen der inhaltlichen Arbeit gewahrt. So konnten auch 2005 und 2006 wieder jeweils gut besuchte Tagungen gemeinsam mit dem Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster veranstaltet werden. Unter dem Titel "Total Transparent – Zukunft der informationellen Selbstbestimmung?" wurde 2005 danach gefragt, wie weit wir uns schon auf dem Weg in eine Rechts- und Gesellschaftsordnung befinden, in der viele Menschen nicht nur den tatsächlichen Überblick darüber verloren haben, wo überall sich welche Daten zu ihrer Person befinden, sondern in der sie selbst mit kräftigstem Bemühen nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Welche Konsequenzen die Ergebnisse der Hirnforschung möglicherweise künftig für die Manipulierbarkeit der Menschen und damit für die Persönlichkeitsrechte haben könnten, war 2006 das Tagungsthema. Die Dokumentationen beider Veranstaltungen sind jeweils als Broschüre erhältlich und unter www.ldi.nrw.de im Netz abrufbar.

Kontinuität bei der Bearbeitung der jährlich steigenden Zahl von Anfragen und Beschwerden zu wahren, wird indes gerade vor dem Hintergrund von Personalkürzungen immer schwieriger. Daher sei meinen Mitarbeiterinnen und Mitarbeitern an dieser Stelle auch öffentlich sehr, sehr herzlich für ihr gleichbleibend hohes Engagement gedankt.

1 Zur Situation von Datenschutz und Informationsfreiheit

Nein, Sie haben nichts zu verbergen! Muss Ihr Leben deshalb aber gleich präventiv überwacht werden? 23. Juli 2009: Tanja Z. wird um 6.45 Uhr von ihrem Radio geweckt und gönnt sich noch ein gemütliches Viertelstündchen im Bett. Nachdem sie das Radio um 7.00 Uhr ausgeschaltet und eine halbe Stunde in ihrem Badezimmer verbracht hat, lässt sie sich während ihres Frühstücks in der Küche von verschiedenen Radiosendern abwechselnd über Neuigkeiten informieren und mit netter Musik auf den Tag einstimmen. Um 8.00 Uhr geht sie aus dem Haus, besorgt sich beim Kiosk um die Ecke noch schnell eine Tageszeitung für die Fahrt zur Arbeit und steigt um 8.09 Uhr an der Goethestraße in den Bus, den sie um 8.42 Uhr an der Salvador-Allende-Straße wieder verlässt. Ihre täglichen Naschereien – wobei sie zwischen Schokolade, Weingummi und Lakritz wechselt – holt sie sich noch schnell um 8.50 Uhr im Supermarkt neben ihrer Arbeitsstelle, die sie dann, je nach Länge der Schlange an der Kasse, spätestens um 9.00 Uhr betritt.

Darauf, die weiteren Einzelheiten des Tagesablaufs von Tanja Z. minutiös zu protokollieren, wird hier verzichtet. Ein "Protokoll" dessen, wo und wann sich Tanja Z. online informiert, wo und wann sie im Netz einkauft, wo und wann sie mit wem anderweitig auf elektronischem Wege kommuniziert, wird allerdings aller Voraussicht nach am 23. Juli 2009 existieren. Wenn es nicht gelingt, die im Bereich der Telekommunikation geplante Vorratsdatenspeicherung noch zu verhindern, wird jede banale Alltagshandlung, die mit Hilfe elektronischer Kommunikationsmittel ausgeführt wird, festgehalten werden. Mit wem wann wie lange und von wo aus telefoniert wird oder mit wem wann von wo aus E-Mails ausgetauscht werden, ist dann ebenso mindestens sechs Monate lang nachvollziehbar wie der Umstand, welche Internetseiten informationshalber oder für Einkäufe aufgerufen wurden und an welchem Standort sich eine Person aufgehalten hat, die mit einem eingeschalteten Handy unterwegs war. Erstmals sollen die Dienstleistungsunternehmen im Bereich der Telekommunikation, des Internetzugangs und der E-Mail-Dienste verpflichtet werden, die eben genannten Telekommunikationsdaten – die unter dem Begriff der Verkehrsdaten zusammengefasst werden – auf Vorrat zu speichern, um sie für einen möglichen Bedarf der Behörden vorzuhalten. Dies betrifft sämtliche

Verkehrsdaten, also auch diejenigen Daten, die die Unternehmen für ihre eigenen Zwecke gar nicht benötigen, zum Beispiel Standortdaten oder Verkehrsdaten bei Flatrate-Vereinbarungen und sogar bei kostenlosen Diensten. Die damit entstehenden gigantischen Datenmengen können außerordentlich aussagekräftige Profile der elektronischen Kommunikation jeder Person bilden. Die Verhältnismäßigkeit der Vorratsdatenspeicherung ist mehr als zweifelhaft und damit auch ihre Verfassungsmäßigkeit.

Maßlosigkeit und sogenannte Vorfelderfassungen sind zwei Stichworte, die das Recht auf informationelle Selbstbestimmung immer stärker in Bedrängnis bringen. Die im Aufbau befindliche gemeinsame Datei von Bundes- und Landesbehörden der Polizei und des Verfassungsschutzes soll auch präventiven Zwecken dienen. Sie wirft nicht nur Fragen im Hinblick auf die Einhaltung des Trennungsgebots auf. Problematisch ist insbesondere die Aufnahme von Personen in die Datei, die als Begleit- und Kontaktpersonen gespeichert werden, aber kaum hinreichend bestimmbar sind. Auch wenn nur flüchtige oder zufällige Kontakte nicht genügen sollen, bleibt die Regelung doch viel zu vage. Gilt danach schon die gutnachbarschaftliche Plauderei im Treppenhaus als Umstand, der den Status einer Kontaktperson begründen kann? Landet schon die Professorin als Kontaktperson in der Datei, weil sie einen Studenten im Seminar sitzen hat, der in der Datei erfasst ist? Auch die große Zahl der zugriffsberechtigten Behörden ist ebenso bedenklich wie die Möglichkeit, neben den vorfestgelegten Datenarten frei wählbare, ergänzende Hinweise und Informationen einspeichern zu können.

Am Ende des Berichtszeitraums war über die Beschwerde gegen die Entscheidung eines Ermittlungsrichters beim Bundesgerichtshof noch nicht entschieden. In der Entscheidung des Ermittlungsrichters jedenfalls war für den Strafprozess immerhin festgestellt worden, dass es mangels Rechtsgrundlage den Behörden nicht erlaubt ist, sich heimlich Zugriff auf Computerfestplatten von Beschuldigten zu verschaffen. Ein Eingriff von solch hohem Gewicht sei nicht mit einer regulären Wohnungsdurchsuchung, die mit Wissen der Betroffenen stattfinde, vergleichbar, sondern entspreche schon wegen der möglichen Sensitivität der Dateien am ehesten dem großen Lauschangriff, also dem Belauschen vertraulicher Gespräche in einer Wohnung. Das neue Verfassungsschutzgesetz Nordrhein-Westfalen räumt dem Verfassungsschutz

jetzt allerdings genau diese Möglichkeit ein, sich unbemerkt auf fremden Festplatten umzuschauen. Dann können Internet-Aktivitäten nachvollzogen und überwacht, gespeicherte E-Mails ausgelesen und die eingerichteten Dateien durchsucht werden. Dabei kann der Verfassungsschutz auch auf Steuererklärungen, Gesundheitsdaten, Tagebuchaufzeichnungen, Liebesbriefe oder ähnliche intime und hochsensible Information stoßen. Somit wäre unter Umständen der Kernbereich privater Lebensgestaltung betroffen, der nach der Rechtsprechung des Bundesverfassungsgerichts absolut geschützt und jedem staatlichen Zugriff entzogen bleiben muss. Ausdrückliche Regelungen zum Schutz der individuellen Entfaltung in diesem Kernbereich sind allerdings nicht vorgesehen, so dass diese Befugnis ebenso verfassungsrechtlichen Bedenken begegnet, wie die unveränderte Beibehaltung der Regelung zur akustischen Wohnraumüberwachung.

Präventiv soll auch die stetig wachsende Zahl von Videoüberwachungskameras wirken. Daran mag in den meisten Fällen gezweifelt werden. Zwar werden erheblich mehr Videoüberwachungssysteme durch Unternehmen und Privatleute betrieben als durch staatliche Stellen, doch darf es aus der Perspektive der Betroffenen nicht zu einer flächendeckenden Rundumüberwachung auf Schritt und Tritt durch wen auch immer kommen. Wie stets gilt auch hier, dass vorhandene Datenbestände Begehrlichkeiten für andere als die ursprünglich festgelegten Verwendungszwecke wecken. Wenn die automatische Gesichtserkennung über kurz oder lang treffsicher funktioniert, werden die Risiken für die informationelle Selbstbestimmung bei der Videoüberwachung einen Quantensprung machen.

Prävention bestimmt auch in weiten Teilen der Wirtschaft das Denken. Kundschaft ist nicht mehr generell königlich. Fast könnte gesagt werden, dass nur noch die durchleuchteten und danach für zahlungskräftig und verlässlich genug erachteten Personen in den Genuss einer stigmatisierungsfreien Teilhabe am Wirtschaftsleben kämen. Für die Betroffen ist derzeit jedenfalls zumeist nicht durchschaubar, nach welchen Kriterien sie im Scoring – etwa der Kreditwirtschaft – bewertet werden oder in welchem Hinweis- und Informationssystem eines Wirtschaftszweiges Daten zu ihrer Person rege ausgetauscht werden. Und auch hier sind gigantomanische Tendenzen erkennbar: Es wird an Daten gesammelt, was sammelbar ist. Ihr nicht gerade kleines Scherflein – beispielsweise im Versandhandel – tragen die Auskunf-

teien bei, die darüber informieren, zu welchen Personen bei ihnen negative Einträge betreffend die Kreditwürdigkeit vorliegen.

Maßlosigkeit und zweifelhaftes Präventionsdenken sind bei nichtöffentlichen Stellen und im öffentlichen Bereich zu beobachten, wie beispielsweise bei der im April 2006 vom Bundesverfassungsgericht festgestellten Verfassungswidrigkeit der Rasterfahndung nach dem 11. September 2001. Überdies sind die heutigen und künftigen Möglichkeiten einer technischen und rechtlichen Infrastruktur für einen Weg in eine fast jede Lebensregung kontrollierende staatliche und gesellschaftliche Gemeinschaft jedenfalls gegeben. Das ist alarmierend.

Im Bereich der Informationsfreiheit gibt es demgegenüber für die Rechte der Bürgerinnen und Bürger positivere Tendenzen zu vermelden. So nimmt sich auch die Verwaltung immer mehr der Ziele des Informationsfreiheitsgesetzes Nordrhein-Westfalens an. Allerdings müssen manch' hartnäckige Informationsverweigerer erst mit Hilfe von Beanstandungen oder gar gerichtlicher Feststellungen dazu gebracht werden, ihren Informationspflichten nachzukommen. Umso erfreulicher sind dann jedoch klare und eindeutige Entscheidungen von Gerichten, die über den Einzelfall hinaus Verbindlichkeit erlangen. So zum Beispiel im langjährigen Streit um die Anwendbarkeit des Informationsfreiheitsgesetzes NRW auf Industrie- und Handelskammern. Auch die Auseinandersetzungen um das Verhältnis des Informationsfreiheitsgesetzes NRW zu § 29 Verwaltungsverfahrensgesetz NRW und zu § 25 Sozialgesetzbuch Zehntes Buch sind mittlerweile gerichtlich so entschieden worden, dass die von mir vertretene Auffassung bestätigt worden ist und die Gesetze nebeneinander anwendbar sind. Nicht zutreffend bemessene Gebühren sind ebenfalls gerichtlich korrigiert worden. Insgesamt ist zu sagen, dass das 2001 von allen Landtagsfraktionen einstimmig verabschiedete Informationsfreiheitsgesetz NRW grundsätzlich ein Erfolgsmodell ist. Es ist in einigen Punkten aber auch noch verbesserungsfähig – so zum Beispiel in Bezug auf die Regelung der Betriebs- und Geschäftsgeheimnisse im Verhältnis zu den Allgemeininteressen an der Offenbarung von möglicherweise unlauteren Praktiken von Unternehmen. Hier wäre zudem eine Diskussion über ein Verbraucherinformationsgesetz wünschenswert.

2 Technik

2.1 Kommunikation über Wireless LAN (WLAN)

WLAN-Kommunikation erfreut sich mittlerweile einer großen Einsatzbreite. Die hohe Übertragungsgeschwindigkeit – verbunden mit der drahtlosen Anbindung – bietet Einsatzmöglichkeiten vom Anschluss privater PCs an das Internet, über das Angebot öffentlicher Hotspots, beispielsweise in Hotels oder auf Flughäfen, bis hin zum Aufbau und Betrieb firmen- und behördeninterner Netze. Wegen der Risiken der Funkkommunikation sind bei WLAN-Netzen umfangreiche Sicherheitsbetrachtungen durchzuführen. Besondere Aufmerksamkeit ist geboten, wenn sensible, personenbezogene Daten verarbeitet werden.

Die weitere technische Entwicklung im Bereich WLAN gibt Anlass, dieses Thema erneut aufzugreifen. Basis ist nunmehr der fortgeschriebene Standard IEEE 802.11i. Ein wesentliches neues Merkmal ist der verbesserte Schutz vor unbefugter Kommunikationsaufnahme sowie die robustere und flexiblere Verschlüsselung über WPA (WI-FI Protected Access der Herstellervereinigung Wi-Fi-Alliance). Der Algorithmus der Version WPA2 arbeitet im Unterschied zum alten WEP Standard mit dynamischer Schlüsselverwaltung, verbesserter Initialisierung beim Kommunikationsaufbau sowie größerer Schlüssellänge und sollte deshalb eingesetzt werden.

Daneben sollten WLAN-Router im geschlossenen Modus betrieben werden, das heißt, der Name (SSID = Service SET Identifier) sollte nicht im Funkverkehr bekannt gegeben werden. Es sollte eine strenge Authentisierung nach IEEE 802.11i erfolgen. Weiter sollten die Filter zur Kontrolle der zugelassenen Geräte nur die Netzadressen (MAC Adresse) der eigenen, bekannten Clients zulassen. Router mit Firewall sollten benutzt werden. Gegebenenfalls ist die Sendeleistung zu reduzieren.

Ergänzend zur Sicherung der Funkschnittstelle sollte ein VPN-Kanal (VPN = Virtual Private Network) vom Client zum Server aufgebaut und damit eine Ende-zu-Ende-Verschlüsselung erreicht werden. Insgesamt ist darauf zu achten, geeignete Produkte zu finden, die die Forderungen der neuen Norm erfüllen, sich mit den Möglichkeiten der Siche-

rung vertraut zu machen und diese für einen sicheren Betrieb umzusetzen und zu administrieren.

➡ Alle Hinweise zum Datenschutz in drahtlosen Netzen sind in einer Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder zusammengefasst, die unter www.ldi.nrw.de veröffentlicht ist.

2.2 Mobile Endgeräte und Push-Dienste, die neuen Datenverteiler

Personal Digital Assistents (PDA) sollen zunehmend auch dafür eingesetzt werden, E-Mails, Kalender- und Kontaktinformationen, die am stationären Arbeitsplatz vorliegen, mit Hilfe von Push-Diensten direkt über das Internet und das Mobilfunknetz an die mobilen Endgeräte weiterzuleiten. Um die Inhalte zu schützen, sind hierbei allerdings hohe Sicherheitsanforderungen zu erfüllen.

Push-Dienst oder Server-Push beschreibt eine meist internetbasierte Methode der Inhalteverbreitung. Hierbei werden Informationen von einem zentralen Server nach Vorgaben der Empfängerinnen und Empfänger an diese ausgeliefert. Beispielsweise können E-Mails wie eine SMS auf das Handy geschickt werden. Dafür wird die Übertragungstechnik des Mobilfunknetzes genutzt, die eine ständige Internet-Verbindung ermöglicht. Die Mails werden nach Erstellung auf dem Server sofort geliefert (gepusht), ohne dass der Client eine Anfrage starten muss.

Die Kommunikation über das Mobilfunknetz und der Einsatz kleiner, mobiler, universell nutzbarer Endgeräte beinhalten allerdings eine Reihe von Risiken. Um insbesondere den Zugriff Unbefugter auf die versandten und mobil gespeicherten Informationen zu verhindern sowie den vorhandenen Sicherheitsstandard interner Netze nicht abzusenken und damit die hier gespeicherten Daten zu gefährden, ist eine geeignete Sicherheitsarchitektur aufzubauen. Bekannt geworden und auch häufig eingesetzt wurde der Blackberry, der von Anfang an unter Sicherheitsaspekten konzipiert wurde. Zu kritisieren war allerdings der Einsatz herstellerspezifischer, nicht offen gelegter Sicherheitsprodukte sowie der Einsatz eines zentral in Großbritannien platzierten Routing

Centers, über das alle Meldungen gesteuert wurden. Insofern wurde in der Landesverwaltung nach alternativen Lösungen gesucht.

Aufgrund der erwähnten Risiken muss eine geeignete Sicherheitsarchitektur für den Einsatz eines Push-Dienstes folgende Merkmale umfassen:

- Ende-zu-Ende-Verschlüsselung des Kommunikationsweges mit sicheren Algorithmen und geeigneter Schlüsselverwaltung
- Zusätzliche Verschlüsselung vertraulicher Nachrichten
- Verbindungsaufbau nur vom internen Netz ausgehend
- Geschütztes, zusätzlich abgesichertes Endgerät mit verschlüsselter Speicherung der Daten und eingeschränkten Nutzungsmöglichkeiten für Dienste
- Zentrale Administration der Endgeräte

  ➧ Es ist zu begrüßen, dass die Landesverwaltung diese Dienste nur unter strenger Beachtung aller Sicherheitsauflagen freigeben will. Öffentliche und private Stellen sollten derartige Dienste nur bei Erfüllung aller Sicherheitsauflagen nutzen.

2.3 Datensicherheit bei Endgeräten

Beschwerden im Zusammenhang mit dem Einsatz von IT-Endgeräten zeigten, dass insbesondere die organisatorischen und technischen Sicherheitsmaßnahmen bei der Beschaffung, beim Einsatz und bei der Entsorgung der Geräte nicht ausreichend getroffen waren. Veröffentlichungen und Statistiken belegten ebenfalls, dass bei Datensicherheitsmängeln in erster Linie Benutzerinnen und Benutzer Schäden verursachten. Eine Fragebogenaktion sollte deshalb einen aktuellen Überblick über die getroffenen Datensicherheitsmaßnahmen geben.

Zielgruppe dieser Umfrage waren jeweils zehn Kreditinstitute, Versicherungen und mittelgroße Städte. Die befragten Stellen hatten die Möglichkeit, unter den beiden Hauptaspekten "technisch" und "organisatorisch" jeweils den Stand der Umsetzung (realisiert, geplant, nicht vorgesehen) der aufgeführten Maßnahmen anzukreuzen.

Die folgende Grafik gibt einen Überblick über die Zahl und Art des Einsatzes der gemeldeten Endgeräte:

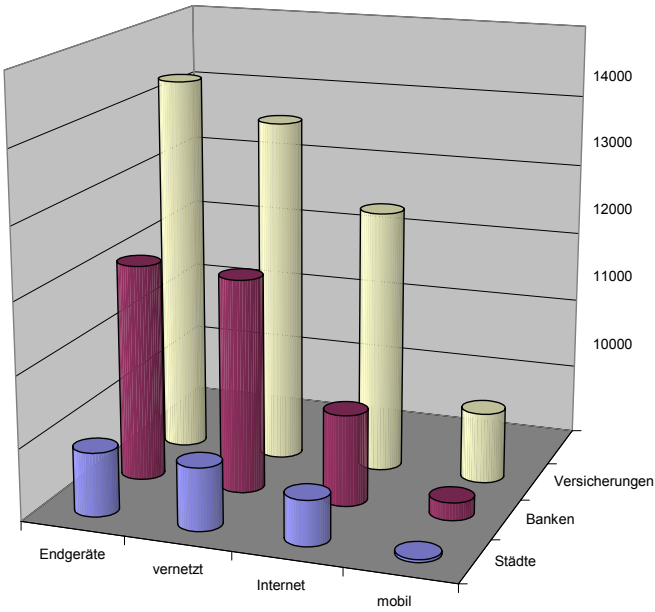

Diagramm 1: Gesamtzahl und Verwendung von Endgeräten

Die Zahl der gemeldeten Endgeräte betrug zwischen 300 und 13.500 Stück pro befragter Stelle. In allen drei Zielgruppen wurde ein hoher Anteil an vernetzten Geräten gemeldet. Er lag zwischen 90% und 100%. Ähnlich hoch war der Prozentsatz der Geräte mit Zugang zum Internet. Mobile Geräte waren bei den Städten mit 4,5%, bei den Banken mit 15% und bei den Versicherungen mit 21% vertreten.

Für alle Gerätegruppen wurden in den einzelnen Fragebereichen die organisatorischen Richtlinien und Regeln in hohem Maße als erfüllt gemeldet (Städte 70%, Banken 86%, Versicherungen 86%). Die konkrete Umsetzung der Regeln lag dagegen niedriger. Sie betrug beispielsweise für Wartung, Reparatur, Aussonderung oder Löschung von Magnetplatten zwischen 50% und 70%. Die Maßnahmentiefe war bei

den verschiedenen Gerätearten, wie mobilen Arbeitsplätzen oder PCs unterschiedlich umgesetzt.

	Städte		Banken		Versicherungen	
	orga.	technisch	orga.	technisch	orga.	technisch
Allgemeine Dienstanweisungen	70	-	87	-	87	-
Konkrete Umsetzung von Regeln	58	50	95	66	86	71
Betriebssicherheit	48	66	61	73	64	75
Absicherung Schnittstellen	45	57	48	73	88	83
Vorgaben für dienstliche/private Nutzung	77	30	80	40	97	27
Festlegung über die Zugriffsbefugnis	60	60	95	100	100	90
Vorgaben für Passworte	47	50	90	97	100	100
Regelung für Internetnutzung	66	78	74	88	80	96
Besondere Maßnahmen für mobile Geräte	30	40	73	53	73	63

Tabelle 1: Prozentuale Erfüllung der technischen und organisatorischen Sicherheitsmaßnahmen

Die höchste Vernetzung und der häufigste Internetzugang fanden sich bei den Versicherungen. Bei ihnen waren auch die zu treffenden Maßnahmen am weitesten erfüllt. Auffällig war, dass bei den Kommunen insgesamt der niedrigste Erfüllungsgrad an Sicherheitsmaßnahmen erreicht wurde. Privatunternehmen hatten insbesondere Defizite bei zu treffenden organisatorischen Maßnahmen. Sie stuften diese häufig als "nicht vorgesehen" ein.

➧ Die Ergebnisse der Umfrage belegen, dass die Umsetzung von organisatorischen und technischen Sicherheitsmaßnahmen noch verbesserungsbedürftig ist.

2.4 Dokumenten-Management-Systeme

Seit geraumer Zeit halten Dokumenten-Management-Systeme (DMS) Einzug in Verwaltungen. Diese Systeme bieten die Möglichkeit, Papierdokumente und elektronische Dokumente zu verwalten. Bei der Umstellung der Aktenführung von der Papierform auf die elektronische Akte gilt es, eine Reihe von Regelungen zu beachten, um auch den datenschutzrechtlichen Anforderungen bei der Nutzung der neuen technischen Möglichkeiten gerecht zu werden.

Ziel des Einsatzes eines DMS ist die "elektronische Akte", in der alle Informationen zu einem Sachverhalt in einheitlicher elektronischer Form zur Verfügung stehen und ohne Medienbrüche weiterverarbeitet werden können.

Die Datenschutzfragen beginnen, wie so oft, gleich am Anfang und haben nicht mit der Technik an sich, sondern mit der Organisation zu tun. Ein kontrollierbarer Einsatz eines DMS kann nur dann erfolgen, wenn die zugrunde liegenden Verwaltungsprozesse beschrieben sind. Heutige DMS sind im Auffinden von Daten – auch aus unstrukturierten Beständen – so leistungsfähig, dass der Einsatz einer Datenbank mit strukturierten Daten, die sichere Transaktionen und den Schutz der personenbezogenen Daten erheblich vereinfachen, als nicht notwendig erscheint. Der Einsatz eines DMS ohne konzeptionelle Einbindung in die zu unterstützenden Prozesse birgt aber die Gefahr, dass Daten unstrukturiert, also nicht transparent und nachvollziehbar abgelegt und damit geeignete Zugriffsrechte nicht vergeben werden können. Weiter ist festzulegen, wie analoge (gedruckte) Schriftstücke in die digitale Ablage eines DMS gelangen. Werden sie lediglich gescannt und ähnlich einem digitalen Foto als Bitmap gespeichert oder werden die Textzeichen über so genannte OCR-Software interpretiert und dann digital gespeichert? Welche Version der originalen Schriftstücke ist aufzubewahren, um Nachvollziehbarkeit und Transparenz zu gewährleisten? Wer ist berechtigt, welche Dokumente einzuscannen und aufgrund welcher Rechtsgrundlage dürfen sie gespeichert werden?

Einen wesentlichen Einfluss auf die Datensicherheit in einem DMS hat auch die Architektur der Datenhaltung. Bei einer dezentralen Datenhaltung werden alle Dokumente bei der Stelle gespeichert, die sie erhoben hat. Das DMS einer solchen Stelle ist geschlossen und

autark. Ein Austausch über diese regionale Grenze hinweg erfordert eine dezidierte Kommunikationsverbindung zwischen zwei DMS. In diesem Fall ist die Komplexität eines Berechtigungs- und Sicherheitskonzepts aufgrund klarer Zuständigkeiten und physikalischer Grenzen relativ gering. Bei zentraler Datenhaltung werden die Datenbestände mehrerer Stellen in einer Speicherkomponente zusammengefasst. Um nun ausschließlich berechtigte Zugriffe auf die Daten zu gewährleisten, muss ein komplexes Zugriffskonzept auf Dokumentenebene realisiert werden.

Im Gegensatz zu strukturierten Daten kann Dokumenten der Schutzbedarf nicht a priori zugewiesen werden. Weil personenbezogene Daten an jeder Stelle eines Dokumentes vorkommen können, ist ihr Schutzbedarf vom Kontext abhängig. An dieser Stelle sei darauf hingewiesen, dass neben der Vertraulichkeit die Verfügbarkeit, die Integrität und die Zurechenbarkeit weitere Schutzziele sind.

Um das Schutzziel der Zurechenbarkeit zu gewährleisten, müssen Bearbeitungsschritte des vorgangsbezogenen Handelns revisionsfähig gespeichert werden. DMS stellen zu diesem Zweck Protokoll- und/oder Verfahrensdaten automatisiert zur Verfügung, wobei Protokolldaten zur Dokumentation der auf der Maschine abgelaufenen Prozesse gespeichert werden und Verfahrensdaten zur Steuerung und Durchführung des jeweiligen Arbeitsablaufs notwendig sind. An dieser Stelle kann ein Konflikt mit dem schutzwürdigen Interesse derjenigen entstehen, die diese Bearbeitungsschritte vornehmen. Wird der komplette Vorgangslauf mit geeigneten Kontrolldaten dokumentiert, so können mit diesen Daten leicht Leistungs- und Verhaltenskontrollen durchgeführt werden. Dies kann vermieden werden, indem nur die zwingend zur Herstellung der Revisionsfähigkeit notwendigen Daten gespeichert werden.

Heutige Datenformate können eventuell von Rechnern künftiger Generationen nicht mehr gelesen werden, wobei die Lebensspanne technischer Systeme durch die rasanten Entwicklungszyklen immer kürzer wird. Es gibt zwar Bemühungen, die so genannte Abwärtskompatibilität zu gewährleisten, doch gelegentliche Quantensprünge führen auch zu kompletten Neuentwicklungen. Selbst das in der ISO 19005-1 festgelegte Archivierungsformat für elektronische Dokumente wird bereits überarbeitet. Aber auch die Speichermedien selbst haben eine physikalische Altersgrenze. Neben der schlichten Verfügbarkeit von Daten

ist deren Integrität sicherzustellen. Durch Signaturverfahren ist zu gewährleisten, dass einmal archivierte Daten in quasi eingefrorenem Zustand manipulationssicher aufbewahrt werden. Sind diese Signaturen aus irgendeinem Grunde nicht mehr gültig, so müssen teilweise riesige Datenmengen mit einer neuen Signatur versehen werden. Gerade dieser Tatsache ist speziell bei öffentlichen Verwaltungen, die lange Aufbewahrungsfristen zu beachten haben, über ein durchdachtes Signatur- und Archivierungskonzept Rechnung zu tragen.

- Der Datenschutz muss bei DMS bereits in die konzeptionelle Planung einbezogen werden. Eine strukturierte Ablage und auch eine nachvollziehbare Dokumentation des Verwaltungshandelns setzen ein systematisches Vorgehen voraus. Zu beachten sind hierbei auch die erheblich erweiterten Auskunftspflichten öffentlicher Stellen nach dem Informationsfreiheitsgesetz.

2.5 Kommunikation über Clearingstellen

Elektronische Kommunikation nimmt bei eGovernment-Anwendungen eine Schlüsselstellung ein. Um einen sicheren Datenaustausch zwischen öffentlichen Stellen zu gewährleisten, hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 15. Dezember 2005 dafür ausgesprochen, den Kommunikationsstandard OSCI (Online Services Computer Interface), der eine sichere, verschlüsselte Kommunikation vom Versand bis zum Empfang (Ende-zu-Ende) enthält, zu nutzen.

Der Standard soll durchgehend, also von der Quelle bis zur Senke, eingesetzt werden. Beispiele sind das automatisierte Rückmeldeverfahren im Meldewesen, der Datenaustausch zwischen Kommunen und dem Bundesamt für Finanzen (ETIN) oder das Einladungsverfahren beim Mammografie-Screening. Wird der Standard eingesetzt, ist eine Einsichtnahme in die Inhaltsdaten beispielsweise durch Clearing- oder Vermittlungsstellen nicht notwendig.

In Nordrhein-Westfalen haben sich die kommunalen Spitzenverbände und die Landesverwaltung dafür ausgesprochen, eine Clearingstelle aufzubauen, die obige Voraussetzungen erfüllt. Um das Angebot für

die einzelnen Kommunen wirtschaftlich attraktiv zu gestalten, soll eine Reihe von Diensten auf der gleichen technischen Basis angeboten werden. Es gibt allerdings auch Bestrebungen, preiswertere Lösungen auf anderer technischer Basis zu realisieren. Diese erfordern dann allerdings aktive Vermittlungsdienste, die eine Entschlüsselung der Daten notwendig machen und somit eine Einsicht in die zu übermittelnden Daten ermöglichen. Aus der Sicht des Datenschutzes sind solche Lösungen nicht zu befürworten.

- OSCI-Produkte, die Verschlüsselung und Signatur als wesentliche Elemente des technischen Datenschutzes nutzen, sollten soweit als möglich eingesetzt werden, auch weil sie einen faktischen Standard bilden.

2.6 Online-Banking

Oftmals fehlt es Kundinnen und Kunden bei der Nutzung des browserbasierten Internet-Banking (Online-Banking) an technischem Wissen und damit an der Grundvoraussetzung für das Erkennen von Sicherheitsrisiken. Kreditinstitute, die Online-Banking anbieten, können nicht erwarten, dass Kundinnen und Kunden für die Sicherung ihrer Systeme alleine sorgen, zumal die Kundenseite im Visier von potentiellen Angreifern liegt und in Schadensfällen die Beweislast mittlerweile von einigen Banken umgekehrt wird.

Streitpunkt war der von einer Online-Bank vertretene Standpunkt, die Verantwortung für die Abmeldung und Schließung aller geöffneten Browserfenster bei der Nutzung des Online-Portals allein ihren Kundinnen und Kunden zu überlassen. Ein unauffälliger Hinweis am unteren Ende der Login-Seite, dass alle geöffneten Browserfenster einzeln zu schließen sind, ist im Hinblick auf die Verantwortung der Online-Bank gegenüber ihren Kundinnen und Kunden aus Datensicherheitsgründen nicht ausreichend. Durch entsprechende Änderungen der Online-Banking-Software könnte die Anzahl der zu öffnenden Browserfenster limitiert oder das Schließen der Fenster beim Wechsel erzwungen werden. Ebenso sollte die Aufklärung über die Risiken und über einzuhaltende Datensicherheitsmaßnahmen bei der Nutzung des Online-Banking stärker forciert werden.

- Online-Banking-Software sollte so aufgebaut sein, dass Risiken, die durch die kundenseitigen Systeme entstehen können, weitestgehend ausgeschlossen werden.

2.7 Phishing – Trickbetrug im Internet

Phishing (Kunstwort aus "Password" und "fishing") bedeutet das betrügerische Erschleichen von Passwörtern. Der geradezu dramatische Anstieg von Phishing-Attacken im Berichtszeitraum führte gleichzeitig auch zu einem sprunghaften Anstieg von Anfragen besorgter Bürgerinnen und Bürger, die Opfer dieser Phishing-Attacken wurden.

Beim "klassischen" Phishing sollen die als Kundeninformation getarnten Phishing-Mails die arglose Online-Kundschaft auf Websites locken, die den echten Web-Auftritten von Kreditinstituten täuschend ähnlich nachempfunden sind, und dort zur Eingabe von Zugangsdaten verleiten. Qualität und Variabilität dieser Online-Angriffe wurden mittlerweile erheblich gesteigert. In letzter Zeit weiten Phisher ihre Täuschungsangriffe wegen der geringen Kosten der Internet-Telefonie (VoIP) zunehmend auch auf das Telefon als Medium aus (sogenanntes Vishing).

Aufgrund der rechtlichen Aufgabenstellung und auch der zur Verfügung stehenden Mittel kann die LDI nur allgemeine Warnhinweise geben. Eine Verfolgung der Absendenden von Phishing-Mails ist nicht möglich. Dies ist Aufgabe der Strafverfolgungs- und Ermittlungsbehörden. Die Verfolgung dieser Delikte ist allerdings sehr schwierig, da sich die gefälschten Webseiten in der Regel außerhalb der Europäischen Union befinden. Laut einem im Juni 2006 veröffentlichen Report der Anti-Phishing Working Group (APWG), stammen die ersten drei Ursprungsorte der Phishing-Websites aus den USA (35,6%), China (15%) und Südkorea (10,2%). Platz vier belegte laut dieser Studie Frankreich mit 5,7%, gefolgt von Deutschland mit 3,2%.

Eine resignative Haltung gegenüber Phishing-Attacken darf nicht die Antwort sein. Neben der Einhaltung der von den Hausbanken und Sicherheitsinstitutionen bekannt gegebenen Schutzmaßnahmen sollten die Phishing- oder Vishing-Angriffe bei Organisationen gemeldet werden, die Phishing-Betrug bekämpfen, beispielsweise bei der Arbeitsgruppe Identitätsschutz im Internet unter https://www.a-i3.org/. Hier

werden auch aktuelle Informationen über Phishing-Mails und Empfehlungen über zu treffende Sicherheitsmaßnahmen bekannt gegeben. Es sollte eine Anzeige bei der Polizei erstattet werden, wenn der Verdacht besteht, dass sensible Daten ausgelesen, irrtümlicherweise weitergegeben wurden oder wenn bereits ein Vermögensschaden durch den Phishing-Betrug entstanden ist.

- Bei Online-Geschäften ist hohe Aufmerksamkeit und Sorgfalt geboten. Persönliche Informationen werden von Banken und anderen Firmen nie per offener E-Mail erfragt.

2.8 Versand sensibler Daten per E-Mail

Bei der Versendung von personenbezogenen Daten per E-Mail ohne besondere Schutzmaßnahmen sind weder die Vertraulichkeit noch die Integrität noch die Authentizität gewährleistet. Es ist hinreichend bekannt, dass E-Mails auf ihrem Weg durch das Internet viele Stationen passieren, an denen sie abgefangen, mitgelesen oder auch verändert werden können.

Bei einigen Online-Anbietern hat sich allerdings folgende sicherheitsgefährdende Praxis im Umgang mit Login-Passwörtern etabliert: Ist ein Login-Passwort für das persönliche Onlinekonto vergessen, so wird ein neues, gültiges im Klartext per E-Mail an die Kundinnen und Kunden gesandt. Das Gleiche geschieht auch bei der Neueinrichtung eines Kontos, bei der nach der erstmaligen Registrierung das Login-Passwort unverschlüsselt an die angegebene E-Mail-Adresse übersandt wird.

Genau so datenschutzunfreundlich waren die Praktiken eines Telefon-Providers und einer Online-Bank: Bei der Beantwortung von Kundenanfragen per E–Mail sowie bei automatisiert erstellten Änderungsbestätigungen waren die gespeicherten Kundendaten im Klartext in den Antworten enthalten. Soweit diese Rückübermittlung nicht erforderlich ist, sollte besser darauf verzichtet werden, andernfalls sollte ein Verfahren gewählt werden, dass die Vertraulichkeit der Kommunikation sicherstellt.

Um den Anforderungen an die Datensicherheit bei der E-Mail-Kommunikation gerecht zu werden, müssen E-Mails mit sensiblen Inhalten vor ihrer Übermittlung durch besondere Maßnahmen wie Verschlüsselung

geschützt werden (siehe hierzu auch den Leitfaden "E-Mails … aber sicher!", abrufbar unter www.ldi.nrw.de).

➡ Aufgrund der bekannten Risiken und Gefahren bei der Internet-Nutzung ist die Versendung von Passwörtern oder anderen vertraulichen Angaben im Klartext per E-Mail unverantwortlich. Ebenso sollte bei der Kommunikation im Internet auf die Übermittlung nicht erforderlicher personenbezogener Daten verzichtet werden.

2.9 Vertraulichkeit von E-Mail-Adressverteilern

Wie würden Sie reagieren, wenn Sie Mahnungen oder Kreditmitteilungen per E-Mail erhalten und feststellen, dass die Nachricht an sämtliche Personen des offen angezeigten E-Mail-Verteiler versendet wurde? Jeder Empfänger und jede Empfängerin wissen nun, wer die E-Mail erhalten hat.

Durch die offene Angabe weiterer Adressen in einer E-Mail können nicht nur Rückschlüsse auf die geschäftlichen oder privaten Beziehungen unbeteiligter Dritter gezogen werden, sondern es besteht darüber hinaus die Gefahr, dass die Adressen auf Spam-Verteiler-Listen gelangen. Die Übermittlung von E-Mail-Adressen ohne Einwilligung an Dritte verstößt gegen das schutzwürdige Interesse der Betroffenen und ist daher unzulässig.

Fast alle auf dem Markt erhältlichen E-Mail-Programme stellen ein spezielles Empfangsfeld (Bcc) zur Verfügung, in das zusätzliche E-Mail-Adressen eingetragen werden können, die gegenüber anderen Empfängerinnen und Empfängern dieser E-Mail geheim bleiben sollen. Bei einigen E-Mail-Programmen wird das Bcc-Feld standardmäßig nicht angezeigt und muss erst freigeschaltet werden. Nach Freischaltung stehen insgesamt drei Felder zur Verfügung, um Adressdaten einzutragen:

- "To" ("An") ist für die eigentliche Hauptadresse bestimmt.
- "Cc" (Carbon Copy, Durchschrift) ist für weitere Adressen bestimmt, die auch darüber in Kenntnis gesetzt werden sollen, wer diese Nachricht erhält (beispielsweise geschlossene Benutzergruppen).

- "Bcc" (Blind-Carbon-Copy, unsichtbare Durchschrift oder Blindkopie) ist dafür bestimmt, E-Mail-Adressverteiler gegenüber Dritten geheim zu halten. Die Funktion gewährleistet, dass die hier eingetragenen Empfangsadressen den anderen Empfängerinnen und Empfängern nicht angezeigt werden.

  ➧ Bei der Zusendung einer E-Mail an Dritte über einen Adressverteiler muss sicher gestellt sein, dass die Adressen nicht allen Empfängerinnen und Empfängern offen gelegt werden. Das Versenden einer E-Mail an Dritte sollte daher als Blindkopie (Bcc) erfolgen.

2.10 Aussonderung und Vernichtung von Unterlagen

Die unzureichende Entsorgung und Vernichtung von Unterlagen mit sensiblem personenbezogenen Inhalt ist in den Datenschutzberichten bereits viele Male thematisiert worden. Ein gravierender, auch von der Presse aufgegriffener Fall, war Auslöser für eine Stichprobenkontrolle bei öffentlichen Stellen.

Aktenfunde werden immer gern von den Medien aufgegriffen und sorgen regelmäßig für negative Schlagzeilen. Vor diesem Hintergrund sollte der Datensicherheitsaspekt bei der Unterlagenvernichtung nicht unterschätzt werden und den notwendigen Stellenwert bei der behördeninternen Sicherheitsbetrachtung erhalten.

Unter dem Gesichtspunkt der Entsorgung lassen sich personenbezogene Unterlagen in zwei Gruppen einteilen. Zum einen werden sie in Akten geführt. Daneben fallen beim täglichen Arbeitsablauf eine Reihe von Notizen, Entwürfen und Aufstellungen an, die nicht Aktenbestandteile werden.

Grundsätzlich gilt, dass in beiden Gruppen die gesetzlichen Bestimmungen des Datenschutzes eingehalten werden müssen. Während die Entsorgung und Archivauslagerung von Akten meist zufrieden stellend geregelt sind, ist die Entsorgung der personenbezogenen Unterlagen des täglichen Arbeitsablaufs meist lückenhaft oder gar nicht geregelt. Genau aber dieser ungeregelte Bereich der Unterlagenvernichtung war die Hauptursache in den meisten bekannt gewordenen Fällen für das Auffinden von personenbezogenen Unterlagen in der Öffentlichkeit.

Bei öffentlichen Stellen werden in den Büros meistens zwei Abfallbehälter für Papier- und Restmüll vorgehalten, die von Reinigungsfirmen entleert werden. Die Papierabfälle werden in Säcke gefüllt und hausintern zwischengelagert, bis sie von Firmen abgeholt und über Papierrecycling entsorgt werden. Die Zwischenlagerung erfolgt in vielen Fällen in durch Kettenschlösser nur schwach gesicherten Containern, die in relativ frei zugänglichen Innenhöfen oder Kellerräumen stehen und damit leicht zu Angriffspunkten werden können. Personenbezogene Unterlagen sollen gar nicht in den Papiermüll geworfen, sondern separat gesammelt, zwischengelagert und anschließend entsorgt werden. Es bestehen allerdings für die Beschäftigten häufig keine konkreten Anweisungen, wie einzelne personenbezogene Unterlagen ordnungsgemäß zu vernichten sind. Ebenso finden nur wenige Kontrollen statt, ob personenbezogene Unterlagen über Papierkörbe entsorgt wurden. Daneben sind meist nur wenige oder gar keine Aktenvernichter vorhanden.

Es bleibt festzustellen, dass personenbezogene Unterlagen – auch im zerrissenen Zustand – auf keinen Fall über eine Papierabfalltonne entsorgt werden dürfen. Wird die Unterlagenvernichtung durch eine Reinigungsfirma im Auftrag erledigt, ist eine entsprechende Vertragsgestaltung notwendig. Am effektivsten ist eine direkte Aktenvernichtung durch geeignete Schredder, die dezentral und zentral mit ausreichenden Kapazitäten aufgestellt werden, da so die Risiken beim Transport und bei der Zwischenlagerung vermieden werden.

Damit die datenschutzrechtlichen Regelungen bei der Vernichtung von personenbezogenen Unterlagen eingehalten werden können, sind folgende Sicherheitsmaßnahmen erforderlich:

- Verbindliche Anweisungen hinsichtlich des Umgangs (Sammlung, Aufbewahrung, Transport, Zwischenlagerung) und der Vernichtung von personenbezogenen Unterlagen

- Sensibilisierung aller Mitarbeiterinnen und Mitarbeiter für die Einhaltung dieser Anweisungen

- Verbindliche Vorgabe von (stichprobenartigen) Kontrollen zur Überprüfung der Einhaltung der Anweisungen

- Aufstellung geeigneter Schredder an für die Beschäftigten gut erreichbaren Standorten (beispielsweise in der Nähe von Kopierern)

- Sichere Aufstellung und Verschluss von Papiercontainern mit geeigneten Schlössern

- Auswahl eines geeigneten Entsorgungsunternehmens sowie Abschluss eines Vertrages mit Festlegung aller technischen und organisatorischen Maßnahmen von der Abholung bis zur Vernichtung, insbesondere auch des Verfahrens der Übernahme oder Übergabe der Altakten (beispielsweise Aufsicht, überwachende Begleitung)

Weitere Hinweise zur Durchführung einer ordnungsgemäßen Unterlagenvernichtung befinden sich in der Orientierungshilfe "Unterlagenvernichtung bei öffentlichen Stellen", abrufbar unter www.ldi.nrw.de.

➡ Die Vernichtung von Akten und Schriftstücken ist in einem ganzheitlichen Sicherheitskonzept zu dokumentieren. Bei der Ermittlung der technischen und organisatorischen Maßnahmen sind die Risiken des gesamten Entsorgungsprozesses, also von der Sammlung über die Zwischenlagerung und den Transport bis zur endgültigen Vernichtung in die Sicherheitsbetrachtung einzubeziehen.

3 Medien

3.1 Die Vorratsdatenspeicherung kam durch die Hintertür!

Das, was im letzten Bericht noch als Frage formuliert war, ist jetzt bittere Realität geworden: Die EU hat im kürzesten Gesetzgebungsverfahren ihrer Geschichte die Vorratsdatenspeicherung von Verkehrsdaten der elektronischen Kommunikation am 15. März 2006 beschlossen. Das bedeutet, dass künftig jedes Telefonat, jede E-Mail und jeder Aufenthalt im Internet gespeichert wird.

Zwischen der Vorstellung des Richtlinienentwurfs und dessen Verabschiedung lagen nur sechs Monate. Noch am 17. Februar 2005 hatte der 15. Bundestag ausdrücklich eine Vorratsdatenspeicherung von Verkehrsdaten abgelehnt. Genau ein Jahr später hat der 16. Bundestag am 16. Februar 2006 die Bundesregierung aufgefordert, der Richtlinie zur Vorratsdatenspeicherung im Rat der Europäischen Union zuzustimmen und sie "mit Augenmaß" umzusetzen. Die Richtlinie ist nun in nationales Recht umzusetzen, sofern nicht der Europäische Gerichtshof sie für rechtswidrig erklärt. Dort ist ein Verfahren anhängig, in dem unter anderem darüber zu entscheiden ist, ob aufgrund des den Binnenmarkt regelnden EU-Vertrages überhaupt Bestimmungen über den Kampf gegen den Terrorismus getroffen werden können.

Die Richtlinie sieht vor, dass alle Verkehrsdaten der elektronischen Kommunikation, also die Daten von Festnetz und Mobilfunk, von SMS, E-Mail–Dienst, Internetzugang und Internet-Telefonie 6 bis 24 Monate gespeichert werden und mit besonderer Begründung auch länger. Die Inhalte der jeweiligen Kommunikation dürfen nicht gespeichert werden. Die Kosten für die Speicherung müssen nicht von den Mitgliedstaaten getragen werden, so dass die Unternehmen selbst die Kosten zu tragen haben und somit letztendlich die Verbraucherinnen und Verbraucher. Der Speicherungszweck ist nicht mehr wie ursprünglich geplant auf Terrorabwehr oder organisierte Kriminalität beschränkt, sondern der Zweck ist die Verfolgung grundsätzlich schwerer Straftaten. Der Bundestag will sogar noch weiter gehen und die Nutzung

von Verkehrsdaten für alle Straftaten zulassen, die mittels Telekommunikation begangen werden.

Der Inhalt der Richtlinie begegnet erheblichen verfassungsrechtlichen Bedenken. Grundsätzlich dürfen personenbezogene Daten nur dann gespeichert werden, wenn dies zu einem gesetzlich bestimmten und zugelassenen Zweck erforderlich ist. Eine solche Speicherung von Daten auf Vorrat widerspricht dem Grundsatz der Erforderlichkeit. Eine verdachtsunabhängige pauschale Speicherung von umfangreichen Datenmengen verletzt in gravierender Weise das Fernmeldegeheimnis, da das Kommunikationsverhalten von unverdächtigen Personen erfasst wird. Durch die Speicherung der Verkehrsdaten ist es möglich, über einen längeren Zeitraum festzustellen, wer wann mit wem wie lange telefoniert oder per E-Mail korrespondiert hat. Bei der Benutzung von Mobilfunktelefonen werden Standortdaten als Verbindungsdaten ebenfalls gespeichert, so dass zusätzlich ein europaweites Bewegungsprofil für einen Großteil der Bevölkerung erstellt werden kann. Auch wenn die Inhalte der Kommunikation nicht gespeichert werden, so kann doch von den im Internet aufgerufenen Seiten über deren Adresse (URL) auf den Inhalt geschlossen werden.

Ob die Vorratsdatenspeicherung überhaupt geeignet ist, die Kriminalität wie gewünscht zu bekämpfen, ist zweifelhaft. Maßnahmen der Strafverfolgung können wirksam und zielgerichtet mit geringerer Eingriffsintensität für die Bürgerinnen und Bürger genutzt werden. So hat sich beispielsweise in den USA das "quick freeze" Verfahren bewährt, in dem Verbindungsdaten bestimmter Personen nur im Bedarfsfall für einen gewissen Zeitraum zu Strafverfolgungszwecken gespeichert werden (siehe auch Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005, abgedruckt im Anhang). Auch der wissenschaftliche Dienst des Deutschen Bundestages hat in seiner Ausarbeitung zur Zulässigkeit der anlasslosen und verdachtslosen Vorratsdatenspeicherung nach europäischem und deutschem Recht Zweifel an der Verfassungsmäßigkeit der Richtlinie und ihrer möglichen Umsetzung in innerdeutsches Recht geäußert.

- Die freie und unbeobachtete Kommunikation ist ein elementarer Bestandteil der freiheitlichen Demokratie. Die mit der Vorratsdatenspeicherung verbundene Überwachbarkeit der Kommunikation darf nicht Wirklichkeit werden.

3.2 Das neue Telemediengesetz

Die bisher getrennten gesetzlichen Regelungen für Mediendienste und Teledienste, die in der Vergangenheit zu einigen Abgrenzungsproblemen führten, sollen im Frühjahr 2007 im neuen Telemediengesetz vereinheitlicht werden.

Die unterschiedliche Regelung von Telediensten und Mediendiensten geht auf die divergierende Gesetzgebungskompetenz von Bund und Ländern zurück. So erfreulich die Zusammenführung von Bundesrecht und Landesrecht für Anbietende, Nutzende und Aufsichtsbehörden im neuen Telemediengesetz (TMG) ist, so ist doch der "große Wurf" ausgeblieben. Auch nach dem neuen Gesetz wird es weiterhin Abgrenzungsprobleme zwischen den verschiedenen elektronischen Medien geben, da Telekommunikationsdienste und Rundfunk nicht unter dieses Gesetz fallen. Bereits heute kann beispielsweise über einen PC nicht nur gesurft, sondern auch telefoniert, Fernsehen empfangen oder Radio gehört werden. Es treffen also in einem Gerät Telekommunikation, Telemedien und Rundfunk aufeinander und werden von einem einzigen Dienstleistungsunternehmen ermöglicht. Das neue TMG bringt keine abschließende Klarheit in die verschiedenen von den Dienstleistungsunternehmen zu beachtenden datenschutzrechtlichen Regelungen und für die Frage, welche Aufsichtsbehörde jeweils zuständig ist. Mit der Neufassung des TMG wurde es leider versäumt, den Schutz der Privatsphäre der Internetnutzerinnen und -nutzer zu stärken und das Telemediengeheimnis einzuführen. Ein Einkaufsbummel im Internet sollte genauso anonym möglich sein wie in der Fußgängerzone.

Eine eklatante Verschlechterung des Datenschutzniveaus wurde gerade noch rechtzeitig abgewendet. Einer der Vorentwürfe zum TMG sah einen so genannten "ebay-Paragraphen" vor. Die Teledienste, wie zum Beispiel Internetauktionshäuser, sollten das Recht erhalten, Nutzungsdaten über das Ende des Nutzungsvorganges hinaus für Zwecke der eigenen Rechtsverfolgung zu speichern. Diese Regelung hätte zu einer verfassungsrechtlich bedenklichen Vorratsdatenspeicherung geführt. Zwar wird diese Bestimmung jetzt nicht Realität, doch wird es voraussichtlich einen Auskunftsanspruch über Bestandsdaten zur Durchsetzung der Rechte am geistigen Eigentum geben. Diese Regelung korrespondiert mit den Bestrebungen zur Änderung des Urheber-

rechtes (siehe hierzu unter 3.3). Somit hätten neben berechtigten öffentlichen Stellen auch Private einen Auskunftsanspruch.

Hervorzuheben sind die neuen Anti-Spam Regelungen. Dadurch wird es nun möglich, Anbietende zur Rechenschaft zu ziehen, die durch Verschleierung des kommerziellen Charakters einer E-Mail gezielte Täuschungshandlungen begehen. Hierfür wurde auch ein Bußgeldtatbestand aufgenommen, der die bisher bestehende Regelungslücke schließen soll.

➡ Es ist bedauerlich, dass die Chance verpasst wurde, das Datenschutzniveau im Bereich der Telemedien zu erhöhen.

3.3 Der Griff nach dem Fernmeldegeheimnis

Erstmals sieht ein Gesetzentwurf vor, dass unbeteiligte Dritte, nämlich Telekommunikationsunternehmen oder Teledienstean-bieter, die dem Fernmeldegeheimnis verpflichtet sind, in einem zivilrechtlichen Streitverfahren Auskunft über Verkehrsdaten erteilen müssen.

Die IPR-Enforcement-Richtlinie der EG (2004/48/EG) soll durch das "Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums" umgesetzt werden. Ziel des Gesetzentwurfs ist die bessere Verfolgung von Urheberrechtsverletzungen durch Nutzende des Internet. Künftig sollen in ihren Urheberrechten Verletzte bei Gericht beantragen können, von Internetprovidern Auskunft über Verkehrsdaten zu erhalten. Diese Daten sind jedoch durch das Fernmeldegeheimnis geschützt und durften bisher nur in Ausnahmefällen zum Zwecke der Strafverfolgung den Sicherheitsbehörden aufgrund richterlicher Anordnungen herausgegeben werden.

Das grundgesetzlich geschützte Fernmeldegeheimnis wird in immer kürzeren Abständen und nun auch für privatwirtschaftliche Interessen eingeschränkt. Mit diesem Gesetzentwurf wird die Hemmschwelle für die Nutzung und Auswertung der durch das Fernmeldegeheimnis geschützten Daten weiter herabgesetzt. Offen bleibt auch, welche Verkehrsdaten zur Auskunftserteilung verwendet werden dürfen. Grundsätzlich stehen derzeit nur die Daten zur Verfügung, die zu Abrechnungszwecken benötigt werden. Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfol-

gung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird (siehe dazu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006, abgedruckt im Anhang).

- Es kann nicht akzeptiert werden, dass das Fernmeldegeheimnis zur Durchsetzung wirtschaftlicher Interessen eingeschränkt wird. Die Musik- und Filmindustrie hat dafür Sorge zu tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle illegale Nutzungen erst gar nicht möglich werden.

3.4 Auskunft über unvollständige Rufnummer

Elektronische Telefonverzeichnisse mit der Möglichkeit der Inverssuche erlauben es nicht nur, die Adressen zu einzelnen Rufnummern zu finden, sondern mit Teilen der Rufnummer unter Eingabe von Sternchen als Platzhalter ganze Rufnummernkreise mit den dazugehörigen Adressangaben zu erhalten.

Seit der letzten Änderung des Telekommunikationsgesetzes ist es erlaubt, bei der Telefonauskunft den Namen und die Adresse der jeweiligen Teilnehmenden zu erfragen, auch wenn nur die Rufnummer bekannt ist (Inverssuche). Diese Funktion ist selbstverständlich auch mit Hilfe der elektronischen Telefonverzeichnisse möglich. Gesetzlich geregelt ist, dass die Inverssuche ausschließlich für bekannte Rufnummern zugelassen ist. Einige der elektronischen Telefonverzeichnisse gehen jedoch so weit, dass sie auch Ergebnisse anzeigen, wenn die Rufnummer nur unvollständig eingegeben wird. Hat sich beispielsweise eine Teilnehmerin oder ein Teilnehmer dazu entschlossen, der Inverssuche nicht zu widersprechen, weil die Adresse nicht ins Teilnehmerverzeichnis aufgenommen wurde, kann jedoch mit der Jokerabfrage möglicherweise zumindest das Stadtviertel, vielleicht sogar die Straße bestimmt werden. Dies kann sich jedenfalls aus dem Vergleich der Rufnummer der betroffenen Person mit den bei der "Jokerabfrage" angezeigten Rufnummern ergeben, zu denen auch Adressen angezeigt werden. Diese Möglichkeit der Recherche mit Platzhaltern ist den Teilnehmerinnen und Teilnehmern nicht unbedingt bekannt, wenn sie sich nicht zu einem Widerspruch der Inverssuche entscheiden.

➡ Die Daten des Teilnehmerverzeichnisses dürfen nur zur Direkt- oder Inversauskunft im Sinne des Telekommunikationsgesetzes genutzt werden, nicht jedoch für die Inverssuche mit Platzhaltern. Die Inverssuche ist auf den gesetzlich vorgegebenen Rahmen zu beschränken.

3.5 Rufnummernunterdrückung

Es wundert schon ein wenig. Sie wählen die Rufnummer Ihres Versandhauses und werden nett und freundlich begrüßt: "Einen wunderschönen guten Tag, Herr Beispiel. Was kann ich für Sie tun?" Wie geht das, werden Sie sich fragen, wenn Sie ausdrücklich von Ihrem Recht auf Unterdrückung der Rufnummer Gebrauch gemacht haben.

TK-Unternehmen bieten Firmen eine Dienstleistung an, bei der sie Zuordnungen von Kundinnen und Kunden zu Rufnummern vornehmen, wenn ihnen zuvor geeignete Zuordnungslisten beispielsweise von Kundennummern oder Namen zu den jeweiligen Rufnummern übermittelt wurden. Die Anrufenden können nun seitens der TK-Unternehmen den übermittelten Merkmalen zugeordnet werden. Die von den jeweiligen Firmen, beispielsweise Versandhäusern oder Call-Centern, angeforderten Kundenmerkmale werden ohne Rücksicht auf eine eingeschaltete Rufnummernunterdrückung weitergeleitet. Die Firmen können jetzt die von ihnen gewünschte Steuerung wie beispielsweise eine direkte Ansprache oder eine bevorzugte Behandlung vornehmen.

Der Dienst ist aus der Sicht des Datenschutzes nicht ganz unbedenklich, da nach dem Telekommunikationsgesetz TK-Unternehmen auf Antrag der Kundinnen und Kunden die Anzeige der eigenen Rufnummer auf dem Display der Angerufenen dauerhaft oder temporär unterdrücken müssen. Für die genannten Dienstleistungen wird aber gerade die Rufnummer als Steuerungselement genutzt und damit eine eventuell vorgegebene Sperrung für diesen Zweck aufgehoben. Notwendige Voraussetzung für einen gesetzeskonformen Betrieb ist deshalb, dass geeignete, nachvollziehbare Einwilligungen der Kundinnen und Kunden vorliegen.

➡ Wollen Firmen den Dienst der automatisierten Kontaktsteuerung einrichten, haben sie sicher zu stellen, dass die erforderlichen Einwilligungen der Kundinnen

und Kunden vor der Übermittlung der Kontaktdaten an die TK-Unternehmen vorliegen. Bei den Firmen als verantwortliche Stellen liegt es deshalb auch, die notwendigen Vorabinformationen zu liefern.

3.6 Sicherung von Webzugriffen (Internetseiten)

Private Unternehmen bieten immer mehr Dienstleistungen über das Internet an. Viele dieser Dienstleistungen sind durch genaue Adressangaben (URL) in der Adresszeile des Browsers direkt einsehbar. Besondere Schutzmaßnahmen, die den Zugriff auf Daten unbeteiligter Dritter verhindern, bleiben dabei oft unberücksichtigt.

Websites werden im Allgemeinen so gestaltet, dass sie einfach und vielfältig nutzbar sind. Bereits vorliegende Daten sollen möglichst für weitere Anwendungen nicht wiederholt eingegeben werden müssen. Auch wenn diese Angebote erst nach Angabe einer Nutzungskennung und eines Passwortes erreichbar sind, lässt sich in der Folge der Zugriff auf die Seiten und somit auf die Daten anderer Kundinnen und Kunden oft über eine kleine Veränderung in der Adresszeile des Browsers herstellen. Wird in der Adresszeile dem jeweiligen Kundenangebot eine feste Zahlenkombination (http://www.beispiel.de/Kunde-24687.htm) zugeordnet, kann durch Veränderung dieser Zahl der Zugriff auf die Seiten anderer Personen hergestellt werden (http://www.beispiel.de/kunde24688.htm). Es kann jetzt beispielsweise leicht herausgefunden werden, ob und in welcher Höhe Kredite beantragt wurden, welche Versicherungen abgeschlossen wurden oder welche Bestellungen vorliegen. Dieser unbefugte Zugriff auf Daten Anderer ist unzulässig, da rechtlich eine Datenübermittlung an Dritte ohne deren Einwilligung erfolgt.

- Nutzungskennung und Passworte alleine reichen nicht aus, um den Schutz personenbezogener Daten im Internet zu gewährleisten. Anbieterinnen und Anbieter von Dienstleistungen im Internet haben geeignete technische und organisatorische Maßnahmen, beispielsweise durch Verschlüsselung, zu treffen, um persönliche Angebote vor Ausspähung durch Dritte zu schützen.

3.7 Veröffentlichung personenbezogener Daten in Weblogs, Chats und Foren

Weblogs, Chats und Foren werden genutzt, um mal eben öffentliche Diskussionen anzustoßen oder Kommentare im Internet zu veröffentlichen. Häufig werden dabei auch personenbezogene Daten Dritter genannt oder Pseudonyme aufgedeckt.

Worauf bei Chats und Foren zu achten ist, wurde bereits im Bericht 2003 unter 3.4 dargestellt. Relativ neu dagegen ist der Begriff "Weblog". Er setzt sich zusammen aus "Web" und "Log". Log kommt von Logbuch und meint eine journalartig geführte Aufzeichnung von Ereignissen. Der wesentliche Unterschied zu Foren liegt in der Handhabung der Software und ist aus Sicht des Datenschutzes nicht relevant. Was jedoch alle diese Kontakt- und Informationsplattformen gemeinsam haben, ist die Tatsache, dass schnell etwas weltweit veröffentlicht werden kann. Leider gehören hierzu auch immer wieder personenbezogene oder personenbeziehbare Daten von Betroffenen, die mit dieser Art der Veröffentlichung nicht einverstanden sind oder gar nichts von dieser Veröffentlichung wissen.

Bei einer Veröffentlichung solcher Daten im Internet handelt es sich um eine Verarbeitung personenbezogener Daten. Der Verarbeitung liegt in diesen Fällen eine Übermittlung an Dritte zu Grunde. Gestattet ist diese Übermittlung nur, wenn das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder die Betroffenen eingewilligt haben. Eine Einwilligung der Betroffenen liegt in der Regel nicht vor, so dass bei der Veröffentlichung der Daten im Internet zwischen der Meinungsfreiheit der Autorinnen und Autoren und dem allgemeinen Persönlichkeitsrecht der Betroffenen abzuwägen ist. Die Abwägung führt dabei in nahezu allen Fällen dazu, dass die Veröffentlichung personenbezogener Daten Dritter im Internet unzulässig ist, weil das Persönlichkeitsrecht der Betroffenen erheblich beeinträchtigt ist. Da die Daten im Internet weltweit abrufbar und recherchierbar sind, verlieren die Betroffenen regelmäßig die Kontrolle über ihre eigenen Daten.

- Die Veröffentlichung personenbezogener Daten im Internet, insbesondere in Weblogs, Chats und Foren hat ohne Einwilligung der Betroffenen zu unterbleiben.

Von einer solchen Veröffentlichung Betroffene haben selbstverständlich einen Löschungsanspruch.

3.8 Nicht jede Werbemail ist Spam

Wer kennt das Problem nicht? Beim Öffnen des E-Mail-Kontos befinden sich zahllose neue Mails im Posteingang. So richtig erwünscht und erwartet sind hierbei die wenigsten. Neben den wenigen neuen Mails von Bekannten erscheinen noch diverse Newsletter, Werbemails und andere Spam-Mails.

Fast täglich erreichen die LDI NRW Beschwerden über unverlangt zugesandte E-Mails. Sie kann in diesen Fällen die absendenden Firmen oder Personen auffordern, Auskunft über die Herkunft der Daten zu geben, Einwilligungen der Empfängerinnen und Empfänger nachzuweisen und Adressen Betroffener zu sperren oder zu löschen.

Die klassische Spam-Mail lässt sich meistens nicht sofort erkennen. Sie enthält in der Betreffzeile in den wenigsten Fällen Hinweise auf zu bewerbende Produkte. Sie kann jedoch häufig daran erkannt werden, dass sie an große, unbestimmte Verteiler geschickt wurde, die Empfangsdresse nicht im Kopf der Mail zu lesen ist und die Absenderangaben auf eine ausländische Domain verweisen. Solche Mails sollten in jedem Fall ungeöffnet gelöscht werden. Bei derartigen E-Mails kann die LDI NRW nur tätig werden, wenn die absendende Firma ihren Sitz in NRW oder zumindest in Deutschland hat.

Werbemails und Newsletter werden dagegen an feste Adressverteiler gesendet. Seriöse Unternehmen versenden sie nur auf Anforderung, oder wenn im Rahmen eines Vertragsabschlusses der Zusendung zugestimmt wurde. Auch am Aufbau der Mails kann in der Regel erkannt werden, ob sie einen seriösen Ursprung haben. Erfolgt eine Adresserhebung nur bei ausdrücklicher, schriftlicher Einwilligung (Double-Opt-In-Verfahren), werden die Daten in der Regel auch nicht an Dritte weitergegeben. Wird ein Link zur Abmeldung des Dienstes angeboten und steht eine Kontaktadresse oder ein Impressum zur Verfügung, so kann davon ausgegangen werden, dass es sich um ein seriöses Angebot handelt, bei dem auch auf Anfragen der Kundschaft reagiert wird. Auskunftsersuchen und Löschungsersuchen der Betroffenen werden hier meist berücksichtigt und schnell umgesetzt.

Bei unseriösem Newsletter- und Werbemailversand werden häufig Adressen gekauft oder gemietet. Dabei wird behauptet, es lägen Einwilligungen zur Zusendung von Werbung vor. Ein Nachweis über die angeblich vorliegenden Einwilligungserklärungen kann jedoch oft nicht erbracht werden. Teilweise erfolgt die Nutzung der Adressen auch in Unkenntnis der Rechtslage. Ärger mit den Betroffenen wird bewusst in Kauf genommen. In den meisten dieser Fälle wird auf Anfragen und Beschwerden der Betroffenen nicht reagiert.

Unabhängig davon, wie unverlangt zugesandte Mails eingeordnet werden, ob als Werbemail, als Newsletter oder als Spam, ist die Zusendung solcher Mails ohne Rechtsgrundlage in erster Linie ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb. Der Bundesverband der Verbraucherzentralen hatte bis zum 31. Dezember 2006 zum Kampf gegen solche Mails eine Spam-Beschwerdestelle eingerichtet. Die aus diesem Projekt gewonnenen Erkenntnisse wollen die Verbraucherzentralen dazu nutzen, ein Anti–Spam–Gesetz mit spürbar harten Sanktionen zu fordern. Sie selbst setzen ihren Kampf gegen Spam nun in Zusammenarbeit mit dem Verband der deutschen Internetwirtschaft e.V. (eco–Verband) fort. Unter der Internetadresse www.internet–beschwerdestelle.de können Betroffene dem eco–Verband per Mail unerwünscht eingetroffene Mails übermitteln.

- Bei unverlangt zugesandten E-Mails besteht neben dem Unterlassungsanspruch auch ein Recht auf Auskunft über die zur Person gespeicherten Daten und deren Herkunft sowie ein Anspruch auf deren Sperrung oder Löschung.

3.9 Ist der Rundfunkstaatsvertrag noch zu retten?

Die weiten Befugnisse der GEZ, an Daten von potentiellen Schwarzsehern zu gelangen, sollen auf Betreiben der Datenschutzbehörden im 10. Rundfunkänderungsstaatsvertrag (RÄStV) endlich datenschutzkonform geregelt werden.

Die Änderungen im 8. RÄStV hatten der Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ) die Befugnis gegeben, wie ein Privatunternehmen Adressen beim kommerziellen Adressenhandel zu erwerben, um ihrer öffentlich-rechtlichen Verpflichtung nachzugehen. Diese Vorschrift ist nicht akzeptabel. Deshalb wurde

vom Arbeitskreis Medien der Datenschutzkonferenz ein Vorschlag für eine Ermächtigungsgrundlage zur Erhebung von personenbezogenen Daten durch die Landesrundfunkanstalten bei nicht-öffentlichen Stellen erarbeitet. Ziel ist es, Art, Umfang, Dauer und Zweckbestimmung der Datenverarbeitung eindeutig festzulegen.

Eine weitere Verschlechterung für den Datenschutz brachte der 8. RÄStV bei den Regelungen der Gebührenbefreiung. Die Betroffenen müssen derzeit die Gebührenbefreiung direkt bei der GEZ beantragen und dazu ihren Sozialhilfebescheid im Original oder in Form einer beglaubigten Abschrift der GEZ übersenden. Diese Regelung beeinträchtigt das Recht auf informationelle Selbstbestimmung der Betroffenen. Mit dem Bescheid erhält die GEZ eine Vielzahl von sensiblen Sozialdaten, die sie für eine Entscheidung über die Gebührenbefreiung überhaupt nicht benötigt. Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit den Rundfunkdatenschutzbeauftragten auf einen gemeinsamen Vorschlag zur Änderung der Regelung geeinigt. Der Nachweis für die Vorraussetzungen der Gebührenbefreiung soll auch über eine Bestätigung des Leistungsträgers möglich werden, so dass der ganze Bescheid nicht mehr an die GEZ versendet werden muss.

- Für den nächsten anstehenden Rundfunkänderungsstaatsvertrag ist darauf hinzuwirken, dass die Vorschläge übernommen werden und die Sozialleistungsträger bei der Gebührenbefreiung an einer datenschutzfreundlichen Lösung mitwirken.

4 Videoüberwachung

4.1 Polizeiliche Videoüberwachung ausgeweitet

Auf der Grundlage des im Sommer 2003 geänderten Polizeigesetzes (PolG NRW) werden nunmehr nicht nur in Bielefeld, sondern auch in Düsseldorf, Mönchengladbach und Coesfeld öffentliche Straßen und Plätze durch Videoüberwachungsanlagen der Polizei beobachtet. Das ist im Hinblick auf die im Grundgesetz garantierten Freiheitsrechte bedenklich (siehe hierzu auch Bericht 2005 unter 8.1).

In Düsseldorf und Mönchengladbach werden jeweils Teile der Altstadt, in Coesfeld das Gelände rund um den Bahnhof durch die Polizei videoüberwacht. Erwartungsgemäß erwies sich dabei die fortlaufende Beobachtung der beständig übertragenen und gespeicherten Bilder als Problem. Insbesondere in Düsseldorf wurden die Bilder 24 Stunden am Tag permanent aufgezeichnet, obwohl die Beobachtung der Bilder durch Polizeibeamtinnen und Polizeibeamte auf die als tatkritisch eingestuften Zeiten beschränkt war. Eine solche Aufzeichnung der übertragenen Bilder "auf Vorrat" kann im Ergebnis ausschließlich der Beweissicherung in künftigen Strafverfahren dienen und ist mit dem präventiven Charakter des Polizeigesetzes nicht vereinbar. Das Polizeipräsidium Düsseldorf ist deshalb der Empfehlung gefolgt, die Aufzeichnung künftig auf die Zeiten zu begrenzen, in denen auch eine Beobachtung der Bilder sichergestellt ist. In Mönchengladbach und Coesfeld haben die mit der Videobeobachtung beauftragten Beamtinnen und Beamten gleichzeitig weitere Aufgaben zu erledigen. Das Polizeipräsidium Mönchengladbach hat die Empfehlung, durch geeignete organisatorische Maßnahmen eine durchgängige Beobachtung sicherzustellen, durch eine entsprechende Klarstellung in der Dienstanweisung zum Betrieb der Videoüberwachungsanlage aufgegriffen.

Grundsätzliche Bedenken bestehen gegen die Videoüberwachung am Bahnhof in Coesfeld. Zulässig ist die polizeiliche Videoüberwachung nur an Kriminalitätsbrennpunkten (Nr. 15a.0 der Verwaltungsvorschriften zum PolG NRW). Hierzu verweist die Kreispolizeibehörde Coesfeld auf die hohe Anzahl von Fahrraddiebstählen, von denen im Jahr 2003 nach Angabe der Kreispolizeibehörde 171 festgestellt worden seien. Ursächlich hierfür ist in erster Linie ein schlecht einsehbarer Abstell-

platz neben dem Bahnhofsgebäude, der gerne von den Kundinnen und Kunden der Bahn genutzt wird. Für 2004 hat die Kreispolizeibehörde Coesfeld die Anzahl der Fahrraddiebstähle nur noch mit 72, die der sonstigen Delikte mit insgesamt 20 beziffert. Ob für diesen erheblichen Rückgang tatsächlich die im Vorfeld geführte öffentliche Diskussion über die erst am 1. Dezember 2004 erfolgte Inbetriebnahme der Videoüberwachung ursächlich ist – so die Polizei – oder eine möglicherweise wenig genaue Erfassungspraxis zunächst zu einer Überzeichnung der tatsächlichen Kriminalitätsbelastung am Bahnhofsgelände geführt hat, mag dahinstehen. Jedenfalls bestehen auf der Grundlage dieser Angaben erhebliche Zweifel daran, dass es sich bei dem Gelände um den Bahnhof in Coesfeld – gemessen an der Kriminalitätsbelastung anderer Örtlichkeiten im Geltungsbereich des Polizeigesetzes – um einen Kriminalitätsbrennpunkt im Sinne des § 15a PolG NRW handelt. Die Argumentation, dass es ausschließlich auf die örtliche Situation ankomme, kann nicht zutreffend sein. Denn dann stünde zu erwarten, dass im Bereich polizeilicher Videoüberwachung jeder Maßstab für einen gleichmäßigen Gesetzesvollzug verloren ginge. Ohne Fahrraddiebstähle zu verharmlosen, muss darüber hinaus die rechtspolitische Frage erlaubt sein, ob der Gesetzgeber mit der personalintensiven, kostspieligen und tief in das Grundrecht auf informationelle Selbstbestimmung eingreifenden polizeilichen Videoüberwachung nach § 15a PolG NRW tatsächlich den etwas abgelegenen Fahrradabstellplatz im Blick hatte, oder ob hier nicht vorschnell ein eher die kommunale Selbstverwaltung und die Bahn berührendes städtebauliches Problem mit polizeilichen Eingriffsinstrumenten gelöst werden soll. Die Kreispolizeibehörde Coesfeld ist der Empfehlung, von einer weiteren Verlängerung der Maßnahme abzusehen, nicht gefolgt. Auch die an das Innenministerium gerichtete Bitte um eine fachaufsichtliche Prüfung der Maßnahme hat zu keinem anderen Ergebnis geführt.

➡ Die Videoüberwachung durch die Polizei muss auf tatsächliche Kriminalitätsbrennpunkte beschränkt bleiben. Bei der Beurteilung ist ein landesweit einheitlicher Maßstab anzuwenden.

4.2 Nicht mehr unbeobachtet in der Uni?

Darf Hochschule A ihre Bibliothek videoüberwachen? Ist es zulässig, in den PC-Pools des Seminars B Videokameras zu installieren? Und erheben sich Bedenken dagegen, eine Überwachungsanlage zu aktivieren, die die Eingangshalle der Universität C erfasst?

Nicht selten ohne großes Aufsehen – wenn auch nicht gerade verdeckt – wurden die ersten Videokameras in Hochschulen installiert, wobei dies gelegentlich gar nicht als Datenschutzproblem wahrgenommen wurde. Studierendenvertretungen, Personalräte und Datenschutzbeauftragte sowie oft auch die Hochschulverwaltungen wurden teilweise erst spät auf die Videoanlagen aufmerksam. Jetzt werden allerdings in einigen Hochschulen lebhafte Diskussionen über die Zulässigkeit von bereits vorhandenen Kameras oder neu zu installierenden Anlagen geführt, und einige Kameras sind bereits wieder deaktiviert und abgebaut worden.

Um kein Missverständnis aufkommen zu lassen: Videokameras in und an Hochschulen bilden bislang noch den Ausnahmefall – und so muss es auch bleiben. Deshalb ist zwar keine Panik, wohl aber erhöhte Aufmerksamkeit geboten.

Rechtsgrundlage für eine Videoüberwachung öffentlich zugänglicher Räume in öffentlichen Hochschulen ist § 29b Datenschutzgesetz NRW (DSG NRW). Eine Beobachtung durch Videokameras ist nur zulässig, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen. Eine Aufzeichnung der Bilder darf nur bei einer konkreten Gefahr zu Beweiszwecken erfolgen, wenn dies zum Erreichen des verfolgten Zwecks unverzichtbar ist. Beobachtung und Aufzeichnung dürfen insbesondere auch die in Art. 5 Abs. 3 Satz 1 Grundgesetz geschützte Freiheit von Wissenschaft, Forschung und Lehre nicht unzulässig einschränken. Im Übrigen haben grundsätzlich alle Personen, die sich zulässigerweise in den Hochschulen aufhalten, das Recht, sich unbeobachtet zu bewegen. Eine Videoüberwachung ist daher nur ausnahmsweise zulässig.

Gerade in Bibliotheksräumen kann sie allenfalls in besonderen Einzelfällen hingenommen werden, da sie einen erheblichen Eingriff in die

Persönlichkeitsrechte der Betroffenen darstellt. Regelmäßig fragt sich bereits, ob die Anlage überhaupt geeignet ist, die Wahrnehmung des Hausrechts – etwa den Schutz des Buchbestands vor Diebstahl und Beschädigung – sicherzustellen. In vielen Bibliotheken finden sich zwischen hohen Bücherregalen Gänge und Winkel, die es nicht wahrscheinlich erscheinen lassen, ein derartiges Vorkommnis überhaupt zu beobachten oder zu erfassen. Fällt der Verlust oder die Beschädigung eines Buches später durch Zufall auf, wird sich regelmäßig nicht mehr feststellen lassen, welche Videoaufnahmen gesichtet werden müssten, um die Täterin oder den Täter zu überführen. Da die Aufnahmen ferner zum frühest möglichen Zeitpunkt gelöscht oder überschrieben werden müssen, dürften die entscheidenden Aufzeichnungen zumeist auch gar nicht mehr vorhanden sein. Wenn das Mittel der Videoüberwachung zur Erreichung des Überwachungsziels indes ungeeignet ist, kommt seine Wahl bereits aus diesem Grund nicht in Betracht. Eine Überwachung von Arbeitsplätzen der Nutzerinnen und Nutzer in Bibliotheken begegnet im Übrigen insbesondere im Hinblick auf die Forschungs- und Wissenschaftsfreiheit der Betroffenen grundsätzlichen Bedenken. Etwas anderes kann nur ausnahmsweise gelten, wenn Videokameras etwa auf Arbeitsplätze im Handschriftenlesesaal einer Bibliothek gerichtet sind. Wegen des außergewöhnlichen Werts und der Einmaligkeit der Werke müssen hier gegebenenfalls die Bedenken gegen die Beobachtung der Nutzerinnen und Nutzer zurückgestellt werden. Die Videoüberwachung ist allerdings auf das erforderliche Mindestmaß zu beschränken.

Besondere Probleme wirft auch die Überwachung von PC-Arbeitsplätzen in sogenannten Cip-Pools auf. Solange Beschäftigte der Hochschulen als Aufsicht in den Räumen anwesend oder die Geräte besonders gesichert sind, dürfte sich die Erforderlichkeit einer Videoüberwachung zum Schutz der Geräte vor Diebstahl und Beschädigung kaum begründen lassen. Deswegen kommt eine Videoüberwachung dieser PC-Räume grundsätzlich nur dann in Betracht, wenn die Wahrnehmung des Hausrechts durch keine Aufsichtsperson oder durch anderweitige technische Sicherheitsmaßnahmen gewährleistet ist. Ferner muss die Überwachung im Einzelfall auch verhältnismäßig sein. Grundsätzlich dürfte es genügen, allenfalls an den Zugängen zu den Räumen Videokameras zu installieren. Dann wäre zumindest sichergestellt, dass die berechtigten Nutzerinnen und Nutzer an den PC-Plätzen unbeobachtet arbeiten können.

Auch die Installation einer Überwachungsanlage in der Eingangshalle einer Universität darf ausschließlich zum Zweck der Wahrnehmung des Hausrechts erfolgen. Jedenfalls solange die Halle regelmäßig bevölkert ist, dürfte die Erforderlichkeit äußerst fraglich sein; in der Regel überwiegen hier die Interessen der sich zulässigerweise in der Eingangshalle aufhaltenden Menschen, sich unbeobachtet zu bewegen. Die Videoüberwachung eines Gebäudeteils kommt im Übrigen grundsätzlich nur in Betracht, sofern es belegbare Vorkommnisse gibt, die die Annahme rechtfertigen, dass auch künftige schwerwiegende Beeinträchtigungen der durch das Hausrecht geschützten Interessen drohen. Gab es beispielsweise nachts bereits Einbruchs- oder Diebstahlsfälle und sind weitere derartige Delikte zu besorgen, kann es erforderlich, aber auch ausreichend sein, in der Nacht eine Videoanlage zu aktivieren.

Soweit die Videoüberwachung im Einzelfall ausnahmsweise zulässig ist, hat die Hochschule die überwachten Bereiche grundsätzlich durch geeignete Hinweisschilder zu kennzeichnen. Im Übrigen muss sie selbstverständlich den allgemeinen Anforderungen insbesondere auch der §§ 8, 10 DSG NRW Rechnung tragen, also gegebenenfalls ein Verfahrensverzeichnis führen und ein Sicherheitskonzept erstellen.

➧ Vor der Installation von Videokameras in Hochschulen ist die Zulässigkeit der geplanten Videoüberwachung in jedem Einzelfall unter Berücksichtigung aller konkreten Umstände sorgfältig zu prüfen und zu begründen. Dabei ist zwischen der Videobeobachtung und der Aufzeichnung zu unterscheiden. Grundsätzlich gilt, dass eine Videoüberwachung im Hochschulbereich nur im Ausnahmefall in Betracht kommt.

4.3 Ich sehe das, was Du so tust – Videoüberwachung an und in Schulen

Videoüberwachung ist in Schulen nach wie vor ein Thema, aber leider nicht nur, weil dies ein wichtiger Unterrichtsgegenstand ist – oder wäre –, sondern weil einige Schulen noch immer erwägen, Überwachungsanlagen zu installieren, oder weil sie Videokameras sogar bereits aktiviert haben.

Videoüberwachung ist grundsätzlich mit dem Schulzweck nicht vereinbar. Auf keinen Fall ist die Überwachung während des Unterrichts zu-

lässig. Aus aktuellem Anlass war diese Problematik bereits im Bericht 2005 unter 4.1 aufgegriffen worden. Vertiefende Hinweise und Empfehlungen gibt nunmehr die neue Orientierungshilfe "Ich sehe das, was Du so tust – Videoüberwachung an und in Schulen" der LDI NRW. Anhand von Beispielen werden wesentliche Probleme dargestellt und erklärt.

- Videoüberwachung an Schulen kann nur in wenigen begründeten Einzelfällen und grundsätzlich nur außerhalb von Schulzeiten zulässig sein. Eine Broschüre zu diesem Themenkomplex ist auf der Internetseite www.ldi.nrw.de zu finden und kann auch in Papierform angefordert werden.

4.4 Videoüberwachung auf Bahnhöfen

Die in Nordrhein-Westfalen im Sommer 2006 versuchten Koffersprengstoffanschläge haben der Forderung nach Ausweitung der Videoüberwachung Nachdruck verliehen. Eine grenzenlose Überwachungseinrichtung auf allen Bahnhöfen dürfte indes eine riesige Datenmenge produzieren, die auf einem unüberschaubaren Datenfriedhof landen wird.

Während die Ausstattung von 33.000 Zügen mit Kameras schon an zu hohen Kosten scheitert, lässt sich eine weitere Ausstattung von Bahnhöfen – bei jetzt bundesweit etwa 3.000 Kameras – finanziell eher bewältigen. Das allein kann aber kein durchschlagendes Kriterium sein. Ein Einsatz von Videoüberwachungseinrichtungen kann nur dann sinnvoll und damit als Eingriff in die Freiheitsrechte der großen Mehrheit der unbescholtenen Bahnreisenden gegebenenfalls hinnehmbar sein, wenn über die Beobachtung der Videoaufnahmen Vorkommnisse erkannt und Einsatzkräfte am Ort des Geschehens rechtzeitig Hilfe leisten und Gefahren abwehren können. Keine Videokamera kann jedoch einen aktuellen Angriff verhindern.

Videoüberwachung, die ausschließlich und allein zu dem Zweck der nachträglichen Aufklärung von Vorkommnissen eingerichtet ist, kann sich nicht aus § 6b Bundesdatenschutzgesetz rechtfertigen. Außerdem gibt diese Rechtsgrundlage eine flächendeckende Videoüberwachung auf allen Bahnhöfen nicht her. Mit einer flächendeckenden Videoüberwachung würde zudem eine Überwachungsinfrastruktur geschaffen,

die es in Verbindung mit zur Zeit getesteten Gesichtserkennungssystemen (wie im Bahnhof Mainz) ermöglichte, Bewegungsprofile bestimmter Personen zu gewinnen, zu speichern und auszuwerten. Dies wäre seiner Eingriffsqualität nach ein weiterer Schritt zum Orwellschen Überwachungsstaat. Die Rechte der Fahrgäste würden hierbei unverhältnismäßig eingeschränkt.

➡ Die Ausweitung von Videoüberwachung auf Bahnhöfen darf nur in dem Maße erfolgen, wie es der Schutz vor gewalttätigen Übergriffen gegen Personen oder vor Zerstörung der Beförderungseinrichtungen gebietet. Die Bedrohungslage muss regelmäßig überprüft werden.

4.5 Videoüberwachung von Arbeitsplätzen

Ob Büro- oder Verkaufsräume, Produktions- oder Lagerhallen oder Betriebshöfe – die Einsatzfelder der Videoüberwachung sind nahezu unbegrenzt und ziehen sich quer durch viele Branchen. Dabei werden von den Kameras regelmäßig auch – beabsichtigt oder nicht – Arbeitsplätze erfasst.

Verständlich sind daher die zahlreichen Anfragen von Betriebsräten und betroffenen Beschäftigten, in deren Betrieben die Videobeobachtung geplant oder bereits betrieben wird. § 6b Bundesdatenschutzgesetz (BDSG) regelt die Videoüberwachung durch private Stellen in öffentlich zugänglichen Räumen wie zum Beispiel in Verkaufsräumen eines Warenhauses. Die Videoüberwachung muss zur Wahrung des Hausrechts oder eines anderen berechtigten Interesses für konkret festgelegte Zwecke erforderlich sein, und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ist § 6b BDSG nicht anwendbar, weil die Videoüberwachung in nicht öffentlich zugänglichen Räumen erfolgt, sind das allgemeine Persönlichkeitsrecht und die allgemeinen Vorgaben des BDSG zu beachten.

Bei einer Videoüberwachung von Beschäftigten an ihren Arbeitsplätzen ist darüber hinaus die arbeitsgerichtliche Rechtsprechung von Bedeutung. Danach erzeugt bereits die bloße Möglichkeit der jederzeitigen Videoüberwachung von Arbeitsplätzen einen mit dem Anspruch der Beschäftigten auf Wahrung ihrer Persönlichkeitsrechte (§ 75 Abs. 2

Betriebsverfassungsgesetz) regelmäßig nicht zu vereinbarenden Überwachungsdruck. Eine solche Überwachung könnte nur durch besondere Sicherheitsinteressen des Unternehmens ausnahmsweise gerechtfertigt sein (siehe Bericht 2005 unter 4.4). Folgende exemplarische Fälle zeigen Lösungsmöglichkeiten:

Vor dem Hintergrund von zum Teil erheblichen Diebstählen sollten auf dem Firmengelände eines Druck- und Verlagsunternehmens Kameras zum Objektschutz sowie zur Unterstützung bei Ermittlungen im Falle krimineller Handlungen installiert werden. Bei der Besichtigung des Firmengeländes musste allerdings festgestellt werden, dass in einem Kamerabereich ständig Arbeitsplätze an einer Verladerampe erfasst werden konnten. Durch einfache Veränderung des Kamerasystems konnte die Erfassung der betroffenen Arbeitsplätze vermieden, gleichwohl aber der zu sichernde Bereich wie beabsichtigt beobachtet werden. Die einzelnen Kamerastandorte wurden in einer Betriebsvereinbarung festgeschrieben.

Zum Schutz vor nächtlichen Einbrüchen und um seine Beschäftigten vor tätlichen Übergriffen zu schützen, hatte ein Funkmietwagenunternehmen die Überwachungskameras in dem Aufenthaltsraum für die Fahrerinnen und Fahrer sowie im Funkraum so positioniert, dass die Betroffenen stets von den Kameras erfasst wurden. Dem Sicherheitsinteresse des Unternehmens kann hier auch durch andere, das Persönlichkeitsrecht weniger einschränkende Maßnahmen Rechnung getragen werden. Dazu wurde empfohlen, die Videokameras allein auf die gefährdeten Raumbereiche (insbesondere Fenster und Türen) auszurichten. Das Funkmietwagenunternehmen hat die Videokameras entsprechend neu justiert.

Bei der Videoüberwachung in Kaufhäusern, Einkaufszentren und sonstigen Verkaufsräumen werden zunehmend sogenannte Dome-Kameras eingesetzt. Wegen ihrer kompakten, kuppelförmigen Bauweise können diese Kameras höchst unauffällig installiert werden und erlauben damit eine diskrete Überwachung. Außerdem verfügen sie über umfangreiche Funktionen wie das Endlos-Schwenken über 360º und Zoommöglichkeiten. Wenngleich mit dieser Technik die Überwachung von Kundinnen und Kunden unter bestimmten Voraussetzungen zulässig sein kann (zu beachten ist insbesondere die Hinweispflicht auf die Videoüberwachung und die Verpflichtung zur unverzüglichen Löschung des Bildmaterials, § 6b Abs. 5 BDSG), ergeben sich aus Sicht des Beschäf-

tigtendatenschutzes Probleme, die in einer Filiale eines großen Lebensmittelunternehmens erkennbar wurden:

Zum Schutz vor Warendiebstahl betreibt die Unternehmensgruppe in zahlreichen ihrer Filialen Videoüberwachungssysteme mit solchen Dome-Kameras. Auf Grund ihres Wirkungsgrades werden die Verkaufsräume in den Filialen nahezu vollständig erfasst. Damit kann auch das Verkaufspersonal mitbeobachtet werden. Durch technische Beschränkung der Erfassungswinkel der Dome-Kameras auf diebstahlgefährdete Bereiche, etwa bestimmte Warengruppen, will das Unternehmen nunmehr eine Mitbeobachtung des Verkaufspersonals auf das unvermeidbare Minimum reduzieren.

➧ Bei der Videoüberwachung ist darauf zu achten, dass die Beschäftigten keiner dauerhaften Beobachtung unterliegen, die einen unverhältnismäßigen Überwachungsdruck zur Folge haben kann.

4.6 Der alte Müll und noch mehr

Was die Videoüberwachung einer Mülldeponie mit Datenschutz zu tun hat? Ganz einfach: Solange Videokameras nur Müllberge und Kleintiere erfassen, gibt es natürlich kein Datenschutzproblem. Probleme treten aber dann auf, wenn Nutzerinnen und Nutzer oder Beschäftigte der Deponie beobachtet und kontrolliert werden.

So ist es auch im vorliegenden Fall: Soweit die Kameras nicht zeitweise aus technischen Gründen deaktiviert sind, wird sowohl eine Mülldeponie als auch eine Müllumladestation videoüberwacht, wobei in diesen – während des Geschäftsbetriebs – öffentlich zugänglichen Bereichen Nutzende und Beschäftigte gleichermaßen erfasst werden. Mit den Kameras kann beobachtet werden, und die Aufnahmen werden zugleich aufgezeichnet. Verantwortlich für die Videoüberwachung ist der öffentliche Betreiber der Deponie, der sich hartnäckig weigert, die Kameras wieder abzubauen.

Dabei sind hier sowohl Videobeobachtung als auch Videoaufzeichnung unzulässig, weil die Voraussetzungen des § 29b Datenschutzgesetz NRW nicht erfüllt sind. Die Beobachtung dient nicht lediglich der Wahrung des Hausrechts, weil der Betreiber der Deponie mit Hilfe der Kameras nicht nur ihren ordnungsgemäßen Zustand, sondern auch

den Betriebsablauf als solchen überwachen und die Erfüllung der gesetzlich übertragenen Aufgaben sicherstellen will. Die Kontrolle der Aufgabenerfüllung hat jedoch nichts mehr mit dem Hausrecht zu tun. Der Eingriff in das informationelle Selbstbestimmungsrecht ist auch erheblich, da die Personen, die sich auf dem Deponiegelände aufhalten, letztlich der Videoüberwachung gar nicht ausweichen können. Bezogen auf die Nutzenden ist die Beobachtung durch den – aus anderen Gründen – gesetzlich ohnehin vorgeschriebenen Einsatz von Personal das mildere Mittel im Verhältnis zur permanenten Beobachtung durch Videokameras. Mit der Überwachung ist überdies zugleich eine ständige Kontrolle der Beschäftigten möglich (insoweit wird auf den Beitrag "Videoüberwachung am Arbeitsplatz" unter 4.5 verwiesen). Der Einsatz der Videokameras ist damit insgesamt nicht gerechtfertigt.

Da bereits die Videobeobachtung der Deponie und des Umladeplatzes unzulässig ist, gilt dies erst Recht für die Speicherung der Videoaufnahmen. Eine solche Speicherung wäre nur bei konkreter Gefahr zu Beweiszwecken erlaubt, wenn dies zum Erreichen des verfolgten Zwecks unverzichtbar wäre. Dass diese Voraussetzungen erfüllt sind, ist weder vorgetragen noch ansonsten ersichtlich.

Die Videokameras könnten allenfalls dann hingenommen werden, wenn sie keine personenscharfen Bilder, sondern ausschließlich Übersichtsaufnahmen auf einen Monitor übertragen würden. Dies ist bislang jedoch nicht der Fall und offensichtlich auch zukünftig nicht beabsichtigt.

➡ Die auf der Deponie und dem Umladeplatz unzulässig installierten Kameras müssen deaktiviert und abgebaut werden. Da sich die verantwortliche Stelle fortdauernd weigerte, diese Konsequenz zu ziehen, ist inzwischen eine Beanstandung ausgesprochen worden.

5 Bildung und Wissenschaft

5.1 Keine Schülerstatistik ohne Datenschutz

Bestrebungen aus dem Bereich der Kultusministerkonferenz gehen seit 2003 dahin, eine detaillierte Bildungsstatistik zu entwickeln. Komplette Bildungsverläufe sollen personenscharf erfasst werden.

Hinter dieser Zielrichtung verbirgt sich ein datenschutzrechtlich brisantes Projekt. Bisher ist geplant, nach einheitlichen Kriterien umfangreiche, bundesweit aktuelle Datensätze aller Schülerinnen und Schüler sowie Lehrerinnen und Lehrer für ihr gesamtes "Schulleben" zu schaffen. Dabei sollen die Betroffenen eine Identifikationsnummer erhalten. Unter anderem soll bei Schülerinnen und Schülern das Geburtsland gespeichert werden, bei nichtdeutscher Herkunft die zu Hause gesprochene Sprache und die Information, ob und wie oft eine Klasse wiederholt worden ist.

Ausdrücklich zu begrüßen ist, dass das Ministerium für Schule und Weiterbildung NRW keine Notwendigkeit für die Einführung einer Identifikationsnummer für Schülerinnen und Schüler sieht. Die Daten haben in den Schulen zu verbleiben. Nur für Zwecke der Planung und Statistik dürfen sie – allerdings lediglich in anonymisierter Form – dem Landesamt für Datenverarbeitung und Statistik übermittelt sowie für Maßnahmen der Qualitätsentwicklung und -sicherung genutzt werden (§ 121 Abs. 6 Schulgesetz NRW).

Gegenüber dieser datenschutzkonformen Vorgehensweise lassen die Planungen von Teilen der Kultusministerkonferenz zur Schaffung einer bundesweiten Datenbank eine präzise und einheitliche Zweckbestimmung bisher nicht erkennen. Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann.

Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden zahlreichen wissenschaftlichen Untersuchungen (wie PISA, IGLU, TIMMS, Shell-Jugendstudien) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- oder lehrerbezogenen "Bil-

dungsregisters" nicht dargetan. Hierauf haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 26./27. Oktober 2006 (abgedruckt im Anhang) hingewiesen.

- Auf eine Identifikationsnummer muss verzichtet werden. Daten von Schülerinnen und Schülern dürfen für statistische Zwecke nur anonymisiert von der Schule an das Landesamt für Datenverarbeitung und Statistik übermittelt werden.

5.2 Kompetenzcheck Ausbildung – ein Service mit unbekannten Folgen

Schülerinnen und Schüler der Klasse 9 hatten auch im Frühjahr 2006 wieder die Gelegenheit, das Angebot einer kostenlosen Trainingsmaßnahme in Anspruch zu nehmen: Den Kompetenzcheck Ausbildung NRW. Dieser Service wurde als Möglichkeit beworben, einmal außerhalb der Schule die eigenen Stärken und Fähigkeiten sowie verschiedene Berufsfelder praktisch kennen zu lernen.

Worüber die Jugendlichen nicht informiert wurden, war die geplante Übermittlung der Testergebnisse an die jeweils zuständige Lehrkraft als wesentlicher Baustein der Förderungsbemühungen des Arbeitsministeriums. Danach soll die Lehrkraft an die Ergebnisse zur sozialen Kompetenz anknüpfen und dadurch eine gezielte Förderung der Jugendlichen unterstützen.

Über diese zusätzliche Zweckbestimmung des Kompetenzchecks sind die betroffenen Personen aufzuklären. In dem an die LDI NRW herangetragenen Fall wurde durch den privaten Bildungsträger jedoch vielmehr der gegenteilige Eindruck erweckt, das Angebot stelle eine (einmalige) Beratungsleistung für die Jugendlichen und deren Eltern dar. Es wurde suggeriert, dass die Jugendlichen Hilfestellungen erhalten, die sie selbst in den eigenen Bewerbungsbemühungen nutzbar machen könnten. Ein weiterer Zweck, insbesondere im Hinblick auf die Lehrtätigkeit der Schule, wurde gerade nicht erwähnt.

Das zuständige Arbeitsministerium wurde darüber unterrichtet, dass eine Übermittlung der Ergebnisse des Kompetenzchecks mangels wirksamer Einwilligung weder an die zuständige Schule noch an Institutionen der Arbeitsvermittlung erfolgen darf. Als Grundlage der Übermitt-

lung der Testergebnisse kommt ausschließlich das Vorliegen einer wirksamen Einwilligungserklärung in Betracht.

- Das Arbeitsministerium muss die umfassende Information der Schülerinnen und Schüler über die Zwecke von Kompetenzchecks sicherstellen. Ohne wirksame Einwilligung der Betroffenen dürfen sensible Angaben zur sozialen Kompetenz und anderer "soft skills" nicht übermittelt werden, auch nicht an die zuständige Lehrkraft.

5.3 Überraschend unbekannt: Die Datenschutzbeauftragten der Schulen

Es gibt sie wirklich, die für Schulen bestellten Datenschutzbeauftragten, auch wenn dies vielen Schülerinnen und Schülern, Eltern und Lehrkräften noch nicht bekannt ist. Nach eigenem Bekunden werden diese Beauftragten häufig allerdings von ihrer Bestellung – mehr oder weniger – selbst überrascht, so dass die erforderlichen Kenntnisse oft noch fehlen.

Die Pflicht zur Bestellung von behördlichen Datenschutzbeauftragten gibt es schon lange: Seit Inkrafttreten der "neuen" Fassung des Datenschutzgesetzes NRW (DSG NRW) im Jahr 2000 müssten – auch – alle öffentlichen Schulen in Nordrhein-Westfalen Datenschutzbeauftragte bestellt haben. Da Theorie und Praxis in diesem Punkt jedoch erheblich auseinander fielen, wurde im Oktober 2004 durch Verordnung – § 1 Abs. 6 Satz 3 der Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer (VO-DV II) – bestimmt, dass für Schulen in kommunaler und staatlicher Trägerschaft das Schulamt eine Person bestellt, die die Aufgaben der oder des behördlichen Datenschutzbeauftragten gemäß § 32a DSG NRW wahrnimmt.

Diese eigentlich eindeutig und unmissverständlich erscheinende Regelung hat vor Ort unerwartet neue Fragen aufgeworfen. Zur Klarstellung: Jedes Schulamt hat für alle Schulen innerhalb seines Bezirks, also auch für jene, die – wie etwa Gymnasien, Realschulen und Berufskollegs – nicht seiner Aufsicht unterliegen, eine gemeinsame Datenschutzbeauftragte oder einen -beauftragten zu bestellen. Diese haben nicht etwa die Datenverarbeitung in den Schulämtern zu kontrollieren, sondern sind vielmehr für die Überwachung der Datenverar-

beitung in den und durch die Schulen zuständig. Auch wenn die Regelung in der VO-DV II verankert ist, unterfallen der Kontrolle durch die schulischen Datenschutzbeauftragten nicht nur die personenbezogenen Daten der Lehrkräfte, sondern auch die der sonstigen Beschäftigen sowie der Schülerinnen, Schüler und Erziehungsberechtigten.

Ursprünglich war davon ausgegangen worden, dass in der Regel Beschäftigte der Schulämter zu schulischen Datenschutzbeauftragten bestellt würden. In der Praxis werden stattdessen oftmals Lehrkräfte mit dieser Aufgabe betraut und hierfür – leider nur zu einem geringen Anteil – von ihrer Lehrtätigkeit freigestellt. Eine Bestellung von Schulleiterinnen und -leitern scheidet allerdings prinzipiell aus, weil es ansonsten zu Interessenkollisionen kommen könnte. Personen mit eigener Leitungsfunktion kommen grundsätzlich nicht für diese Aufgabe in Betracht.

Wie viele Rückfragen von neu bestellten Datenschutzbeauftragten zeigen, fehlen oftmals noch fundamentale Grundkenntnisse. Einzelne Bezirksregierungen haben dieses Problem inzwischen erkannt und kurzfristig zweitägige Basisseminare initiiert. Ganz sicher bedarf es noch ähnlicher und vertiefender Fortbildungen. Zu begrüßen wäre außerdem, wenn die schulischen Datenschutzbeauftragten in Arbeitsgruppen regelmäßig ihre Erfahrungen untereinander austauschen würden, so wie es bereits seit vielen Jahren im Bereich der Hochschulen geschieht. Nicht für jedes Problem muss "das Rad neu erfunden" werden. Dies gilt auch und gerade in Sachen Datenschutz und Datensicherheit.

- Die Bestellung von Datenschutzbeauftragten für die Schulen ist wichtig. Dabei allein kann es jedoch nicht bleiben; vielmehr muss das Fortbildungsangebot ausgebaut und der gegenseitige Erfahrungsaustausch gefördert werden. Vor allem aber sollte in den Schulen auch bekannt gegeben werden, wer die oder der schulische Datenschutzbeauftragte ist.

5.4 Qualitätssicherung und -entwicklung in Schulen

Wer macht in der Schule was warum wozu? Welche Modernisierungen würden Sie als Lehrkraft an Ihrer Schule einführen? Was hältst Du von Deiner Schule, und wie wünschst Du Dir Dei-

nen Unterricht? Welchen Änderungsbedarf sehen Sie in der Schule Ihres Kindes?

Dass Schulen sowohl Gegenstand zahlreicher Forschungsvorhaben als auch beliebte Kontaktstellen für Forschende sind, die vor allem Schülerinnen und Schüler zu den unterschiedlichsten Themen befragen, wurde bereits im Bericht 2001 unter 13.3 eingehend thematisiert und gilt noch heute. In den letzten Jahren sind darüber hinaus – nicht zuletzt durch Vergleichsstudien wie etwa PISA, IGLU und DESI – die Themen Qualitätssicherung und Qualitätsentwicklung in Schulen zunehmend in den Focus der Diskussion gerückt: Schulaufsichtsbehörden und Schulleitungen, Lehrkräfte und Erziehungsberechtigte, Schülerinnen und Schüler haben letztlich ein gemeinsames Interesse daran, dass Schulen qualitativ optimiert werden.

Der Gesetzgeber reagierte auf diesen Trend schon in der Vergangenheit, indem das damalige Schulverwaltungsgesetz dahingehend ergänzt wurde, dass standardisierte Tests und schriftliche Befragungen von Schulanfängerinnen und -anfängern, Schülerinnen und Schülern fortan ohne Einwilligung der Betroffenen oder ihrer Erziehungsberechtigten durchgeführt werden durften, soweit dies für Maßnahmen der Qualitätsentwicklung und -sicherung erforderlich war. Eine entsprechende Regelung wurde zeitgleich auch in Bezug auf die Lehrkräfte eingeführt. Schülerinnen und Schüler sowie Lehrerinnen und Lehrer sind seitdem verpflichtet, sich nach Maßgabe entsprechender Vorgaben der Schulaufsicht an Maßnahmen der Qualitätsentwicklung und -sicherung, insbesondere auch an Vergleichsuntersuchungen, zu beteiligen. Diese Vorschriften sind fast wortgleich in das neue Schulgesetz übernommen worden, das in diesem Zusammenhang zudem eine Neuerung enthält: Nunmehr dürfen für die in Rede stehenden Zwecke – unter bestimmten gesetzlich festgelegten Voraussetzungen, unter anderem der Genehmigung durch das Schulministerium – auch Bild- und Tonaufnahmen des Unterrichts erfolgen.

Damit sind verschiedene Befugnisse geschaffen worden, personenbezogene Daten zum Zweck der Qualitätssicherung und -entwicklung ohne die Einwilligung der Betroffenen zu verarbeiten. Dieser Datenverarbeitung sind zugleich aber feste Grenzen gesetzt. Insbesondere muss eine Datenverarbeitung zu dem genannten Zweck geeignet und erforderlich sein, und es besteht eine Beteiligungspflicht nach Maßgabe entsprechender Vorgaben der Schulaufsicht.

Dass diesen Voraussetzungen hinreichend Rechnung getragen wird, ist in der Praxis leider nicht immer sichergestellt. Probleme ergeben sich vor allem, wenn eine Schule oder eine Lehrkraft in eigener Initiative eine Befragung durchführt. Zwar gibt es kein Datenschutzproblem, solange ausschließlich anonymisierte Daten erhoben werden, aber Vorsicht: Der Teufel steckt hier oft im Detail. So wird in der Schule X unschwer zu ermitteln sein, wer der 14jährige Schüler der Klasse 5a ist, der den Fragebogen ausgefüllt hat; damit sind zugleich auch alle in dem Bogen enthaltenen Angaben auf ihn beziehbar. Ebenso wird in der Klasse Y die Klassenlehrerin, die einen Fragebogen mit offenen Antwortkategorien ausgegeben hat, viele der ausgefüllten Bogen allein anhand der Handschriften einzelnen Kindern zuordnen können. Davon abgesehen betreffen die Fragen oft – jedenfalls mittelbar – einzelne Lehrkräfte, und die Antworten sind mithin ebenfalls insoweit personenbezogen.

Werden bei einer Befragung in Schulen indes personenbezogene oder -beziehbare Daten erhoben, genügt es nicht, dass dies nach der subjektiven Zielsetzung der verantwortlichen Person etwa die Qualität der Schule verbessern soll und dass die Daten nach ihrer Einschätzung zu diesem Zweck geeignet und erforderlich sind. Vielmehr muss es entsprechende Vorgaben der Schulaufsicht geben, damit die Datenverarbeitung ohne Einwilligung der Betroffenen zulässig ist. Wie diese Vorgaben aussehen müssen, ist gesetzlich nicht geregelt.

Wird – wie bei den bekannten Vergleichsstudien – die Durchführung des jeweiligen Forschungsvorhabens durch das Schulministerium genehmigt, umfasst diese Genehmigung auch die Prüfung und Feststellung, dass den Datenschutzbelangen der Betroffenen hinreichend Rechung getragen wird. Die Lehrkräfte sowie gegebenenfalls auch die Schülerinnen und Schüler können aufgrund und nach Maßgabe dieser Genehmigungen zur Teilnahme verpflichtet werden. Wenn dagegen kein konkretes Projekt genehmigt wird und die genannten Personengruppen gleichwohl verpflichtend an einer Qualitätssicherungsuntersuchung teilnehmen sollen, müssen die Vorgaben der Schulaufsicht insbesondere auch Bestimmungen über Art, Umfang und Behandlung der zu erhebenden und zu verarbeitenden Daten der betroffenen Personen enthalten, wobei die Vorgaben selbstverständlich zugleich auch den Grundsätzen der Erforderlichkeit und der Datenvermeidung Rechnung tragen müssen. Ohne derartig bestimmte Vorgaben oder eine konkrete

Genehmigung der Schulaufsicht ist eine Umfrage, bei der personenbezogene Daten erhoben und verarbeitet werden, grundsätzlich nur mit wirksamer Einwilligung der Betroffenen und damit nur auf freiwilliger Basis zulässig.

- Das Schulgesetz sieht Möglichkeiten vor, personenbezogene Daten der Schülerinnen und Schüler sowie der Lehrkräfte auch ohne deren Einwilligung zum Zweck der Qualitätssicherung und -entwicklung zu verarbeiten – allerdings nur unter Beachtung der normierten Voraussetzungen und nach Maßgabe hinreichend bestimmter Vorgaben der Schulaufsicht.

5.5 Schulen ans Netz! – Fotos auf die Schulhomepage?

Schulen möchten – gerade im Wettbewerb mit anderen – ihre Homepages attraktiv gestalten. Für viele gehört dazu scheinbar zwingend, auch Fotos von Schülerinnen, Schülern, Eltern und Lehrkräften ins Internet zu stellen. Leider werden dabei die Voraussetzungen einer solchen – weltweiten – Veröffentlichung wie auch die möglichen Folgen für einzelne Betroffene nicht immer hinreichend berücksichtigt.

Wie dringend der Wunsch ist, Fotos auf die Website der Schule zu stellen, wird im Rahmen der Veranstaltungsreihe "IT-Sicherheit macht Schule in NRW" immer wieder deutlich. An diesen Veranstaltungen, die seit November 2004 von der Landesinitiative "secure-it.nrw" in Zusammenarbeit mit dem Verein Schulen ans Netz und anderen durchgeführt werden, beteiligt sich die LDI NRW regelmäßig mit einem Kurzreferat sowie anschließendem Workshop zum Thema: "Datenschutz – Was darf auf die Schulhomepage?" Zentraler Diskussionsstoff ist dabei zumeist die Frage, welche Fotos die Schule unter welchen Bedingungen ins Netz stellen darf.

Wie alle anderen öffentlichen Stellen des Landes dürfen Schulen personenbezogene Daten – also auch Fotos, auf denen Personen erkennbar abgebildet sind – nur veröffentlichen, wenn eine Rechtsvorschrift dies erlaubt oder die Betroffenen eingewilligt haben. Besondere Rechtsvorschriften, die die Veröffentlichung von Abbildungen von Personen zum Gegenstand haben, finden sich insbesondere im Kunsturhebergesetz (KunstUrhG): Nach § 22 dürfen Fotos grundsätzlich nur

mit Einwilligung der abgebildeten Person verbreitet oder öffentlich zur Schau gestellt werden; § 23 lässt eng begrenzte Ausnahmen von diesem Grundsatz beispielsweise für Bilder zu, auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen oder etwa für Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben, sofern dabei nicht die berechtigten Interessen der abgebildeten Person verletzt werden. Manche Schulen halten diese Regelung irrtümlich für eine Generalermächtigung zum Einstellen aller Fotos, auf denen beispielsweise mehrere Personen abgebildet sind, oder die anlässlich von Veranstaltungen (etwa Schul- und Sportfesten) aufgenommen wurden. Damit verkennen sie nicht nur die engen Grenzen, innerhalb derer das KunstUrhG eine Veröffentlichung ohne die Einwilligung der Betroffenen erlaubt. Vielmehr übersehen sie vor allem den entscheidenden "Haken": Schulen haben vorrangig die schulspezifischen Datenschutzregelungen der §§ 120 ff. Schulgesetz NRW (SchulG NRW) zu beachten, die in ihrem Anwendungsbereich die Veröffentlichungsbefugnisse nach dem KunstUrhG verdrängen.

Prinzipiell dürfen Schulen personenbezogene Daten nur verarbeiten, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Eine Schule hat dabei ganz andere Aufgaben als beispielsweise die Presse, auf die in den Diskussionen in diesem Zusammenhang immer wieder verwiesen wird. Welche Daten an wen übermittelt werden dürfen, ist im SchulG NRW geregelt. Eine bereichsspezifische Regelung für die Datenübermittlung an Dritte – die damit auch für die Veröffentlichung von Fotos im Internet maßgeblich ist – findet sich in §§ 120 Abs. 5 Satz 3, 121 Abs. 1 Satz 4 SchulG NRW. Danach ist eine solche Übermittlung grundsätzlich nur zulässig, wenn ein rechtlicher Anspruch auf die Bekanntgabe der Daten besteht und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden oder wenn die Betroffenen im Einzelfall eingewilligt haben. Da ein rechtlicher Anspruch bei einer Veröffentlichung von Fotos auf der Schulhomepage ersichtlich nicht gegeben ist, bleibt nur die zweite Alternative, nämlich die Einwilligung. Konsequenz: Die Veröffentlichung von Fotos auf der Homepage der Schule bedarf in jedem Fall der wirksamen Einwilligung der betroffenen Personen oder – wenn diese noch nicht selbst einwilligungsfähig sind – ihrer Erziehungsberechtigten.

Diese "Einwilligungslösung" ist gerade im Schulbereich richtig und wichtig. Zum einen halten sich die Betroffenen in der Sphäre der Schule oftmals nicht freiwillig, sondern aufgrund bestehender Pflichten auf, so dass ihnen insoweit kein Wahlrecht bleibt. Sie müssen auch bei schulischen Veranstaltungen darauf vertrauen dürfen, dass Fotos von ihnen nicht ohne Weiteres ins Internet gestellt werden. Zum anderen verdeutlichen Praxisberichte nachhaltig, dass eine Veröffentlichung von Fotos für die Abgebildeten in Einzelfällen durchaus gravierende Folgen haben kann. So berichteten Lehrkräfte beispielsweise, dass die Aufenthaltsorte bestimmter Kinder unbedingt geheimgehalten werden müssten, da sie bereits Opfer von Entführungen im Zuge innerfamiliärer Streitigkeiten gewesen seien oder derartige Kindesentziehungen drohten. Solche familiären Probleme sind den Schulen oftmals gar nicht bekannt. Manche Eltern haben Angst, dass Fotos ihrer Kinder Sexualstraftaten begünstigen könnten. Ferner gibt es Abbildungsverbote aus religiösen Gründen.

Wo der Wille zu datenschutzgerechtem Handeln besteht, lassen sich für die Schulen auch praktikable Wege finden, um die erforderlichen Einwilligungen einzuholen. So kann mit vorheriger umfassender Information eine erstmalige Einwilligung beispielsweise zeitgleich mit der Anmeldung in der Schule erklärt werden, wobei allerdings – wie auch später – stets die Freiwilligkeit der Entscheidung sichergestellt werden muss. Wird die Einwilligung verweigert oder widerrufen, hat die Schule dies zu respektieren. Durch verschiedene Ankreuzalternativen sollten die Betroffenen ferner über den Umfang ihrer Einwilligung selbst entscheiden können.

Schulen, die die Datenschutzbelange ernst nehmen, haben übrigens erfahrungsgemäß durchaus keine Nachteile zu befürchten. Im Gegenteil: Bei entsprechender (Selbst-) Darstellung dürfte ihr datenschutzgerechtes Handeln vielmehr zu einem echten Wettbewerbsvorteil führen.

- Fotos, auf denen Personen erkennbar abgebildet sind, dürfen prinzipiell nur mit wirksamer Einwilligung der Betroffenen auf der Schulhomepage veröffentlicht werden.

5.6 Alumni-Kontaktpflege? – Ja, aber...

... bitte nur freiwillig! Viele Hochschulen haben inzwischen ihr Interesse an den ehemaligen Studierenden, den sogenannten Alumni, entdeckt. Deren Daten sollen möglichst auf Dauer gespeichert, zu Kontaktzwecken sowie eventuell zu Befragungen genutzt und gegebenenfalls auch an private Alumni-Vereine weitergegeben werden.

Wie ein Erfahrungsaustausch mit dem Forum Alumni-Arbeit an Hochschulen zeigte, gibt es ganz unterschiedlich weitreichende Vorstellungen geplanter Datenverarbeitungsprozesse: Angefangen von Listen, in denen die Kontaktdaten erfasst werden, über interne Dateien, in denen die Angaben sowie zusätzliche Informationen verwaltet werden, bis hin zu Datenbanken, die ins Internet eingestellt werden sollen. Auch die Organisationsformen variieren: Zum Teil gibt es in Hochschulen integrierte Alumni-Stellen, die mithin regelmäßig öffentlich-rechtlich organisiert sind, und teilweise bilden sich außerhalb der Hochschulen Alumni-Vereinigungen, die – zumeist als eingetragene Vereine – privatrechtlich geführt werden.

Gemeinsam ist allen Projekten der Alumni-Arbeit, dass personenbezogene Daten verarbeitet werden, die ursprünglich zur Erfüllung festgelegter Aufgaben der Hochschulen erhoben und verarbeitet wurden. Daten müssen regelmäßig gelöscht werden, sobald sie zum ursprünglichen Zweck der Erhebung nicht mehr benötigt werden. Die Nutzung, Speicherung und Übermittlung der Daten für die Alumni-Kontaktpflege und damit die Verarbeitung zu einem neuen Zweck ist grundsätzlich nur mit wirksamer vorheriger Einwilligung der betroffenen Alumni zulässig. Nicht die Hochschulen und die Alumni-Vereine haben also darüber zu entscheiden, ob und inwieweit sie die Daten der ehemaligen Studierenden verarbeiten dürfen, sondern diese Entscheidung obliegt allein den Betroffenen selbst.

Wichtig ist, bereits die Kontaktaufnahme zu den Alumni datenschutzgerecht zu gestalten. Werbung für Alumni-Projekte etwa auf der Hochschul-Homepage, durch Aushänge, Informationsstände bei Hochschulveranstaltungen, Medienberichte, Zeitungsannoncen und dergleichen sind besonders datenschutzfreundliche Wege, den Kontakt zu interessierten Alumni herzustellen. Sollen ausscheidende Studierende gezielt angeschrieben werden, kann dies im Wege des Adressmittlerverfah-

rens geschehen: Die Alumni-Stelle oder der Alumni-Verein erstellt geeignete Informationsunterlagen und übergibt diese – etwa – dem Studierendensekretariat mit der Bitte, sie – beispielsweise zusammen mit der Exmatrikulationsbescheinigung – an die Betroffenen weiterzuleiten. Bei Interesse können sich letztere sodann unmittelbar an die Alumni-Stelle oder den Alumni-Verein wenden. Auf diese Weise gibt die verantwortliche Stelle weder intern noch extern Daten ohne Einwilligung der Betroffenen weiter. Dasselbe Verfahren kann grundsätzlich auch in Bezug auf früher ausgeschiedene Alumni praktiziert werden, soweit ihre Daten noch zulässigerweise in der Hochschule gespeichert sind. Ist der Kontakt hergestellt, können die Alumni im Weiteren darüber entscheiden, welche ihrer Daten in welchem Umfang und in welcher Weise von wem zum Zweck der Kontaktpflege verarbeitet werden dürfen, ob sie an Befragungen teilnehmen und ob sie beispielsweise einem Alumni-Verein beitreten wollen.

Hieran ändert auch die Neufassung des Hochschulgesetzes (HG NRW) grundsätzlich nichts. Dieses Gesetz sieht nunmehr vor, dass Alumni in den Grundordnungen der Hochschulen zu Hochschulangehörigen bestimmt werden können.

Sollte diese Regelung nach ihrem Wortlaut so verstanden werden, dass den Hochschulen nunmehr die Möglichkeit eröffnet wird, Daten der Alumni uneingeschränkt zu Zwecken der Kontaktpflege ohne deren Einwilligung – und dies sogar möglicherweise ihr Leben lang – zu nutzen, würde dies das Grundrecht der Betroffenen auf informationelle Selbstbestimmung unzulässig einschränken. Die Vorschrift muss deshalb verfassungskonform dahingehend ausgelegt werden, dass die Angaben der Alumni allenfalls für eine bestimmte Zeit zum Zweck der Kontaktaufnahme genutzt und gespeichert werden dürfen. In der Einschreibungsordnung sind Art und Umfang der zulässigen Datenverarbeitung verbindlich festzulegen. Im Übrigen kann eine Datenverarbeitung zum Zweck der Kontaktpflege auch weiterhin prinzipiell nur freiwillig und auf der Grundlage wirksamer Einwilligungen erfolgen.

Einer verfassungskonformen Auslegung der oben genannten Regelung des HG NRW bedarf es auch in Bezug auf die Teilnahme von Alumni an Evaluationsverfahren der Hochschulen. Bislang war eine solche Teilnahme freiwillig und nur mit wirksamer Einwilligung zulässig. Auch zukünftig können Alumni, die nach Maßgabe der gesetzlichen Neureglung zu Angehörigen der Hochschulen bestimmt werden, nicht

uneingeschränkt zur Teilnahme an den Befragungen verpflichtet werden. Ihre Daten dürfen auch zum Zweck der Evaluation nicht dauerhaft in den Hochschulen gespeichert und genutzt werden. Vielmehr bedarf es diesbezüglich konkreter Festlegungen in den jeweiligen Evaluationsordnungen der Hochschulen.

- Daten der Alumni dürfen zum Zweck der Kontaktpflege grundsätzlich nur verarbeitet werden, wenn und soweit die Betroffenen zuvor wirksam in diese Datenverarbeitung eingewilligt haben. Nur in engen Grenzen und nach Maßgabe konkreter Regelungen in den Ordnungen der Hochschulen kann eine Datenverarbeitung zum Zweck der Kontaktaufnahme und der Teilnahme an Bewertungsverfahren auch ohne eine solche Einwilligung zulässig sein.

6 Fußball-WM 2006

6.1 Fragwürdiges Akkreditierungsverfahren

Die Fußball-WM 2006 in Deutschland hat wegen ihrer spannenden Spiele und der großen Begeisterung in und außerhalb der Stadien viel Lob erfahren. Weniger gut fällt die Bilanz der Fußball-WM aus der Sicht des Datenschutzes aus. Insbesondere das Verfahren zur Überprüfung der vielen Helferinnen und Helfer geriet zu einem glatten Eigentor.

Rund 150.000 Menschen haben bei der Durchführung der Fußball-WM geholfen oder über das Medienereignis berichtet. Zu ihnen gehörten etwa die Ordnungs- und Sicherheitskräfte, das Reinigungs- und sonstige Servicepersonal, das Personal der vielen gastronomischen Betriebe in den Stadien genauso wie die vielen Journalistinnen und Journalisten. Sie alle mussten im Rahmen des Akkreditierungsverfahrens auch eine Überprüfung durch Polizei und Verfassungsschutz über sich ergehen lassen. Zu diesem Zweck wurden ihre Daten zunächst von ihren Arbeitgeberinnen und Arbeitgebern an das Organisationskomitee und von dort an das Bundeskriminalamt übermittelt. Das Bundeskriminalamt leitete die Daten sodann an die Bundespolizei und die für den Wohnort der betroffenen Person zuständige Landespolizei sowie an die Verfassungsschutzbehörden weiter. Dort wurden die Daten mit den vorhandenen Datenbeständen abgeglichen. Nach erfolgter Prüfung wurde dem Organisationskomitee auf dem gleichen Weg zu jeder betroffenen Person ein positives oder negatives Votum übermittelt. Bei einem negativen Votum hat das Organisationskomitee eine Akkreditierung abgelehnt. Zur Ablehnung führten beispielsweise frühere Verurteilungen wegen einer Straftat von erheblicher Bedeutung oder eine Erfassung in der Datei "Gewalttäter Sport". Auf diese Weise wurden von den Dienststellen der nordrhein-westfälischen Polizei insgesamt 28.222 Personen überprüft. In 291 Fällen hatte die Polizei Bedenken gegen eine Akkreditierung. In 186 Fällen erfolgte darüber hinaus eine Überprüfung durch den nordrhein-westfälischen Verfassungsschutz, die in 10 Fällen zu einer Ablehnung führte.

Das in dieser Größenordnung wohl einmalige Überprüfungsverfahren begründet nicht nur Zweifel an der Verhältnismäßigkeit, sondern leidet darüber hinaus an einer Reihe erheblicher Mängel. So existiert für eine

solche Zuverlässigkeitsüberprüfung im Rahmen einer privaten Sportveranstaltung keine Rechtsgrundlage. Die Betroffenen mussten sich deshalb zuvor gegenüber ihren Arbeitgeberinnen und Arbeitgebern oder dem Organisationskomitee mit ihrer Überprüfung durch Polizei und Verfassungsschutz ausdrücklich einverstanden erklären. Dies ist rechtlich eine zumindest fragwürdige Verfahrensweise. Fehlende gesetzliche Aufgabenzuweisungen für Polizei und Nachrichtendienste dürfen nicht einfach an den Parlamenten vorbei durch massenhafte Einwilligungserklärungen ersetzt werden. Dies gilt umso mehr, als ohne eine Einverständniserklärung eine Akkreditierung in jedem Falle abgelehnt wurde. In vielen Fällen sind deshalb erhebliche Zweifel an der erforderlichen Freiwilligkeit der Einwilligungserklärung angebracht. Aus verständlicher Sorge um den Arbeitsplatz wird kaum eine betroffene Person der Überprüfung nicht zugestimmt haben. Bedenken bestehen auch gegen die konkrete Verfahrensweise. Die Einwilligungserklärungen der Betroffenen verblieben bei den Arbeitgeberinnen und Arbeitgebern. Das weitere Verfahren wurde ausschließlich online abgewickelt. Veranstalter, Polizei und Verfassungsschutz mussten sich deshalb auf die lediglich "per Mausklick" übermittelte Mitteilung verlassen, dass eine wirksame Einwilligungserklärung vorliege. Insbesondere Polizei und Verfassungsschutz hatten deshalb keine Möglichkeit, die Authentizität der Einwilligungserklärungen selbst zu prüfen.

Erfreulich ist immerhin, dass zumindest in Nordrhein-Westfalen die Polizei durch das Innenministerium angewiesen war, den Betroffenen vor Abgabe eines negativen Votums noch einmal Gelegenheit zu einer Stellungnahme zu geben. Auf diese Weise wurden nach Angaben des Innenministeriums in 23 Fällen zunächst vorgesehene negative Voten noch einmal geändert und nach erneuter Prüfung keine Bedenken mehr gegen eine Akkreditierung geltend gemacht.

- Die rechtlich fragwürdige Mitwirkung von Polizei und Nachrichtendiensten an den Zuverlässigkeitsprüfungen eines privaten Veranstalters muss ein einmaliger Vorgang bleiben. Massenhafte Einwilligungserklärungen können fehlende gesetzliche Aufgabenzuweisungen und Befugnisse nicht am Grundrecht auf informationelle Selbstbestimmung vorbei ersetzen.

6.2 Gelbe Karte für Ticketingverfahren

Auch mit dem aufwendigen Vergabeverfahren für die Eintrittskarten zur Fußball-WM 2006 haben sich die Veranstalter ins datenschutzrechtliche Abseits gestellt.

Hier mussten die Interessentinnen und Interessenten bei der Bestellung ihre persönlichen Daten einschließlich ihrer Pass- oder Ausweisnummer angeben. Die Daten wurden sodann mit Hilfe von RFID-Chips auf den Eintrittskarten gespeichert, die jederzeit an den Stadieneingängen ausgelesen werden konnten. Nach der Berichterstattung in den Medien ist indes nur vereinzelt bei Eintritt in das jeweilige Stadion geprüft worden, ob die Besuchsperson auch tatsächlich identisch mit der betreffenden Erwerberin oder dem Erwerber der Eintrittskarte war. Der vorgebliche Sicherheitsgewinn durch die Erhebung und Speicherung der Daten der Käuferinnen und Käufer erscheint deshalb im Nachhinein mehr als fraglich. Die Datenschutzbeauftragten des Bundes und der Länder hatten sich bereits in ihrer Entschließung vom 10./11. März 2005 (abgedruckt im Anhang) gegen eine übermäßige Erhebung personenbezogener Daten im Rahmen der Ticketvergabe ausgesprochen.

➡ Die aufwendige und übermäßige Verarbeitung personenbezogener Daten anlässlich der Vergabe der Eintrittskarten für die Fußball-WM 2006 darf kein Vorbild für andere Großveranstaltungen werden. Es muss weiter möglich bleiben, Großveranstaltungen wie Fußballspiele ohne Identifizierungszwang zu besuchen.

7 Wirtschaft

7.1 Von der Black Box zum Score-Simulator

Das Thema "Credit Scoring" hat weiterhin Konjunktur. Score-Werte als Prognosen über das künftige Zahlungsverhalten bekommen für die Bürgerinnen und Bürger im Alltagsleben eine immer größere Bedeutung. Von den statistischen Schätzwerten, die ihnen zugeordnet werden, hängen Vertragsabschlüsse, Kredite und die Höhe der dafür zu zahlenden Zinsen ab. Gleichwohl geht die Geheimniskrämerei der Auskunfteien und Banken über die Bewertungsverfahren und die darin einfließenden Daten der Betroffenen weiter. Eine zentrale Forderung ist daher, mehr Transparenz zu schaffen. Die mühsam errungenen Rechte und Möglichkeiten der Betroffenen in den USA zeigen, wie die Unternehmen die hierzulande diskutierten Forderungen ohne Schwierigkeiten umsetzen können.

Was Score-Werte sind, wie sie berechnet werden und in welchen Bereichen sie zum Einsatz kommen, wurde bereits im Bericht 2005 unter 5.7 erläutert. Auch wurden Risiken unfairer und unseriöser Score-Verfahren dargestellt und drei wesentliche datenschutzrechtliche Anforderungen an Score-Verfahren zur Bonitätsbewertung skizziert.

Diese Forderungen und ihre Umsetzbarkeit sind Gegenstand der aktuellen Diskussionen um das Credit Scoring. Die Frage, welche datenschutzrechtlichen Anforderungen realisierbar sind, lässt sich mit einem Blick auf die Rechte und Möglichkeiten der Betroffenen im Mutterland des Credit Scoring, den USA, leichter beantworten.

Bis vor wenigen Jahren wurde das Credit Scoring auch in den USA gegenüber den Verbraucherinnen und Verbrauchern als Geschäftsgeheimnis (black box) behandelt. Das hat sich in den letzten Jahren gründlich geändert. In den USA, ansonsten kein Musterland des Datenschutzes, wurden einige datenschutzrechtliche Fortschritte für Betroffene des Credit Scoring erzielt:

Aufgrund eines Diskriminierungsverbotes dürfen Merkmale wie Herkunft, Religionszugehörigkeit, Geschlecht, Familienstand, Bezug öffentlicher Leistungen, Alter (letzteres mit Ausnahmen) nicht in die Entscheidung über einen Kredit und dessen Ausgestaltung einfließen. Sie

sind daher auch bei der Bewertung der Bonität als Score-Merkmale unzulässig.

Der Marktführer Fair Isaac, auf dessen Score-Modelle die Score-Berechnungen aller großen Auskunfteien in den USA basieren, verzichtet darüber hinaus ausdrücklich auch auf die Nutzung von Merkmalen wie Alter, Arbeitsstelle, Wohnumfeld, Unterhaltsverpflichtungen, Anfragen zu Kreditkonditionen sowie alle sonstigen Informationen, die nicht in der Bonitätsauskunft enthalten sind. In die Score-Berechnungen deutscher Unternehmen fließen diese Merkmale durchaus ein.

Aufgrund des Diskriminierungsverbots besteht auch die gesetzliche Pflicht, Kreditentscheidungen zum Nachteil der Betroffenen zu begründen. Unzulässig sind vage Begründungen ("zu niedriger Score-Wert"). Akzeptiert werden Gründe wie: "Ausschlaggebend war Ihr zu niedriges Einkommen". Eine Unterrichtungspflicht besteht nicht nur bei der Ablehnung eines Kredits, sondern auch dann, wenn die Höhe des Zinssatzes von den bei bester Bonität gewährten Konditionen abweicht.

Was sich Verbraucherinnen und Verbraucher in Deutschland wünschen und die hiesigen Auskunfteien und Banken gerne als unrealistisch bezeichnen, praktiziert der Marktführer für Score-Modelle in den USA: Fair Isaac veröffentlicht alle die in die Berechnung seines Score-Verfahrens einfließenden Merkmale und ihre ungefähre Wertigkeit. Die Merkmale und ihre prozentuale Gewichtung sind im Internet abrufbar.

Wegweisend für die deutsche Diskussion ist auch die umfassende Auskunftspflicht der Auskunfteien zum Credit Score. So sind unter anderem die vier für den individuellen Score-Wert bedeutsamsten Merkmale nach dem Grad des Einflusses aufzulisten. (Wird der konkrete Score durch das Merkmal "Zahl der Bonitätsauskünfte in jüngster Zeit" negativ beeinflusst, ist die betroffene Person auch dann darüber zu unterrichten, wenn es nicht zu den vier bedeutsamsten Merkmalen gehört.) Dieses um die den Score prägenden Merkmale erweiterte Auskunftsrecht gibt den Betroffenen die Chance, die wesentlichen Gründe für die Bonitätsprognose nachzuvollziehen. Das hat Modellcharakter für die Antwort auf die derzeit in Deutschland diskutierte Frage, wie transparent Score-Berechnungen für die Betroffenen sein können und müssen.

Ein in den USA eingehend erörtertes Thema ist die Qualität der Bonitätsinformationen, auf deren Grundlage die Scores berechnet werden.

Mehrere Studien ergaben, dass die in die Score-Berechnungen einfließenden Daten der Betroffenen häufig unrichtig oder unvollständig sind. Nach dem Motto "Stärkere Betroffenenrechte erhöhen die Score-Qualität" hat der dortige Gesetzgeber deswegen 2003 einen vereinfachten und kostenlosen Zugang der Betroffenen zu den über sie gespeicherten Bonitätsinformationen beschlossen. Damit soll die Qualität der Datenbasis für das Credit Scoring erhöht werden. Auch verstärkte Transparenz- und Prüfungspflichten der Unternehmen sowie verbraucherfreundlich ausgestaltete Gegendarstellungsrechte der Betroffenen dienen diesem Zweck.

Nicht nur Fair Isaac bietet – wie oben dargestellt – detaillierte Informationen über die in den Score einfließenden Merkmale und ihre Wertigkeit. Auch Auskunfteien und Finanzunternehmen vermarkten nun kundenorientiert individuelle Informationen und Serviceangebote rund um den Score. Selbst wenn der Nutzen einiger Angebote durchaus fraglich ist, zeigt sich in der Vermarktung von Beratungsleistungen doch ein Paradigmenwechsel zu einer stärkeren Orientierung an den Interessen der Betroffenen.

An einem Angebot der verantwortlichen Stellen wird der Wandel besonders deutlich: Fair Isaac und die drei führenden Auskunfteien bieten den Betroffenen die Möglichkeit, im Internet mit einem sogenannten Score-Simulator die Auswirkungen eines bestimmten Kredit- und Zahlungsverhaltens auf den Score zu testen. Der Score-Simulator zeigt den Betroffenen zwar nicht ihren genauen Score, vermittelt ihnen aber, welche Merkmale und Handlungen ihren Credit Score stark positiv oder negativ beeinflussen können. Die Score-Berechnung wird nachvollziehbarer und verliert den Charakter einer "black box". Das erhöht die Transparenz und damit auch das Verständnis für das Credit Scoring.

Um Missverständnisse zu vermeiden: Das Credit Scoring in den USA entspricht – trotz der mühsam errungenen Fortschritte – in vielen Aspekten weder den Wunschvorstellungen der dortigen noch denen der hiesigen Datenschützerinnen und Datenschützer. Es bleibt jedoch die Frage, weshalb die Auskunfteien und Banken hierzulande nicht wenigstens die technisch mögliche und in den USA teilweise realisierte Transparenz der Verfahren gewährleisten. Die Anforderungen an das Credit Scoring sollten in Deutschland nicht hinter die in den USA errungenen Standards zurückfallen.

➧ Die Aufsichtsbehörden in Deutschland haben auf Vorschlag der LDI NRW zur Transparenz von Scoring-Verfahren im Bereich der Kreditwirtschaft Folgendes beschlossen: Für die Betroffenen muss nachvollziehbar sein, welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen, welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt werden und welches die vier bedeutsamsten Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach dem Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden.

7.2 Bankübergreifende Warnmeldungen

Sogenannte Sicherheitsbeauftragte werten bei den Banken interne und externe Warnmeldungen zu Kundinnen und Kunden aus und informieren sich gegenseitig über tatsächlich oder vermeintlich auffälliges Kundenverhalten. Wie leicht es ist, in ihr Visier zu geraten, zeigt ein im Berichtszeitraum bekannt gewordener Fall.

Der Betroffene wurde verdächtigt, bei der Beantragung eines Kredites eine gefälschte Gehaltsabrechnung vorgelegt zu haben. Woraus sich dieser Verdacht konkret ergab, konnte im Nachhinein nicht mehr vollständig aufgeklärt werden. Die Bank vermutete jedoch, dass der Verdacht dadurch ausgelöst worden sei, dass die vorgelegte Gehaltsabrechnung mittels einer bestimmten, in jedem Computershop frei erhältlichen Computersoftware erstellt wurde, als Arbeitgeberin eine GmbH angegeben und auf der Abrechnung keine Versicherungsnummer verzeichnet war. Aufgrund der Summe dieser verschiedenen für sich gesehen völlig unverdächtigen Umstände sah sich der Sicherheitsbeauftragte der Bank veranlasst, an viele unterschiedliche auch in anderen Bundesländern ansässige Banken per E-Mail eine Warnmeldung zu verschicken, laut der der Betroffene versucht habe, sich unter Vorlage offensichtlich gefälschter Unterlagen einen Kredit zu erschleichen.

Bankübergreifende Warnmeldungen können für die Betroffenen weitreichende Folgen haben. Unabhängig von der erheblichen Rufschädi-

gung, die mit einer derartigen Warnmeldung in der Regel verbunden ist, kann es auch zu größerem finanziellen Schaden kommen, etwa wenn infolge einer derartigen Meldung ein Kreditgeschäft platzt. Im Berichtsfall hatte eine der die Meldung empfangenden Banken gegenüber einem Geschäftspartner des Betroffenen verlauten lassen, es lägen Erkenntnisse vor, die es als ratsam erscheinen ließen, mit dem Betroffenen besser keine Geschäfte mehr einzugehen.

Die Überprüfung des Falles ergab, dass die mit der Warnmeldung verbundene Übermittlung von personenbezogenen Daten an andere Kreditinstitute einen Verstoß gegen datenschutzrechtliche Bestimmungen darstellte. Es fehlte an einer Rechtsgrundlage, auf die sich die Bank diesbezüglich hätte stützen können. Der die Warnmeldung auslösende Verdacht war einerseits in keiner Weise erhärtet und konnte im Übrigen später noch nicht einmal mehr nachvollzogen werden. Unter diesen Umständen war der Betroffene durch die mit der Warnmeldung verbundene Übermittlung von Angaben zu seiner Person in nicht hinnehmbarer Weise in seinen schutzwürdigen Interessen verletzt.

Wenngleich – wie der Berichtsfall zeigt – bankenübergreifende Warnmeldungen die davon Betroffenen nur allzu leicht in ihren schutzwürdigen Interessen verletzen, können sie doch in Einzelfällen durchaus zulässig sein, wenn sich die Warnmeldung auf einen gerichtlich bestätigten Vorwurf wie etwa die rechtskräftige Verurteilung wegen Kreditbetruges bezieht. Über derartige Umstände dürfen sich die Banken auch untereinander informieren. Bevor eine Warnmeldung an andere Banken abgesetzt werden kann, muss jedoch grundsätzlich eine Interessenabwägung unter Berücksichtigung auch der Interessen der Betroffenen erfolgen. Das Ergebnis muss dokumentiert werden, damit nachvollziehbar bleibt, aus welchen Gründen der Vorwurf überhaupt bestand und warum die Bank es für erforderlich hielt, andere Institute zu warnen. Die ausgetauschten Angaben müssen sich auf Informationen zu Vermögens- und damit zusammenhängenden Delikten beschränken. Soweit lediglich der Verdacht einer Straftat besteht, muss dieser hinreichend erhärtet sein, um eine Warnmeldung rechtfertigen zu können. Dies wird in der Regel dann anzunehmen sein, wenn die die Warnmeldung veranlassende Bank zuvor auch eine Strafanzeige wegen der vermuteten Straftat bei der zuständigen Strafverfolgungsbehörde gestellt hat.

Neben dem beschriebenen direkten Austausch zwischen verschiedenen Banken existiert auf der Grundlage eines im Jahr 1980 zwischen den Banken und dem Bundeskriminalamt abgestimmten Verfahrens auch ein zentraler Informationsaustausch mit den Strafverfolgungsbehörden. Ziel ist unter anderem die Aufklärung von Wertpapierfälschungen, Betrugsfällen sowie anderen Vermögens- und Eigentumsdelikten von einer gewissen Erheblichkeit. Die von den Banken bestellten Sicherheitsbeauftragten werden dabei auf die Warn- und Suchmeldungen der Strafverfolgungsbehörden hin tätig. Das Verfahren wird zur Zeit überarbeitet. Dabei sind die oben skizzierten datenschutzrechtlichen Anforderungen zu beachten.

➧ Warnmeldungen zwischen Banken und anderen Stellen sind nur ausnahmsweise zulässig, wenn den schutzwürdigen Interessen der Betroffenen hinreichend Rechnung getragen ist. Insbesondere muss der den Meldungen zugrunde liegende Verdacht hinreichend erhärtet sein.

7.3 Versicherungen: Weiß es eine, wissen es alle

Die Versicherungen tauschen monatlich mit Hilfe sogenannter Hinweis- und Informationssysteme (HIS) umfangreiche Daten über mehrere Millionen Personen aus. Für die Betroffenen kann das gravierende Folgen haben. Dennoch werden sie oftmals weder über ihre konkrete Einmeldung in das System noch über die Gründe dafür unterrichtet. Auch fehlt es an einer wirksamen Rechtsgrundlage für den regen Datenaustausch.

Betroffen sind Versicherte, aber auch abgelehnte Antragstellende, gekündigte Versicherte und in einigen Sparten sogar Unfallgeschädigte, Zeuginnen und Zeugen sowie Sachverständige, die irgendeinen der größtenteils geheimen Einmeldegründe erfüllen. Zugriff auf die Informationen haben etwa 90% aller Versicherungen in Deutschland, ohne dass ein berechtigtes Interesse an den Daten und eine zweckgebundene Nutzung geprüft werden. Für die Betroffenen sind HIS eine undurchschaubare "black box", für die Versicherungen ein Datenpool, der weit über die von den Versicherungen hervorgehobene Betrugsprävention gewinnbringend genutzt werden kann.

Zweck des Datenaustausches ist neben der Betrugsprävention vor allem die Risikoprüfung bei Vertragsschluss. Die Versicherungen wollen sich vor "schlechten Risiken" schützen und als solche werten sie beispielsweise Personen, deren Verträge in der Vergangenheit von anderen Versicherungen gekündigt wurden. Die Betroffenen haben es dann oft schwer, eine andere Versicherung zu finden, die bereit ist, sie zu versichern. Häufig wird ihnen ein Vertragsschluss nur gegen einen erheblichen Risikoaufschlag angeboten.

In die HIS eingemeldet werden im Bereich der Rechtsschutzversicherungen unter anderem Versicherte, denen gekündigt wurde, weil sie dreimal in drei Jahren oder zweimal in zwölf Monaten angefragt haben, ob die Versicherung Kostendeckung für eine rechtliche Auseinandersetzung gewährt. Nach den Erfahrungen aus der Aufsichtspraxis spielt es häufig keine Rolle, ob die Versicherung tatsächlich in Anspruch genommen worden ist oder zahlen musste. Wer etwa mehrfach von streitfreudigen Menschen in Rechtsstreitigkeiten verwickelt wird und vorsichtshalber bei der für diesen Zweck abgeschlossenen und bezahlten Versicherung anfragt, findet sich also gegebenenfalls nicht nur ohne Rechtsschutzversicherung wieder, sondern wird auch bundesweit als "unrentables Risiko" gebrandmarkt.

Ähnliches gilt für Personen, die versuchen, eine Kranken- oder Berufsunfähigkeitsversicherung abzuschließen, und etwa wegen Vorerkrankungen abgelehnt oder nur gegen eine Risikoprämie versichert werden. Auch diese Personen sind anschließend allen anderen Kranken- oder Berufsunfähigkeitsversicherungen mit den entsprechenden Folgen als "schlechte Risiken" bekannt.

Im Bereich der Kfz-Versicherungen erfolgen die Einmeldungen anhand einer geheimen Liste von tatsächlichen oder vermeintlichen "Auffälligkeiten", beispielsweise im Zusammenhang mit einem Unfall oder einer Schadensregulierung. Die einzelnen Indizien für einen auffälligen oder betrügerischen Sachverhalt werden mit Punkten bewertet. Ab einer bestimmten Punktzahl erfolgt die Einmeldung in die HIS. Die nach diesem Scoring-Verfahren ermittelten Personen wissen gar nicht, dass sie von nun an bei allen Kfz-Versicherungen als Betrugsverdächtige gelten. Wie oben erwähnt, kommen selbst Zeuginnen und Zeugen, Geschädigte und Sachverständige allein aufgrund des geheimen Bewertungsverfahrens und vielfach wohl auch ohne objektiv erhärtete Ver-

dachtsmomente in die HIS. Mangels Transparenz haben sie keine Chance, den Verdacht mit einer Gegendarstellung zu entkräften.

Etwa alle drei Wochen erhalten die angeschlossenen Versicherungen über den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) den aktuellen Gesamtbestand aller eingemeldeten Daten zu mehreren Millionen Personen, unabhängig davon, ob die jeweilige Versicherung tatsächlich ein berechtigtes Interesse an den konkreten Informationen hat oder nicht. Es findet also eine datenschutzwidrige Vorratsdatenübermittlung statt. So sind auch Neugierabfragen und die Nutzung der Daten für Werbe- und Marketingzwecke nicht wirksam ausgeschlossen.

Die Versicherungen verweisen zur Rechtfertigung ihrer Praxis häufig auf die phonetische Codierung der Daten. Dadurch würden die Daten angeblich anonymisiert, so dass das Datenschutzrecht keine Anwendung finde. Tatsächlich jedoch haben alle beteiligten Versicherungen den Schlüssel und können etwa durch Eingabe eines Namens und des Ortes die Daten von der gewünschten wie auch von unbeteiligten Personen personenbeziehbar abrufen. Wer beispielsweise "Petra Meier" und "Dortmund" eingibt, erhält alle gleich lautenden eingemeldeten Namen (Petra Maier, Petra Mayer, Petra Meier, Petra Meyer) in Dortmund mit Anschriften, weiteren Informationen und gegebenenfalls auch den Einmeldegrund. Über die Anschrift oder das Geburtsdatum kann dann ohne großen Aufwand auf die gesuchte Person rückgeschlossen werden. Falls zusätzliche Informationen erforderlich sind, erleichtert eine angegebene Kontakttelefonnummer die Nachfrage bei der einmeldenden Versicherung.

Da es sich bei den in den HIS enthaltenen Daten um personenbezogene Daten handelt, benötigen die Versicherungen eine Rechtsgrundlage für das Einmelden oder Abrufen der Daten. Die Versicherungen berufen sich in diesem Zusammenhang auf eine Erklärung, die die Versicherten bei Vertragsschluss mit einer im Kleingedruckten der Versicherungsanträge enthaltenen Standarderklärung unterschrieben haben: "Ich willige ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/ Vertragsänderungen) ergeben, (...) sowie zur Beurteilung dieses Risikos und der Ansprüche an andere Versicherer (und/oder an den .... Verband zur Weitergabe dieser Daten an andere Versicherer) übermittelt. Die Einwilligung gilt

auch (unabhängig vom Zustandekommen des Vertrages) für entsprechende Prüfungen bei anderweitig beantragten (Versicherungs-) Verträgen und bei künftigen Anträgen."

Nur Eingeweihte dürften diese Erklärung in ihrer Tragweite und ihren Auswirkungen verstehen. Völlig unklar bleibt, unter welchen Umständen die Betroffenen damit rechnen müssen, von der Versicherung in die HIS eingemeldet zu werden. Auch das sogenannte "Merkblatt der Datenverarbeitung" der Versicherungen enthält nicht die Meldekriterien, die von den Versicherungen als streng geheim betrachtet werden. Im Übrigen wird das Merkblatt häufig nicht vor Vertragsschluss zur Verfügung gestellt, sondern erst mit der Übersendung des Versicherungsscheines. Zu diesem Zeitpunkt haben die ahnungslosen Versicherten die Erklärung jedoch schon längst unterschrieben.

Nach Auffassung der Aufsichtsbehörden des Bundes und der Länder ist die oben zitierte Erklärung keine hinreichende Rechtsgrundlage für die mit HIS verbundenen Datenverarbeitungen. Denn bereits aufgrund ihrer Unverständlichkeit genügt sie nicht den gesetzlichen Anforderungen an eine rechtswirksame Einwilligungserklärung. Auch verstößt sie gegen grundsätzliche Wertungen des Bundesdatenschutzgesetzes (BDSG) und ist daher als Bestandteil allgemeiner Geschäftsbedingungen unwirksam. Zudem haben gar nicht alle eingemeldeten Personen die Erklärung unterschrieben, wie etwa die Zeuginnen und Zeugen, Unfallgeschädigten und Sachverständigen im Kfz-Bereich.

Auch auf eine gesetzliche Rechtsgrundlage können sich die Versicherungen nicht stützen, da die schutzwürdigen Interessen der Betroffenen in der gegenwärtigen Einmeldepraxis nicht ausreichend berücksichtigt werden. Bei einer Vielzahl der bislang einer Einmeldung zugrunde gelegten Kriterien ist nämlich unklar, ob sie überhaupt eine Aussagekraft für das Vorliegen eines Falles von Versicherungsmissbrauch oder für ein erhöhtes Risiko besitzen. Wie oben dargestellt, werden Personen nicht nur aufgrund von sogenannten harten Negativmerkmalen, wie zum Beispiel einer rechtskräftigen Verurteilung wegen Versicherungsbetrugs, eingemeldet. Der gemeldete Verdachtsfall resultiert vielmehr aus einer Vielzahl für sich gesehen völlig unauffälliger Umstände, die erst in ihrer Summe von der einmeldenden Versicherung nach ihrem Ermessen so schwer gewichtet werden, dass eine Einmeldung erfolgt.

Eine Unterrichtung der Betroffenen über die beabsichtigte Einmeldung im Einzelfall erfolgt gegenwärtig nicht. Damit ist den Versicherten die Möglichkeit genommen, ihre gemäß § 6 BDSG unabdingbaren Rechte auf Auskunft und Berichtigung, auf Löschung und Sperrung geltend zu machen. Nicht zuletzt aus diesen Gründen sind die Betroffenen durch die Einmeldung und einen Abruf ihrer Daten aus HIS in unzumutbarer Weise in ihren schutzwürdigen Interessen verletzt. Die Datenverarbeitung im Zusammenhang mit HIS ist daher rechtswidrig. Zur Zeit verhandeln die Aufsichtsbehörden mit dem GDV über die Neufassung der in den Versicherungsanträgen enthaltenen standardisierten Einwilligungserklärung. Auch die HIS stehen dabei auf dem Prüfstand. Nach Auffassung der LDI NRW lassen sich diese nur nach einer grundlegenden Änderung der Struktur und des Verfahrens datenschutzgerecht gestalten.

- Die Einmeldung von Personen in die Hinweis- und Informationssysteme kann überhaupt nur dann zulässig sein, wenn den Betroffenen aussagekräftige Gründe für die Einmeldung zuvor im jeweiligen Einzelfall plausibel dargelegt worden sind, die Betroffenen Gelegenheit zur Stellungnahme hatten und die Versicherung die Angelegenheit auf ihre Einwände hin nochmals überprüft hat. Liegen sogenannte harte Negativdaten mit Bezug zum Versicherungsbetrug vor, ist es ausreichend, die Betroffenen über die Übermittlung an eine andere Versicherung zu unterrichten. Die Versicherungen dürfen nur Zugriff auf die Daten erhalten, für die sie im Einzelfall ein berechtigtes Interesse glaubhaft machen können. Um eine Kontrolle zu ermöglichen, ist jeder Zugriff einschließlich der dargelegten Gründe für das berechtigte Interesse zu dokumentieren.

7.4 Versicherungen fragen Zahlungsverhalten ab

Einige Versicherungen sind mittlerweile anscheinend dazu übergegangen, flächendeckend vor dem Abschluss eines Versicherungsvertrages oder im Rahmen der Schadensbearbeitung Bonitätsauskünfte zu den betroffenen Kundinnen und Kunden einzuholen. Dabei mag es eine Rolle spielen, dass die Auskunfteien gegenwärtig sehr offensiv ihre Geschäftsfelder um den Bereich der Versicherungen zu erweitern versuchen und

ihre Werbeaktivitäten in diesem Bereich signifikant verstärkt haben.

Versicherungen dürfen bei Abschluss eines Versicherungsvertrages nur in Ausnahmefällen Informationen über die potentiellen Versicherungsnehmerinnen und Versicherungsnehmer einholen (siehe Bericht 2005 unter 5.5). Nach dem Gesetz müssen sie dafür zunächst im konkreten Einzelfall ein berechtigtes Interesse an der Kenntnis der Bonitätsdaten glaubhaft dargelegt haben, und es darf kein Grund zu der Annahme bestehen, dass die Antragstellenden ein schutzwürdiges Interesse daran haben, dass Bonitätsauskünfte durch Auskunfteien zu ihrer Person an die Versicherung unterbleiben. Ein berechtigtes Interesse haben die Versicherungen dabei nur dann, wenn ihnen aus dem Geschäft ein erhebliches Ausfallrisiko entstehen kann. In diesem Zusammenhang wird von den Versicherungen häufig die Auffassung vertreten, dass bereits das Risiko, dass die Versicherungsnehmerinnen und Versicherungsnehmer ihren vertraglichen Zahlungspflichten nicht beziehungsweise nicht rechtzeitig nachkommen oder angefallene Mahn- und Verzugskosten nicht realisiert werden können, die Versicherungen berechtige, Bonitätsabfragen einzuholen. Dabei sollte jedoch berücksichtigt werden, dass gerade die Versicherungen durch die für sie sehr günstigen Regelungen des Versicherungsvertragsgesetzes (VVG) im Verhältnis zu anderen Wirtschaftsbereichen deutlich im Vorteil sind. So wird die Versicherung zum Beispiel von ihrer Leistungsverpflichtung frei, wenn die erste oder einmalige Versicherungsprämie zur Zeit des Eintritts des Versicherungsfalls noch nicht gezahlt ist. Sie kann außerdem im Leistungsfall den Beitrag einer fälligen Prämienforderung oder einer anderen ihr aus dem Vertrag zustehenden Forderung von der von ihr zu leistenden Zahlung in Abzug bringen. Das erforderliche erhebliche Ausfallrisiko wird von der LDI NRW daher bislang lediglich in den folgenden Fällen anerkannt:

- Abschluss einer Kreditversicherung
- Abschluss einer Kfz-Versicherung mit einer vorläufigen Deckungszusage
- Einräumung eines Hypothekendarlehens im Rahmen der Kreditvergabe durch Versicherungen
- Vermietungen von Immobilien durch Versicherungen

- Konkreter Betrugsverdacht im Einzelfall

Die genannten Fallgruppen sind abschließend. Rückschlüsse auf andere Konstellationen sind nicht ohne weiteres möglich. Insbesondere können die im Hinblick auf die Kfz-Haftpflichtversicherung mit vorläufiger Deckungszusage entwickelten Grundsätze nicht auf andere Versicherungstypen übertragen werden. Im Berichtszeitraum war beispielsweise der Fall einer Versicherung zu entscheiden, die bei Abschluss einer Hausratsversicherung eine vorläufige Deckungszusage erteilt hatte. Wie bei jedem anderen Versicherungsvertrag mit vorläufiger Deckungszusage bestand auch hier für die Versicherung die Gefahr, zur Schadensregulierung verpflichtet zu sein, obwohl die Prämie gar nicht oder erst verspätet gezahlt wurde. Die Versicherung hatte sich deswegen vor Vertragsschluss durch die Einholung einer Bonitätsauskunft vergewissern wollen, nicht an zahlungsschwache oder zahlungsunwillige Vertragspartnerinnen und Vertragspartner zu geraten. Dabei wurde jedoch nicht berücksichtigt, dass sie bei einem Ausbleiben der Prämienzahlung gemäß § 35b VVG die von ihr aufzuwendenden Kosten der Schadensregulierung mit der ausgefallenen Prämienforderung hätte aufrechnen, das heißt ihre Zahlung um die Höhe der noch offenen Prämie hätte kürzen können. Ihr wären im Ergebnis dann nicht mehr Kosten entstanden, als ihr auch bei vertragsgemäßer Zahlung der Prämie entstanden wären. Eine solche Aufrechnung wäre selbst dann möglich gewesen, wenn die Versicherung die Zahlung nicht an ihre Versicherungsnehmerin oder ihren Versicherungsnehmer selbst, sondern an einen geschädigten Dritten hätte leisten müssen. Ein erhebliches Ausfallrisiko, welches zur Einholung einer Bonitätsauskunft berechtigt hätte, lag daher nicht vor. Die Einholung der Bonitätsauskunft wurde dementsprechend als datenschutzwidrig beanstandet.

Im Unterschied zu der beschriebenen Situation gibt es bei der vorläufigen Deckung in der Kfz-Haftpflichtversicherung ebenso wie bei anderen Pflichtversicherungen zumindest gegenüber geschädigten Dritten keine Möglichkeit der Aufrechnung. Die Kfz-Haftpflichtversicherung hat also gegenüber Dritten, denen sie zur Leistung aus dem Haftpflichtfall verpflichtet ist, nicht das Recht, eine noch offene Prämienforderung in Abzug zu bringen. Es besteht daher für sie bei der Inanspruchnahme durch einen geschädigten Dritten das Risiko, dass ihre Versicherungsnehmerin oder ihr Versicherungsnehmer die Prämie

nicht zahlt, sie dem Dritten gegenüber aber voll zur Zahlung verpflichtet ist. Aus diesem Grund ist die Einholung von Bonitätsauskünften vor dem Abschluss von Pflichtversicherungen mit vorläufiger Deckungszusage, wie zum Beispiel der Kfz-Haftpflichtversicherung, zulässig.

Auch die im Bericht 2005 unter 5.5 gebildete Fallgruppe des "konkreten Betrugsverdacht im Einzelfall" bedarf der einschränkenden Erläuterung. Der damals gebildeten Fallgruppe lag die folgende Konstellation zugrunde: Ein Versicherungsmakler hatte einer Kundin, mit der er auch persönlich verbunden war, eine Lebensversicherung zu vermitteln versucht. Beiden war klar, dass sich die Antragstellerin die sehr hohen Beitragsraten nicht würde leisten können. Es gab konkrete Anhaltspunkte dafür, dass es dem Versicherungsmakler lediglich darum ging, die sehr hohe Provisionszahlung für den Vertragsabschluss von der Versicherung zu erhalten. Die in dieser Situation berechtigte Bonitätsauskunft ergab, dass die Antragstellerin wegen Zahlungsunfähigkeit bereits eine Versicherung an Eides statt abgegeben hatte. Gibt es bei Vertragsschluss hinreichend sicherere Anzeichen dafür, dass der Vertrag in betrügerischer Absicht geschlossen werden soll, so dürfen Versicherungen Bonitätsauskünfte einholen.

Dagegen bestehen generell Bedenken dagegen, dass Versicherungen auch bei der Schadensbearbeitung zur Erhärtung eines nur unbestimmten Betrugsverdachts eine Bonitätsauskunft einholen. In einem ebenfalls im Berichtszeitraum bekannt gewordenen Fall hatte eine Versicherung über die Regulierung eines Schadens an einem von ihrer Versicherungsnehmerin beschädigten Auto zu entscheiden. Dabei ergaben sich Zweifel hinsichtlich des Bestehens der Leistungspflicht, da die Versicherungsnehmerin in ihrer Schadensschilderung angegeben hatte, dass der Unfallgeschädigte sie abgedrängt und auf diese Weise den Unfall provoziert hätte. Warum aber die Versicherung zur weiteren Klärung auf eine Bonitätsauskunft zurückgriff, die ihr im Übrigen auch keine zusätzlichen Erkenntnisse verschaffte, blieb unklar. Fragen bezüglich des Tatherganges und der Unfallverursachung kann eine Versicherung nur über den üblichen Weg der Einschaltung von Schadenssachverständigen aufklären, nicht aber durch eine Bonitätsauskunft. Die Einholung von Auskunfteidaten war daher in dieser Situation unzulässig.

Zunehmend preisen Auskunfteien den Versicherungen ihre Bonitätsinformationen mit dem Argument an, dass zwischen einer schlechten Bonität und einem erhöhten Schadensrisiko ein statistischer Zusammenhang bestünde. Mit der Erhebung von Bonitätsauskünften vor Vertragsschluss könnten die Versicherungen daher das durchschnittliche Risiko reduzieren, später für die gezahlten Prämien stark in Anspruch genommen zu werden. Bislang gibt es indes nur Auftragsgutachten der Auskunfteien und keinen Nachweis durch eine unabhängige Stelle für eine sogenannte statistische Signifikanz zwischen dem allgemeinen Zahlungsverhalten und der Inanspruchnahme einer konkreten Versicherung.

Entscheidend ist jedoch, dass die Einholung von Bonitätsdaten durch die Versicherungen für diesen Zweck selbst dann unzulässig wäre, wenn ein solcher statistischer Zusammenhang belegt würde. Die Versicherungen würden sich in diesem Fall nämlich nicht vor finanziellen Ausfallrisiken oder Vertragsverletzungen schützen wollen, sondern vor einer vertragsgemäßen Inanspruchnahme der von ihnen zu erbringenden Leistung. Die Erhebung von Bonitätsinformationen durch Versicherungen ohne bestehendes Bonitätsrisiko verletzt die schutzwürdigen Interessen der betroffenen Antragstellerinnen und Antragsteller.

Zu dem Gesamtkomplex der Bonitätsabfragen durch Versicherungen hat die LDI NRW in Abstimmung mit den übrigen Aufsichtsbehörden den Gesamtverband der Deutschen Versicherungswirtschaft (GDV), in dem alle großen Versicherungsunternehmen Mitglieder sind, um Stellungnahme gebeten. Durch die Einschaltung des Verbandes soll eine bundesweit einheitliche Praxis bei den Versicherungen erreicht werden. Zur Zeit bestehen innerhalb der Versicherungswirtschaft Bestrebungen, die Kundinnen und Kunden – ähnlich wie dies auch die Banken mit der SCHUFA-Klausel tun – in die mit den Bonitätsauskünften verbundene Verwendung ihrer Angaben einwilligen zu lassen. Eine Klausel im Kleingedruckten vermag dagegen nach Auffassung der LDI NRW die Einholung von Bonitätsauskünften nicht zu rechtfertigen. Anders als die Banken trifft die Versicherungen in der Regel bei einem in Aussicht genommenen Vertragsschluss kein erhebliches finanzielles Ausfallrisiko. Eine pauschale Einwilligung in Bonitätsauskünfte wäre aus Sicht der Antragstellenden eine überraschende Klausel und würde außerdem den wesentlichen Grundgedanken des Bundesdatenschutz-

gesetzes zuwiderlaufen. Sie wäre aus diesen Gründen zivilrechtlich unzulässig und daher als Rechtsgrundlage hinfällig.

- Versicherungen dürfen keineswegs pauschal bei Abschluss von Versicherungsverträgen oder im Rahmen der Schadensbearbeitung Bonitätsauskünfte zu den Betroffenen einholen. Eine Berechtigung besteht nur in Ausnahmefällen, in denen der Versicherung ein erhebliches finanzielles Ausfallrisiko aus dem Geschäft entstehen kann.

7.5 Was nicht im Katalog steht: Einmal bestellt, auf Dauer durchleuchtet

Nicht nur die Kataloge des Versandhandels, sondern auch die häufig heimlichen oder im Kleingedruckten verklausulierten Datentransfers zwischen Versandhandel und Auskunfteien bieten die eine oder andere Überraschung. Selbst die sekundenschnelle Bestellung im Internet kann mitunter jahrelange ungewollte Nach- und Nebenwirkungen haben, wie die folgenden Fälle zeigen, in denen Auskunfteien und Versandhandel unabhängig von einzelnen Bestellvorgängen Bonitätsdaten austauschen.

Versandhandelsunternehmen dürfen bei Auskunfteien Informationen über die Kreditwürdigkeit der Kaufinteressierten einholen, wenn sie im konkreten Einzelfall ein finanzielles Ausfallrisiko haben, etwa bei Zahlung auf Rechnung, und die Betroffenen vorab über die Bonitätsabfrage unterrichten. Doch leider beschränkt sich der Datenaustausch zwischen Auskunfteien und dem Versandhandel in einigen Fällen nicht auf diese einmalige Abfrage bei Vertragsschluss.

So informiert die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) die Versandhandelsfirmen auch noch Jahre nach Abschluss des Bestellvorgangs über neue oder aktualisierte SCHUFA-Einträge und Adressänderungen früherer Kaufinteressierter. Dabei haben die Firmen weder ein berechtigtes Interesse im Sinne des Bundesdatenschutzgesetzes an diesen Daten noch eine laufende Vertragsbeziehung mit den betroffenen Personen. Das Vertragsverhältnis ist mit Lieferung und Zahlung bereits beendet und ein die Bonitätsauskunft rechtfertigendes finanzielles Ausfallrisiko somit ausgeschlossen.

SCHUFA und Versandhandel begründen ihren regen Datenaustausch damit, dass die meisten Personen nicht nur einmal, sondern immer wieder Waren bei demselben Unternehmen bestellen. Damit die Firmen nicht bei jeder Bestellung eine erneute Anfrage bei der SCHUFA stellen müssten, melde die SCHUFA ihnen automatisch alle neuen Daten – unabhängig davon, ob eine neue Bestellung vorliegt oder nicht.

Um diese sogenannten Nachmeldungen zu erhalten, melden die Versandhandelsunternehmen der SCHUFA, dass sie für die bestellende Person ein Kundenkonto ("Versandhauskonto") eingerichtet hätten. Oft erfahren die Betroffenen dies erst nach Einsicht ihrer bei der SCHUFA gespeicherten Daten und sind von dem Eintrag eines solchen "Kontos" bei der SCHUFA vollkommen überrascht. Dabei führt der Eintrag des Merkmals "Versandhauskonto" nicht nur zu der geschilderten rechtswidrigen Datenübermittlung und -speicherung, sondern fließt auch in die Berechnung des sogenannten SCHUFA-Scores ein (siehe hierzu Bericht 2005 unter 5.7).

Auch andere Auskunfteien bieten Versandhandelsunternehmen einen vergleichbaren Service an, der sich zwar an den Interessen des Versandhandels und der Auskunfteien, nicht aber am Datenschutz orientiert. Der Service sieht wie folgt aus: Das Unternehmen übermittelt einmal oder mehrmals im Jahr seine Kundendatei an die Auskunftei. Die Kundendatei enthält Neukundinnen und -kunden, aber auch sogenannte Bestandskundinnen und -kunden, bei denen der Bestellvorgang einschließlich der Zahlung bereits beendet ist. Die Auskunftei gleicht nun die Kundendatei mit den Auskunfteidaten ab und teilt dem Versandhandelsunternehmen mit, über welche Kundinnen und Kunden negative Einträge vorliegen. Der Abgleich ist unzulässig, soweit das Unternehmen zu dem Zeitpunkt kein finanzielles Ausfallrisiko im Verhältnis zu den Betroffenen trägt. Gegen ein Versandhandelsunternehmen in Nordrhein-Westfalen wurde daher ein Bußgeldverfahren eingeleitet. Da die geschilderten unberechtigten Datentransfers zwischen Auskunfteien und Versandhandelsunternehmen bundesweit zu beobachten sind, wird die LDI NRW sich darüber hinaus um abgestimmte Aufsichtsmaßnahmen aller Aufsichtsbehörden bemühen.

- Versandhandelsunternehmen müssen die Daten ihrer Kundinnen und Kunden nach Abwicklung des Vertrags löschen oder sperren. Unabhängig davon dürfen sie von der SCHUFA oder anderen Auskunfteien nur dann

Bonitätsdaten erheben, wenn sie aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko haben.

7.6 Bonitätsauskünfte über Mietinteressierte

Um sich vor zahlungsunfähigen oder zahlungsunwilligen Mieterinnen und Mietern oder gar vor "Mietnomaden" zu schützen, möchten Vermieterinnen und Vermieter vor Eingehung eines Mietvertrages die finanzielle Situation der potentiellen Mietpartei überprüfen. Dazu bedienen sie sich der Bonitätsinformationen, die sie bei herkömmlichen Auskunfteien oder speziellen Warndateien im Wohnungswesen über die Betroffenen einholen können.

Die Zulässigkeit der Erteilung von Auskünften über Mietinteressierte durch Auskunfteien und Warndateien im Wohnungswesen an Vermieterinnen und Vermieter vor Eingehung eines Mietvertrages richtet sich nach § 29 Bundesdatenschutzgesetz (BDSG).

Auf eine Einwilligung der am Mietverhältnis interessierten Personen als Rechtsgrundlage für die Erhebung von Bonitätsdaten können sich die Vermieterinnen und Vermieter grundsätzlich nicht stützen. Denn eine Einwilligung ist nur wirksam, wenn sie freiwillig erteilt wird. Bei Anbahnung eines Mietverhältnisses müssen die Mietinteressierten in der Regel befürchten, dass die Verweigerung der Einwilligung in die Datenerhebung zum Rückschluss führt, sie hätten etwas zu verbergen. Um diesen Anschein zu vermeiden, werden sich Mietinteressierte je nach Lage des Wohnungsmarktes und ihrer persönlichen Verhältnisse gezwungen sehen, die Einwilligung zu erteilen, um ihre Chance auf den gewünschten Mietvertrag zu wahren. Mangels Freiwilligkeit kommt daher eine Einwilligung als Rechtsgrundlage für die Erhebung von Bonitätsdaten nicht in Betracht. Deshalb dürfen auch keine sogenannten Score-Werte an Vermieterinnen und Vermieter übermittelt werden. Denn deren Übermittlung kann nicht auf eine gesetzliche Grundlage (§ 29 BDSG), sondern nur auf eine wirksame Einwilligung der Betroffenen gestützt werden.

Hinsichtlich der Prüfung, in welchem Umfang nach § 29 BDSG Daten über Mietinteressierte übermittelt werden dürfen, hat der Düsseldorfer Kreis als Gremium der obersten Aufsichtsbehörden im Datenschutz für

den nicht-öffentlichen Bereich zuletzt 2004 beschlossen, dass im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung die schutzwürdigen Belange der Mietinteressierten in besonderer Weise zu berücksichtigen sind. Daher sind Auskunftssysteme vorzuziehen, die auf mietrelevante Daten beschränkt sind, und deren Daten gesicherte Rückschlüsse auf Mietausfallrisiken zulassen. Uneingeschränkte Auskünfte über Mietinteressierte durch Auskunfteien, die branchenübergreifende Daten übermitteln, sind nach Auffassung der Aufsichtsbehörden dagegen unzulässig.

Die Weitergabe von Negativeintragungen durch Auskunfteien und Warndienste über Mietinteressierte ist daher nur eingeschränkt zulässig. Dies berücksichtigt, dass die Anmietung einer Wohnung für die Betroffenen eine existentielle Bedeutung hat. Ein in den verschiedenen Lebensbereichen unterschiedlich ausgeprägtes Zahlungsverhalten der Betroffenen lässt noch keine Aussage darüber zu, ob die jeweilige Person im Einzelfall künftig ihre Miete zahlen wird oder kann. Nicht bezahlte Telefon- oder Versandhandelsrechnungen bedeuten nicht, dass die betroffene Person ihr Mietverhältnis durch Nichtzahlung der Miete gefährden wird.

Bei der im Rahmen der Datenübermittlung gebotenen Abwägung der berechtigten Interessen der Vermieterinnen und Vermieter mit den schutzwürdigen Belangen der Mietinteressierten ist ferner zu berücksichtigen, dass Vermieterparteien im Vergleich zu anderen Gläubigerinnen und Gläubigern folgende Sicherheiten und Vorteile genießen: Mietkaution, Vermieterpfandrecht und in die Zahlungspflicht eintretende Sozialbehörden, die in vielen Fällen auch nachträglich für zahlungsunfähige Mieterinnen und Mieter die Mietzahlung zur Vermeidung von Obdachlosigkeit übernehmen.

Aus diesen Gründen dürfen Auskunfteien und Warndienste im Wohnungswesen an Vermieterinnen und Vermieter über Mietinteressierte nur solche Daten übermitteln, die durch eine rechtliche Titulierung und damit im Wege eines rechtsförmigen Verfahrens gesichert sind und zugleich eine Aussage über das zu erwartende Vertragsverhalten als Mietpartei treffen. Insoweit kommen nur Urteile und Vollstreckungsbescheide mit mietrechtsrelevantem Inhalt in Betracht. Mietferne Daten, wie Negativeintragungen zu Forderungen aus Handel und Dienstleistung, sind für Vermieterinnen und Vermieter nur bonitätsrelevant,

wenn es sich um Einträge aus dem öffentlichen Schuldnerverzeichnis handelt.

Unter Einhaltung dieser Rahmenbedingungen dürfen zur Bewertung der Bonität von Mietinteressierten nur folgende Daten übermittelt werden:

1. Personalien der Mietpartei (um Identitätsverwechslungen zu vermeiden): Name, Vorname, Geburtsdatum, Geburtsname, Geburtsort, Anschrift des vorherigen Wohnsitzes
2. Folgende Negativmerkmale:
   - Rechtskräftige Urteile zur fristlosen Kündigung wegen vertragswidrigen Verhaltens der Mietpartei gemäß §§ 543, 569 Bürgerliches Gesetzbuch (ausgenommen Fälle, in denen vor der Kündigung wegen Zahlungsverzugs Mietminderung geltend gemacht wurde)
   - Rechtskräftige Räumungsurteile nach fristloser Kündigung wegen vertragswidrigen Verhaltens der Mietpartei (ausgenommen Fälle, in denen vor Kündigung wegen Zahlungsverzugs Mietminderung geltend gemacht wurde)
   - Vollstreckungsbescheide wegen Rückständen der Mietzahlung in Höhe von mindestens zwei Monatsmieten einschließlich Nebenkosten (ausgenommen Fälle, in denen Mietminderung gelten gemacht wurde)
   - Bescheinigungen der Gerichtsvollzieher über die fruchtlose Pfändung einer titulierten Forderung aus einem Mietverhältnis
   - Abgabe der eidesstattlichen Versicherung und Haftbefehle (Daten aus öffentlichen Schuldnerverzeichnissen)

Vor diesem Hintergrund ist auch die Einmeldung von Mahnbescheiden wegen Mietforderungen mit den genannten Kriterien nicht zu vereinbaren. Die Einmeldung eines Negativeintrags über Mietschulden bedarf mindestens eines rechtskräftigen Vollstreckungsbescheides.

Darüber hinaus ist die Einmeldung von Daten über "Mietnomaden" unter Einhaltung bestimmter Anforderungen zulässig. Eine zulässige Einmeldung erfordert, dass die betroffene Person von den ersten drei Monatsmieten zwei nicht gezahlt hat. Ausgenommen sind auch hier

Fälle, in denen die Mietpartei Mietminderung oder andere zur Nichtzahlung berechtigende Einreden geltend macht. Darüber hinaus muss die geschädigte Mietpartei bei der Strafverfolgungsbehörde einen Strafantrag wegen Eingehungsbetruges gestellt haben. Sollte das eingeleitete Strafverfahren zu einem späteren Zeitpunkt eingestellt werden, ist der erfolgte Eintrag in der Auskunftei oder Warndatei umgehend zu löschen.

Diese Auskünfte dürfen Auskunfteien und Warndienste gemäß § 29 Abs. 2 BDSG nur dann an potentielle Vermieterinnen und Vermieter erteilen, wenn diese ein berechtigtes Interesse an den Informationen glaubhaft dargelegt haben. Ein berechtigtes Interesse besteht nur, soweit der Abschluss eines Mietvertrages unmittelbar bevorsteht und dabei die Vermieterpartei bei Vertragsschluss ein wirtschaftliches Ausfallrisiko hat. So besteht beispielsweise kein Ausfallrisiko und damit kein berechtigtes Interesse an einer Auskunft, wenn eine Sozialbehörde die Mietzahlung übernimmt. Die persönliche wirtschaftliche Situation der Mietpartei ist insoweit schon nicht mehr relevant.

Anfragende Vermieterinnen und Vermieter haben die Mietinteressierten gemäß § 4 Abs. 3 BDSG bereits bei der Erhebung der für die Bonitätsanfrage erforderlichen Identitätsdaten über den Zweck der Erhebung (Risikoprüfung) und die Empfängerinnen und Empfänger der Daten (die jeweilige Auskunftei oder Warndatei) zu informieren. Die Auskunfteien und Warndateien wiederum sind den Betroffenen gegenüber gemäß § 34 BDSG zur Auskunft verpflichtet und unterliegen den gesetzlichen Berichtigungs-, Löschungs- und Sperrungspflichten.

- Nur titulierte Negativmerkmale, die aus öffentlichen Schuldnerverzeichnissen stammen oder mietrechtlichen Bezug aufweisen, dürfen neben bestimmten Informationen zu "Mietnomaden" unter Einhaltung der genannten Anforderungen übermittelt werden. An jede Auskunftei oder Warndatei sind aufgrund des Gleichbehandlungsgrundsatzes identische Anforderungen zu stellen.

7.7 Datenschutz angemahnt? – Datenschutzfragen rund ums Inkasso

Eine nicht bezahlte Rechnung kann für Schuldnerinnen und Schuldner unangenehme Folgen nach sich ziehen. Spätestens mit Einschaltung eines Inkassounternehmens, durch das die Gläubigerinnen und Gläubiger die ausstehende Forderung mit Nachdruck eintreiben möchten, erinnert sich manche Person an die zuletzt vergessene Telefonrechnung oder die achtlos entsorgte Mahnung vom Versandhandel. Die Betroffenen stellen sich immer wieder die Frage, ob und welche Daten das Inkassounternehmen überhaupt speichern darf. Insbesondere fürchten sie wirtschaftliche Nachteile durch die dortige Speicherung und Verarbeitung von Negativdaten zu ihrem Zahlungsverhalten.

Häufig bedienen sich Unternehmen in den Fällen, in denen ihre ausstehenden Forderungen nicht bezahlt werden, der Dienste von Inkassobüros. Inkassobüros sind Dienstleistungsunternehmen, die sich gewerbsmäßig mit der Einziehung von Forderungen befassen. Handelt es sich um Forderungen, die von den ursprünglichen Gläubigerinnen und Gläubigern an das Inkassobüro zur weiteren Einziehung abgetreten sind, können die Inkassobüros die Forderungen im eigenen Namen geltend machen. In den übrigen Fällen betreibt das Inkassobüro die Forderungseinziehung im Namen der auftraggebenden Gläubigerinnen und Gläubiger. Beide Fälle setzen die Weitergabe der Schuldnerdaten an das Inkassobüro voraus, die für die Geltendmachung der Forderung erforderlich sind.

Wenn das Inkassobüro eine an sie abgetretene Forderung im eigenen Namen geltend macht, hat das Inkassobüro diese zuvor von der ursprünglichen Gläubigerpartei, beispielsweise einem Telekommunikationsunternehmen oder einem Onlineshop, erworben. Das Inkassobüro ist damit anstelle der ursprünglichen Vertragspartei neuer Gläubiger der betroffenen Person geworden. An den Erwerb der Forderung ist untrennbar auch die Übermittlung der Schuldnerdaten geknüpft, ohne die das Inkassobüro keine Forderungseinziehung vornehmen kann. Die übergegangene Forderung berechtigt das Inkassobüro zur Erhebung und Verarbeitung der Schuldnerdaten, die regelmäßig Angaben zu Name und Anschrift der Schuldnerpartei sowie zur Forderungshöhe und zu ursprünglichen, der Forderung zugrunde liegenden Vertrags-

daten umfassen. Die insoweit relevante Datenerhebung und Datenverarbeitung beim Inkassobüro ist als Mittel für die Forderungseinziehung zulässig und dient der Zweckbestimmung des Vertragsverhältnisses mit der betroffenen Person.

Soll die Forderung in fremdem Namen eingezogen werden, so geht der Forderungseinziehung durch das Inkassounternehmen eine Datenübermittlung der Gläubigerpartei an das Inkassobüro voraus. Diese Datenübermittlung ist regelmäßig zulässig, da die Forderungseinziehung durch ein Inkassounternehmen der Wahrung berechtigter Interessen der Gläubigerpartei dient. Jedes Unternehmen und jede Privatperson muss grundsätzlich das Recht haben, bestehende Forderungen, die die Schuldnerpartei nicht begleicht, mit Hilfe eines Inkassounternehmens einziehen zu lassen.

Die betroffenen Schuldnerinnen und Schuldner können gegenüber den Inkassounternehmen von ihren gesetzlichen Betroffenenrechten Gebrauch machen. Sie können ihr Auskunftsrecht nach § 34 Bundesdatenschutzgesetz (BDSG) wahrnehmen und erfahren, welche Daten das Inkassobüro zu ihrer Person gespeichert hat. Das dürfte grundsätzlich relevant sein, wenn die Betroffenen sich einer Forderung gegenüber sehen, die sie nicht zuordnen können oder für unberechtigt halten. Diese Auskunft ist den Betroffenen kostenlos zu erteilen.

Darüber hinaus kann den Betroffenen nach § 35 BDSG im Einzelfall ein Anspruch auf Berichtigung, Sperrung oder Löschung der zu ihrer Person gespeicherten Daten zustehen:

- Die Daten sind zu berichtigen, wenn unrichtige Angaben zur betroffenen Person oder hinsichtlich der ausstehenden Forderung gespeichert sind, insbesondere wenn die Forderung bereits ausgeglichen wurde und so erledigt ist.

- Die Daten sind zu löschen, wenn ihre Speicherung unzulässig ist. Davon ist regelmäßig auszugehen, wenn es sich bei der in Anspruch genommenen Person aufgrund einer Identitätsverwechslung nicht um die richtigen Forderungsgegnerinnen oder -gegner handelt.

- Die Daten sind zu sperren, sobald die Schuldnerpartei die Forderung dem Grunde oder der Höhe nach bestritten hat.

Häufig arbeiten Inkassounternehmen mit Auskunfteien zusammen – teilweise sogar als zwei Geschäftsbereiche unter einem Unternehmensdach – und stellen diesen Negativinformationen über das Zahlungsverhalten der Betroffenen zur weiteren Auskunftserteilung zur Verfügung. Diese Übermittlung beziehungsweise Nutzung der Daten für Auskunfteizwecke ist nur zulässig, wenn die Negativdaten aus dem Inkassobereich gesichert einen Rückschluss auf die Zahlungsunfähigkeit oder Zahlungsunwilligkeit der betroffenen Schuldnerinnen und Schuldner zulassen. Für die Feststellung, dass zweifelsfrei eine Zahlungsunfähigkeit oder Zahlungsunwilligkeit vorliegt, sind jedoch unbedingt folgende Kriterien einzuhalten:

- Es muss sich um eine unbestrittene Forderung handeln.

- Sowohl Gläubigerpartei als auch Inkassounternehmen haben die der Einmeldung zugrunde liegende Forderung gegenüber der Schuldnerpartei nachweisbar mindestens zweimal vergeblich angemahnt.

- Die Schuldnerpartei wird darüber informiert, dass eine Einmeldung bei einer Auskunftei erfolgt, soweit die Forderung unbestritten ist und keine Zahlung innerhalb der gesetzten Frist erfolgt. Diese Unterrichtung kann bereits mit den Mahnschreiben des Inkassobüros verbunden werden. So wird sichergestellt, dass nur Forderungen eingemeldet werden, die bis zum Zeitpunkt der Einmeldung unbestritten sind.

- Die Einmeldung bei einer Auskunftei darf frühestens dann erfolgen, wenn vier Arbeitstage seit Ablauf der im letzten Mahnschreiben des Inkassounternehmens genannten Zahlungs- beziehungsweise Rückantwortfrist von zehn Tagen verstrichen sind.

    - ➡ Zu Zwecken der Forderungseinziehung dürfen Inkassounternehmen personenbezogene Daten, die die Schuldnerpartei und die ausstehende Forderung betreffen, erheben und verarbeiten. Jede weitere Verarbeitung und Nutzung dieser Informationen ist nur unter den genannten strengen Voraussetzungen zulässig.

7.8 Gläsernes Fahrverhalten statt datenfreier Fahrt

Der zunehmende Einsatz elektronischer Systeme, die Kfz-Hersteller zur Aufzeichnung von Fahrdaten seit einiger Zeit in Neuwagen der gehobenen Mittelklasse einbauen, ermöglicht nicht nur die Speicherung sämtlicher Fahrzeugdaten während der Autofahrt. Die Technik bietet zugleich die Möglichkeit, das individuelle Fahrverhalten der Betroffenen zu überwachen.

Bei der Technologie der Aufzeichnungsgeräte handelt es sich regelmäßig um zwei verschiedene Systeme, die einen Teil der vom Fahrzeug erzeugten Daten während des Betriebes und darüber hinaus speichern.

Ein eingebauter Fehlerdatenspeicher zeichnet jeden aufgetretenen technischen Fehler am Fahrzeug neben weiteren Systemangaben wie beispielsweise Informationen zu Geschwindigkeit, Drehzahl, Gang, Motortemperatur, Außentemperatur, Zusammensetzung des Luft-Treibstoffgemisches und Getriebeöldruck zum Zeitpunkt des Fehlers auf. Darüber hinaus verfügen die Fahrzeuge über einen Unfalldatenschreiber, der durch die Auslösung der Airbags aktiviert wird und Informationen zum Steuerungssystem speichert. Dabei handelt es sich beispielsweise um Angaben zu Auslösungszeit, Aufprallimpuls, Benutzung der Anschnallgurte durch die im Fahrzeug befindlichen Personen, Geschwindigkeit und Bremsvorgang. Die Kfz-Hersteller berufen sich insoweit darauf, dass die Daten beider Systeme ausschließlich zu Zwecken der Produkt- und Qualitätsüberwachung ausgelesen und ausgewertet werden.

Selbst wenn beide Systeme in der Regel keine Informationen darüber enthalten, welche Person zum Zeitpunkt des Aufzeichnungsereignisses das Fahrzeug geführt hat, so stellt sich jedoch die Frage nach dem Personenbezug oder der Personenbeziehbarkeit der Aufzeichnungsdaten. Schließlich ist davon auszugehen, dass zum Zeitpunkt des Auslesens des jeweiligen Aufzeichnungssystems in jedem Fall die Halterin oder der Halter des Fahrzeugs bekannt ist, so dass leicht zu ermitteln ist, wer das Fahrzeug zum Zeitpunkt des Aufzeichnungsereignisses geführt hat.

Die Aufzeichnungstechnologie ermöglicht eine Rundumüberwachung der betroffenen Autofahrerinnen und Autofahrer und eine Kontrolle

ihres individuellen Fahrverhaltens. Der von Herstellerseite regelmäßig vorgesehene Einbau der Systeme nimmt den Betroffenen bereits die Entscheidung ab, eine derartige Technik im eigenen Fahrzeug überhaupt verwenden zu wollen. Die Betroffenen haben ferner keine Möglichkeit, die Aufzeichnung der Daten zu unterbinden oder abzubrechen und gespeicherte Daten zu löschen. Darüber hinaus ist bedenklich, dass künftig im Falle eines Unfalls möglicherweise Dritte wie Unfallgegnerinnen und Unfallgegner, beteiligte Versicherungen oder Ermittlungsbehörden die Herausgabe der Aufzeichnungsdaten verlangen könnten.

Diese Umstände widersprechen dem Recht jeder einzelnen Person, sich frei von Registrierung und Überwachung zu bewegen. Vor diesem Hintergrund kann die Erhebung und Verarbeitung dieser Informationen nur mit ausdrücklicher Einwilligung der Betroffenen datenschutzrechtlich zulässig sein.

- Die Systeme sind so zu gestalten, dass keine personenbezogenen Daten erhoben und verarbeitet werden. Die Freigabe und Weitergabe der Daten muss den Betroffenen selbst vorbehalten sein. Alternativ darf eine Aufzeichnung und Verwendung nur mit entsprechender Einwilligung erfolgen.

7.9 Noch nicht fit für den Datenschutz: Fitnessstudios erfassen Kundenprofile

Viele Fitness- und Sportstudios speichern routinemäßig die Anwesenheitszeiten, Verzehrdaten oder auch ein Passfoto ihrer Kundinnen und Kunden mit Hilfe von eigens dafür vorgesehenen Software-Programmen. Einige Betroffene zweifelten an der Zulässigkeit der Datenerfassung und baten um eine datenschutzrechtliche Überprüfung.

Weit verbreitet ist die Praxis, die Zeiten des Betretens und Verlassens der Sportstudios mittels einer computerlesbaren Mitgliedskarte zu erheben. Dadurch werden individuelle Anwesenheitsprofile der Trainierenden gespeichert. Die Erfassung derartiger Profile ist in der Regel ohne eine ausdrückliche und freiwillige Einwilligung der Kundinnen und Kunden unzulässig, da die Studios die Daten in diesem Umfang weder

für Vertragszwecke noch für sonstige berechtigte Interessen benötigen.

Das Erfassen der Daten beim Betreten des Studios ("Check-in") kann jedoch kurzfristig erforderlich sein, um insbesondere die Zahlung des Mitgliedsbeitrags zu überprüfen oder in bestimmten Fällen eine Bescheinigung über den Besuch des Kurses zur Vorlage bei einer Krankenkasse ausstellen zu können. Werden bei krankheits- oder urlaubsbedingtem Aussetzen des Trainings Zeitgutschriften gewährt, kann für die entsprechende Überprüfung der Abwesenheitsdauer ebenfalls eine Speicherung des Check-in notwendig sein. Für andere Zwecke reicht die Erhebung und Speicherung statistischer Daten ohne Personenbezug.

Das Erfassen der Daten beim Verlassen des Studios ("Check-out") ist nur in seltenen Ausnahmefällen erforderlich und daher ohne Einwilligung der Betroffenen grundsätzlich unzulässig. Lediglich bei besonderen Vertragsgestaltungen, etwa wenn Mitglieder einen geringeren Beitrag zahlen, falls sie nur eine begrenzte Stundenzahl im Monat trainieren, kann eine Speicherung der Anwesenheitsdauer erforderlich und zulässig sein.

Bei Sportstudios mit Gastronomiebereich sehen die eingesetzten Datenverarbeitungssysteme oft eine Erfassung aller Umsätze der Kundinnen und Kunden vor ("Verzehrkonto"). Dies ist nur zulässig, wenn die Getränke oder Speisen nicht bar, sondern erst beim Verlassen des Studios oder sogar am Ende eines längeren Abrechnungszeitraums bezahlt werden. Sind die Verzehrdaten für die Rechnungsstellung nicht mehr erforderlich, sind sie zu löschen oder – soweit sie aus handels- oder steuerrechtlichen Gründen noch gespeichert werden müssen – jedenfalls zu sperren.

Weitere Nachfragen der Betroffenen beziehen sich auf das zentrale Speichern von Porträtfotos der Kundinnen und Kunden im Rechner des Studios. Begründet wird das Speichern der Bilddaten mit dem Zweck der Einlasskontrolle. Um eine Weitergabe der Mitgliedskarte an Unbefugte zu verhindern, erscheint beim Einlesen der Karte das gespeicherte Bild auf dem Monitor und wird mit der Person abgeglichen. Für die Einlasskontrolle bedarf es allerdings keiner zentralen Speicherung der Bilder im Datenverarbeitungssystem des Studios. Ausreichend ist vielmehr der Abgleich mit dem Foto in einem Ausweis. Daher ist die

zentrale Speicherung von Portraitfotos im Rechner des Studios ohne freiwillige und schriftliche Einwilligung der Betroffenen unzulässig.

- "Weniger ist oft mehr", gilt nicht für jeden Trainingsplan, ganz bestimmt aber für die Datensammlungen vieler Sportstudios. Die von den entsprechenden Software-Unternehmen angepriesenen EDV-Systeme für Sportstudios verführen zum Erfassen überflüssiger, für den Vertragszweck nicht erforderlicher Mitgliederdaten. Wer auf diese Daten nicht verzichten will, benötigt dafür eine freiwillige, schriftlich erteilte und jederzeit widerrufbare Einwilligung der über die Datenverarbeitung informierten Kundinnen und Kunden.

7.10 Unerwünschte Werbung

Aufdrängen per Telefon, Brief oder E-Mail: Manchen Werbetreibenden scheint jedes Mittel für eine Geschäftsanbahnung recht.

Vielfach klagen Bürgerinnen und Bürger über lästige und aufdringliche Werbung und fragen sich, wie die Unternehmen an ihre Adresse kommen. Eine Vielzahl von Anfragen und Beschwerden betrifft dabei das zögerliche Verhalten von werbetreibenden Unternehmen, den Betroffenen Auskunft über die Datenherkunft zu erteilen. Auch wird zu Recht das oft rüde Vorgehen bei ungebetenen, ohne vorheriges Einverständnis unzulässigen Werbeanrufen moniert. Manche Verantwortliche im Telefonmarketing kennen Datenschutzvorschriften offenbar nicht oder wollen sie nicht kennen. Bei Überprüfungen von Unternehmen muss der Nachweis erbracht werden, dass die Betroffenen in die werbliche Nutzung ihrer Telefonnummer eingewilligt haben.

- Gemeinsam mit anderen Datenschutzbeauftragten wurde ein Merkblatt "Adressenhandel und unerwünschte Werbung – Tipps und Informationen" in überarbeiteter Fassung herausgegeben (abrufbar unter: www.ldi.nrw.de).

8 Verfassungsschutz

8.1 Kernbereich privater Lebensgestaltung unzureichend geschützt

Die sicherheitspolitische Diskussion der vergangenen Jahre ist von dem ständigen Ruf nach zusätzlichen Rechten und Kompetenzen für Polizei und Nachrichtendienste geprägt. Mit der im Dezember 2006 verabschiedeten Änderung des Verfassungsschutzgesetzes NRW (VSG NRW) sind bisher noch befristet geltende Eingriffsbefugnisse dauerhaft zementiert und neue Befugnisse geschaffen worden. Hinweise auf verfassungsrechtliche Risiken hatten keine Chance auf Gehör.

Nicht zuletzt unter dem Eindruck der Anschläge vom 11. September 2001 waren dem Verfassungsschutz im Dezember 2002 befristet bis zum Ende des Jahres 2006 zahlreiche neue Auskunfts- und Eingriffsbefugnisse eingeräumt worden. Die Auskunftsrechte des neu geschaffenen § 5a VSG NRW gegenüber Kreditinstituten, Luftfahrtunternehmen sowie Post- und Telekommunikationsdienstleistern waren seinerzeit bewusst auf die Bekämpfung des internationalen Terrorismus beschränkt worden. Nunmehr gelten diese Befugnisse nicht nur auf Dauer, sondern ihr Anwendungsbereich wurde kurzerhand auf alle Aufgabenbereiche des Verfassungsschutzes, insbesondere auch auf inländische Bestrebungen gegen die freiheitliche demokratische Grundordnung (§ 3 Abs. 1 Nr. 1 VSG NRW) ausgedehnt. Der Versuch einer tatbestandlichen Eingrenzung auf die nach der Begründung des Änderungsgesetzes neu erkannten Gefahren sogenannter Homegrown–Netzwerke wurde gar nicht erst unternommen. Gleichzeitig sind die seinerzeit bewusst mit den neuen Auskunftsrechten verknüpften Verfahrensregelungen zum Schutz des Grundrechts auf informationelle Selbstbestimmung abgebaut worden. Kontostammdaten und Auskünfte von Luftfahrtunternehmen darf der Verfassungsschutz künftig ohne Beteiligung der G 10-Kommission einholen.

Wenig Beachtung schenkt das geänderte Verfassungsschutzgesetz der Entscheidung des Bundesverfassungsgerichts zum großen Lauschangriff vom 3. März 2004 (BVerfGE 109, 279). Das Bundesverfassungsgericht hatte festgestellt, dass zur Menschenwürde gemäß Art. 1 Abs. 1 Grundgesetz (GG) die Anerkennung eines absolut geschützten

Kernbereichs privater Lebensgestaltung gehört, der jedem staatlichen Eingriff entzogen ist. Die seinerzeit gültige Regelung der akustischen Wohnraumüberwachung in der Strafprozessordnung wurde für verfassungswidrig erklärt, da sie dem nicht hinreichend Rechnung trug (siehe Bericht 2005 unter 9.1). Auch die unverändert beibehaltene Regelung der akustischen Wohnraumüberwachung in § 7 Abs. 2 VSG NRW genügt den vom Bundesverfassungsgericht aufgestellten Anforderungen nicht und hätte deshalb entweder gestrichen oder zumindest um Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung ergänzt werden müssen. Gleichwohl hat der Gesetzgeber unverändert an der Regelung zur akustischen Wohnraumüberwachung festgehalten. Das in der Begründung des Änderungsgesetzes nachzulesende Argument, es solle zunächst die weitere Rechtsprechung des Bundesverfassungsgerichts abgewartet und sodann eine Lösung im Verbund der Verfassungsschutzbehörden gesucht werden, kann die verfassungsrechtlichen Bedenken nicht ausräumen.

Erstmals wird dem Verfassungsschutz zudem ausdrücklich auch die Befugnis eingeräumt, wie ein "Hacker" mit Einsatz technischer Mittel heimlich auf gespeicherte Computerdaten Zugriff nehmen zu können. Mit großer Selbstverständlichkeit werden heute sensible Daten wie Steuererklärungen, ärztliche Abrechungen oder tagebuchartige Aufzeichnungen in privaten Computern gespeichert. Das heimliche Auslesen gespeicherter Computerdaten greift deshalb nicht nur tief in das Grundrecht auf informationelle Selbstbestimmung ein, sondern kann im Einzelfall auch den absolut geschützten Kernbereich privater Lebensgestaltung verletzen. Auch hier wäre es deshalb verfassungsrechtlich geboten gewesen, dass der Gesetzgeber selbst Regelungen zum Schutz der Menschenwürde trifft. Das Bundesverfassungsgericht hat jedenfalls keine Zweifel daran gelassen, dass die Notwendigkeit, Regelungen zum Schutz der individuellen Entfaltung im Kernbereich privater Lebensgestaltung zu treffen, nicht auf die akustische Wohnraumüberwachung beschränkt ist (BVerfGE 113, 348/391 f.).

Darüber hinaus bleiben Zweifel, ob der Zugriff auf gespeicherte Computerdaten nicht auch am Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) zu messen ist, wenn sich der Computer oder Laptop in einer Wohnung befinden. In seiner Entscheidung zum großen Lauschangriff vom 3. März 2004 hat das Bundesverfassungsgericht ausgeführt, dass der Schutzbereich des Art. 13 GG nicht nur durch ein

physisches Betreten oder Eindringen berührt werde. Vielmehr erlaubten es die heutigen technischen Gegebenheiten, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Art. 13 Abs. 1 GG umfasst wäre (BVerfGE 109, 279/309). Den strengen Voraussetzungen des Art. 13 GG wird der Gesetzentwurf jedenfalls nicht gerecht. Weder wird die vorgesehene Eingriffsbefugnis an eine nach Art. 13 Abs. 4 GG erforderliche dringende Gefahr für die öffentliche Sicherheit noch an eine richterliche Entscheidung gebunden.

➡ Die Novellierung des Verfassungsschutzgesetzes reiht sich ein in die Kette sicherheitspolitischer Gesetzgebungsvorhaben des Bundes und der Länder, mit denen das Grundrecht auf informationelle Selbstbestimmung und andere freiheitssichernde Grundrechte immer weiter beschnitten werden. Die beabsichtigte Übernahme zunächst befristeter Eingriffsbefugnisse in dauerhaftes Recht zeigt einmal mehr, dass entsprechende Befristungs- und Evaluierungsregelungen kaum mehr als "datenschutzrechtliche Beruhigungspillen" darstellen, die bei nächster Gelegenheit abgesetzt werden.

9 Polizei

9.1 Rasterfahndung rechtswidrig

Die nach den Terroranschlägen vom 11. September 2001 durchgeführte Rasterfahndung war verfassungswidrig. Dies stellte das Bundesverfassungsgericht in seiner Entscheidung vom 4. April 2006 fest (BVerfG, 1 BvR 518/02).

Die Daten von rund 8,4 Millionen Männern, davon allein in Nordrhein-Westfalen mehr als 5 Millionen, wurden nach dem 11. September 2001 im Rahmen einer in dieser Größenordnung einmaligen Rasterfahndung von den Polizeibehörden erhoben und mit Hilfe von "Kommissar Computer" auf der Suche nach potentiellen islamistischen Terroristen, sogenannten "Schläfern", durchleuchtet (siehe hierzu Bericht 2003 unter 16 und Bericht 2005 unter 8.2). Von der schon wegen grundsätzlicher Bedenken mehr als zweifelhaften Verdachtsschöpfungsmethode Rasterfahndung betroffen war auch ein in Deutschland lebender marokkanischer Student. Dieser wehrte sich mit einer Verfassungsbeschwerde gegen die Erhebung seiner Daten. Mit Erfolg: Die Anordnung der Rasterfahndung war rechtswidrig, so das Bundesverfassungsgericht in seiner Entscheidung vom 4. April 2006.

In seiner Begründung stellt das Bundesverfassungsgericht fest, dass die Rasterfahndung tief in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen eingreift, weil die gesetzlichen Grundlagen (in Nordrhein-Westfalen § 31 Polizeigesetz) es der Polizei gestatten, riesige Mengen von Daten aus unterschiedlichen Beständen einer Vielzahl öffentlicher und privater Stellen miteinander zu verknüpfen und abzugleichen. Von der Eingriffsmaßnahme sind alle Personen betroffen, die die von der Polizei bestimmten Auswahlkriterien erfüllen, ohne dass es Anforderungen an die Nähe dieser Personen zur Gefahr gibt oder die Adressaten der Eingriffsmaßnahme für die Gefahr verantwortlich sein müssen. Die Rasterfahndung erlaubt somit verdachtslose Grundrechtseingriffe mit großer Streubreite. Darüber hinaus begründet die Rasterfahndung für die betroffenen Personen ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden. Dieses "rechtsstaatliche Defizit", so wörtlich das Bundesverfassungsgericht (BVerfG a.a.O., Absatz-Nr. 140), das mit dem für die Rasterfahndung typischen Verzicht auf eine Nähebeziehung zwischen

dem gefährdeten Rechtsgut und den von dem Grundrechtseingriff Betroffenen verbunden ist, gebietet es deshalb verfassungsrechtlich zwingend, die Zulässigkeit der Rasterfahndung an das Erfordernis einer konkreten Gefahr für die bedrohten hochrangigen Rechtsgüter zu knüpfen. Eine solche konkrete Gefahr konnte das Bundesverfassungsgericht auf der Grundlage der mit der Verfassungsbeschwerde angegriffenen Entscheidung des Oberlandesgerichts Düsseldorf sowie den zugrunde liegenden instanzgerichtlichen Entscheidungen des Landgerichts und Amtsgerichts Düsseldorf, die die Rasterfahndung für zulässig hielten, nicht feststellen. Eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden habe, oder außenpolitische Spannungslagen reichen dagegen für die Anordnung einer Rasterfahndung nicht aus.

- Das Bundesverfassungsgericht hat mit dieser Entscheidung einmal mehr dem ausufernden Datenhunger der Sicherheitsbehörden klare Grenzen gesetzt. Rasterfahndungen auf polizeirechtlicher Grundlage sind nur bei konkreter Gefahr für hochrangige Rechtsgüter zulässig. Daran wird sich künftig jede gesetzliche Regelung zur polizeilichen Rasterfahndung sowie jede konkrete Anordnung einer solchen Maßnahme messen lassen müssen.

9.2 Datenübermittlung – schneller als die Polizei erlaubt

Nach wie vor gehört die polizeiliche Verbunddatei "Gewalttäter Sport" zu den Dauerbrennern unter den eingehenden Anfragen und Beschwerden. In ihr werden bundesweit Personen gespeichert, die im Zusammenhang mit Sportveranstaltungen, insbesondere mit Fußballspielen, strafrechtlich in Erscheinung getreten sind oder Adressaten einer polizeilichen Personalienfeststellung, eines Platzverweises oder einer Ingewahrsamnahme waren.

So beklagte ein Betroffener zu Recht eine unzulässige Übermittlung seiner in der Datei "Gewalttäter Sport" gespeicherten Daten durch die Polizei. Ein Fußballverein der zweiten Bundesliga hatte gegen den Betroffenen ein Stadionverbot ausgesprochen. Der Beschwerdeführer wehrte sich gegen das Hausverbot mit einer zivilrechtlichen Klage vor

dem Amtsgericht. Der Anwalt des beklagten Bundesligavereins ersuchte daraufhin das für den Wohnort des Betroffenen zuständige Polizeipräsidium um Auskunft über den Betroffenen, um die über den Beschwerdeführer gespeicherten Daten in den Prozess einbringen zu können. Das Polizeipräsidium nahm diese Bitte des Anwalts zum Anlass, dem Amtsgericht – ohne von diesem hierzu aufgefordert worden zu sein – Auskunft über die in der Datei "Gewalttäter Sport" über den Betroffenen gespeicherten Daten zu erteilen. Hierzu war die Polizei nicht befugt. Die Polizei darf einer anderen öffentlichen Stelle, auch einem Gericht, nur dann "von sich aus" personenbezogene Daten übermitteln, wenn dies zur Erfüllung ihrer Aufgaben, also Aufgaben der Polizei, erforderlich ist oder die Kenntnis der Daten zur Aufgabenerfüllung der empfangenden Stelle, hier des Gerichtes, für den Bereich der Gefahrenabwehr erforderlich erscheint (§ 28 Polizeigesetz NRW). Diese Voraussetzungen lagen indes nicht vor. Weder gehört es zu den Aufgaben der Polizei, eine Partei in einem Zivilprozess ohne Anforderung durch das Gericht zu unterstützen und mit polizeilichen Informationen zu versorgen, noch nimmt ein Zivilgericht selbst Aufgaben der Gefahrenabwehr wahr. Das Polizeipräsidium hat zugesagt, bei Datenübermittlungen an öffentliche Stellen, insbesondere auch an Gerichte, das Vorliegen der genannten gesetzlichen Vorgaben künftig genauer zu prüfen.

Die Datei "Gewalttäter Sport" war darüber hinaus Gegenstand einer stichprobenartigen Überprüfung bei einer anderen für einen Bundesligastandort zuständigen Kreispolizeibehörde. Dabei wurden, gemessen an den Kriterien der geltenden Errichtungsanordnung, erfreulicherweise nur wenige Mängel festgestellt. So wurde in einigen Fällen die Löschungsprüffrist geringfügig zu lang berechnet. In anderen Fällen wurde es versehentlich versäumt, nach einer erfolgten elektronischen Löschung des Datensatzes auch den vorhandenen Papierrückhalt zu vernichten oder das Tatdatum zu speichern mit der Folge, dass die Prüf- beziehungsweise Löschungsfrist nicht mehr nachvollziehbar berechnet werden konnte. Grundsätzlichen Bedenken begegnen unter Verhältnismäßigkeitsgesichtspunkten Eintragungen, die lediglich aufgrund polizeilicher Personalienfeststellungen, Platzverweise oder Ingewahrsamnahmen im Zusammenhang mit Fußballspielen erfolgen, ohne dass gegen die Betroffenen konkrete strafrechtliche Vorwürfe erhoben werden (siehe hierzu Bericht 2001 unter 4.). Die in diesen Fällen gleichzeitig erforderliche Prognose, dass die von der Maßnahme

betroffene Person sich künftig an anlassbezogenen Straftaten beteiligen werde, war in einer Reihe von Fällen nicht hinreichend dokumentiert. Allerdings konnte der im Rahmen der Prüfung hinzugezogene szenekundige Beamte auf Nachfrage in allen fraglichen Einzelfällen das zur Begründung der Prognoseentscheidung erforderliche Hintergrundwissen darlegen und die Gründe, die zur Aufnahme der jeweiligen Person in die Datei geführt haben, nachvollziehbar schildern. Es wurde zugesagt, die Thematik intern aufzugreifen und die Qualität der Dokumentation verbessern zu wollen. Schließlich fiel auf, dass der Ausgang strafrechtlicher Ermittlungsverfahren, soweit diese zu einer Speicherung in der Datei "Gewalttäter Sport" führen, von der Polizei nicht nachgehalten wurde. Das Innenministerium hat diese Feststellung zum Anlass für einen Hinweis an die Polizeibehörden genommen, Mitteilungen der Staatsanwaltschaften über den Ausgang strafrechtlicher Ermittlungsverfahren nicht nur im Rahmen der Führung von Kriminalakten, sondern auch hinsichtlich einer möglichen Speicherung der betroffenen Person in der Datei "Gewalttäter Sport" zu berücksichtigen.

➡ Ungeachtet fortbestehender Bedenken gegen eine Speicherung von Personen, gegen die keine strafrechtlichen Vorwürfe erhoben werden, hat die stichprobenartige Prüfung der Datei "Gewalttäter Sport" bei einer "Bundesligabehörde" keine schwerwiegenden Mängel der Speicherpraxis offenbart. Auch in Zukunft wird aber sorgfältig darauf zu achten sein, dass der Grundsatz der Verhältnismäßigkeit in jedem Einzelfall beachtet wird.

9.3 Heimlich, still und unzulässig

Bei dem Versuch des niedersächsischen Gesetzgebers, eine polizeirechtliche Ermächtigung zur Überwachung von Telekommunikation einzuführen, handelte es sich um einen gesetzgeberischen Fehlschuss, der eine Mehrzahl von Verfassungsverstößen enthält und sich daher nicht zur Nachahmung durch andere Landesparlamente empfiehlt.

Mit Gesetz vom 11. Dezember 2003 wollte der Landesgesetzgeber in Niedersachsen seinen Polizeibehörden die Befugnis einräumen, zu den Zwecken der Gefahrenabwehr und der Strafverfolgungsvorsorge die Telekommunikation von Personen zu überwachen, die verdächtigt wer-

den, möglicherweise zukünftig Straftaten von erheblicher Bedeutung zu begehen. Erhebliche Bedeutung besaßen nach Ansicht des Gesetzgebers nicht nur alle Verbrechen, sondern auch eine Vielzahl von Vergehen, die nicht abschließend definiert wurden. Eine nachträgliche Unterrichtung über die heimliche Überwachung konnte aufgrund von Ausnahmebestimmungen jahrelang zurückgestellt werden oder gar ganz unterbleiben.

Das Bundesverfassungsgericht hat am 27. Juli 2005 dieses Gesetz – jeweils aus mehreren Gründen – für formell und materiell verfassungswidrig erklärt (BVerfGE 113, 348). Es betonte die prinzipielle Verschiedenheit der Datenerhebung zur Gefahrenabwehr (Verhinderung von Rechtsgutsverletzungen) und zur Strafverfolgung (Aufklärung und Ahndung begangener Straftaten). Während die Gefahrenabwehr unter die Gesetzgebungskompetenz des Landes fällt, gehört die Strafverfolgung zum Kompetenzbereich des Bundes. Das Gericht verlangte von den Ländern zu respektieren, dass der Bundesgesetzgeber bei der Regelung der zulässigen strafrechtlichen Ermittlungsmaßnahmen bewusst auf eine Ermächtigung zu derartigen Beweiserhebungen im Vorfeld eventueller künftiger Strafverfahren verzichtet habe. Das hier vom Bundesverfassungsgericht hervorgehobene Verbot für die Länder, sich mittels Polizeirecht zur Beweisbeschaffung auf Vorrat für eventuelle Strafverfahren zu ermächtigen, verdient auch in anderen Bereichen, wie zum Beispiel der polizeilichen Videoüberwachung, besondere Beachtung.

Angesichts der Heimlichkeit und Schwere des Eingriffs, dessen rechtfertigende Basis nur in einer unsicheren Prognoseentscheidung besteht, kritisierten die Verfassungsrichterinnen und –richter ferner die zu unbestimmte und viel zu weite Fassung der Ermächtigungsgrundlage, die auch durch einschränkende Auslegung nicht als noch verfassungsgemäß zu retten sei. Neben strengen nachträglichen Mitteilungspflichten fehlten in dem Gesetz auch und vor allem die verfassungsrechtlich gebotenen Vorkehrungen zum Schutz vor Eingriffen in den unantastbaren Kernbereich der privaten Lebensgestaltung (siehe BVerfGE 109, 279 zum "Großen Lauschangriff"). Zwar sei der Schutz der freien Telekommunikation anders ausgestaltet als die Garantie der Unverletzlichkeit der Wohnung. Dennoch dürfe das im Bereich der Telekommunikation nicht ganz ausschließbare Risiko, bei Datenerhebungen unvorhergesehen in den absolut geschützten Kernbereich privater

Lebensgestaltung einzudringen, nur zum Schutz besonders hochrangiger Rechtgüter in Kauf genommen werden. Für derartige Ausnahmefälle müssten ein absolutes Beweisverwertungsverbot und ein unverzügliches Löschungsgebot normiert werden.

➡ Mit dieser von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßten Entscheidung (siehe die Entschließung vom 27./28. Oktober 2005, abgedruckt im Anhang) hat das Bundesverfassungsgericht bestätigt, dass der jeweilige Gesetzgeber bei allen verdeckten Überwachungsmaßnahmen, egal ob sie im Rahmen von polizeilicher Gefahrenabwehr, Strafverfolgung oder Verfassungsschutz stattfinden, die erforderlichen Vorkehrungen dafür zu treffen hat, dass der absolut geschützte Kernbereich privater Lebensgestaltung unangetastet bleibt.

10 Justiz

10.1 DNA-Asservatenkammer im Computer

"Ein starker Rechtsstaat ist bescheiden" lautet ein denkwürdiger Ausspruch eines ehemaligen Richters am Bundesverfassungsgericht. Diesem Grundsatz sollte auch im Hinblick auf die Schaffung von immer weiteren Ermächtigungsgrundlagen für Grundrechtseingriffe und angesichts der Tendenz zu ausufernden Datensammlungen auf Vorrat größere Beachtung geschenkt werden.

Die DNA-Analyse beschäftigt den Datenschutz seit Jahren als Dauerthema (siehe Berichte 1999 unter 3.3, 2003 unter 17.1 und 2005 unter 9.2). DNA-Identifizierungsmuster sind Persönlichkeitsmerkmale in Form von Zahlencodes. Sie haben kein Verfallsdatum und brauchen kaum Speicherplatz. Zu groß ist daher die Versuchung für die Ermittlungsbehörden, die digitale Vorratskammer für die Straftatenvorsorge gut zu füllen. Die stete Erweiterung des Einsatzes der DNA-Analyse im Strafverfahrensrecht geht mit einer enormen Zunahme des in der DNA-Analyse-Datei gespeicherten Datenbestandes einher. Enthielt die Datei im April 2000 rund 39.000 Datensätze (35.000 Personen und 4.000 Spuren), ist der Datenbestand bis zum September 2006 bereits auf über 500.000 Datensätze (über 400.000 Personen und rund 97.000 Spuren) angewachsen. Zu befürchten ist ein weiterer rasanter Anstieg der Einträge.

Denn die Rechtslage stellt sich aufgrund der Änderung der Strafprozessordnung seit 1. November 2005 wie folgt dar: Neben der Begehung einer Straftat von erheblicher Bedeutung kann die mehrfache Begehung nicht erheblicher Straftaten als so schwerwiegend eingeschätzt werden, dass sie bei Wiederholungsgefahr zur Aufnahme der DNA-Daten in die Datei führt. Die DNA-Analyse darf zudem jetzt zur Tataufklärung und zur Identifizierung in künftigen Strafverfahren auch ohne richterliche Anordnung eingesetzt werden, wenn die betroffene Person einwilligt. Die Wirksamkeit dieser Einwilligungen ist allerdings fraglich, da weder in der Vernehmungssituation von Verdächtigen noch bei bereits verurteilten, inhaftierten Personen von einer echten Freiwilligkeit gesprochen werden kann.

In Nordrhein-Westfalen ist auch die Umsetzung der Einwilligungslösung problematisch, weil der Inhalt der gesetzlichen Bestimmungen, in deren Rechtsfolgen eingewilligt werden soll, in den entsprechenden Einwilligungsformularen und Hinweisblättern nicht vollständig erläutert wird. Außerdem ist problematisch, dass die nordrhein-westfälischen Erlasse zwar eine polizeiliche Prüfung der Speichervoraussetzungen für einen Eintrag in die DNA-Analyse-Datei fordern; anders als in anderen Ländern und entgegen der Empfehlung der LDI wird aber keine Dokumentation dieser Prüfung verlangt.

Wozu es führen kann, wenn die Speichervoraussetzungen nicht aktenkundig gemacht werden müssen, zeigt der folgende Beispielsfall: Anlässlich der Durchführung der Fußballweltmeisterschaft wurde in Dortmund ein zufällig in einen Polizeikessel geratener jugendlicher Besucher als "potenzieller Gewalttäter" mit sogenannten Gefährderansprachen überzogen, in deren Zusammenhang – je nach Perspektive – die Einwilligung in eine DNA-Analyse "erfragt" oder "nahegelegt" wurde. Für die Erfüllung der weiteren gesetzlichen Speichervoraussetzungen gab es keinerlei Anhaltspunkte. Auf Nachfrage erklärte die zuständige Kreispolizeibehörde, sie habe auch bei Einwilligung des Betroffenen vorgehabt, vor einer Speicherung noch die weiteren gesetzlichen Voraussetzungen zu prüfen. Eine solche Einholung von Einwilligungen auf Vorrat ist jedoch – polizeiliche Effektivitätsüberlegungen einmal hintangestellt –, auch wenn es sich um tatsächliche Beschuldigte handelt, mangels Aufklärung über den Zweck der Datenerhebung datenschutzrechtlich unzulässig.

➡ Richterliche Anordnungen sind der Einwilligungslösung vorzuziehen. In der Praxis muss mindestens dafür gesorgt werden, dass das Vorliegen der Speicherungsvoraussetzungen sorgfältig geprüft und dokumentiert wird, bevor um die Einwilligung gebeten wird.

10.2 Immer der Reihe nach

Mit "Offensive der Wattestäbchen" und ähnlichen Schlagworten wurden in der Presse Fälle im ganzen Bundesgebiet bezeichnet, in denen DNA-Proben einer Vielzahl, oft Tausender von Unbeteiligten analysiert wurden, um auf die Spur von Tatverdächtigen zu gelangen.

Für die bereits seit vielen Jahren durchgeführten sogenannten DNA-Reihenanalysen, auch als Massengentests bezeichnet, ist ebenfalls im Zuge der Änderung der Strafprozessordnung vom 12. August 2005 eine Rechtsgrundlage geschaffen worden. Danach ist der Einsatz dieser Maßnahme in Ermittlungsverfahren nur bei bestimmten schweren Straftaten erlaubt und bedarf einer richterlichen Anordnung, in der auch der Personenkreis festgelegt werden muss, dessen DNA mit der Tatortspur abgeglichen werden soll. Für die Entnahme und Untersuchung bei den immerhin an sich unverdächtigen Personen ist dann zusätzlich die schriftliche Einwilligung der Betroffenen erforderlich. Weil den Betroffenen damit – abgesehen von dem sozialen Druck, der die Freiwilligkeit gefährdet – die Teilnahme freigestellt ist, darf eine Ablehnung im weiteren Verfahren nicht zu ihrem Nachteil verwendet werden. Daher sollten Erlasse und Informationsschreiben die Strafverfolgungsbehörden wie auch die Betroffenen deutlich darauf hinweisen, dass auf die Verweigerung der Teilnahme allein kein Beschuldigtenstatus gegründet werden darf. Ferner muss bei Anwendung der neuen Rechtsgrundlage der betroffene Personenkreis aus Gründen der Verhältnismäßigkeit klar und eng bestimmt werden. DNA-Reihen-Analysen dürfen nicht als Standardmittel, sondern nur als ultima ratio eingesetzt werden, wenn andere Ermittlungswege nicht zum Erfolg führen.

- Werden DNA-Reihenanalysen im Strafverfahren eingesetzt, ist darauf zu achten, dass die Unschuldsvermutung auch für diejenigen gilt, die zu einer freiwilligen Mitwirkung an den DNA-Tests nicht bereit sind.

10.3 Kein Einsehen bei der Justiz

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen. Dies setzt die Kenntnis darüber voraus, ob und welche Daten bei einer Behörde über die eigene Person gespeichert sind (BVerfGE 65, 1/43).

Das Recht auf Auskunft und Akteneinsicht in die zur eigenen Person gespeicherten Daten ist in § 18 Datenschutzgesetz NRW (DSG NRW) geregelt. Allerdings scheint dieses Recht nicht bei allen Behörden und Gerichten bekannt zu sein. Diese Erfahrung musste auch ein Bürger

machen, der sich zunächst mit einer Beschwerde über ein Landgericht an den Petitionsausschuss des nordrhein-westfälischen Landtags gewandt hatte. Wie in solchen Fällen üblich, forderte der Petitionsausschuss zunächst über das zuständige Justizministerium einen Bericht des Landgerichts an. In diesem Bericht wurde der Beschwerdeführer aufgrund einer Personenverwechselung zu Unrecht als kürzlich verurteilter Straftäter dargestellt. Um der Angelegenheit auf den Grund zu gehen, begehrte der Betroffene nunmehr Einsicht in den zu seiner Petition beim Landgericht geführten Vorgang. Eigentlich kein Problem, sieht doch § 18 DSG NRW einen solchen Anspruch ausdrücklich vor. Umso größeres Erstaunen ruft deshalb die Reaktion des Landgerichts hervor, bei dem der Beschwerdeführer mit seinem Einsichtsbegehren auf völliges Unverständnis stieß. Hartnäckig weigerte sich das Landgericht, dem Beschwerdeführer Einsicht in die über seine Person gespeicherten Daten zu gewähren. Dabei berief es sich zunächst auf Vorschriften des Informationsfreiheitsgesetzes, ohne zu beachten, dass das Recht auf Auskunft über und Einsicht in die zur eigenen Person gespeicherten Daten nach § 18 DSG NRW vorrangig ist. Später meinte das Landgericht rechtsirrig, nicht selbst für die im Rahmen der Petitionsbearbeitung erfolgte Verarbeitung der personenbezogenen Daten des Betroffenen verantwortlich zu sein, da es lediglich aufgrund eines Berichtsauftrags des Justizministeriums gehandelt und die Entscheidung des Petitionsausschusses vorbereitet habe. Auch insoweit musste sich das Landgericht belehren lassen, dass es bei der Erstellung seines Berichts – ungeachtet bestehender Berichtspflichten – die personenbezogenen Daten des Beschwerdeführers als verantwortliche Stelle im Sinne des § 3 Abs. 3 DSG NRW verarbeitet hatte.

➡ Trotz mehrerer Hinweise auf die Rechtslage konnte das Landgericht erst nach Einschaltung des Justizministeriums dazu bewegt werden, das Einsichtsrecht des Beschwerdeführers dem Grunde nach anzuerkennen.

10.4 Immer gleich das ganze Grundbuch?

Überrascht waren die Käuferinnen und Käufer mehrerer Baugrundstücke, als sie eines Tages Post ihres Amtsgerichts vorfanden. Das Schreiben enthielt einen kompletten Grundbuchauszug einer gleichzeitig von allen Käuferinnen und Käufern im Bruchteilseigentum miterworbenen Spielplatzfläche einschließ-

lich aller eingetragenen Belastungen. Jede Käuferin und jeder Käufer wurde auf diese Weise bestens über die zur Finanzierung aufgenommenen Grundschulden und Hypotheken der Nachbarschaft ins Bild gesetzt.

Die von den Grundbuchabteilungen der Amtsgerichte geführten Grundbücher enthalten in der Abteilung I nicht nur Angaben über die genaue Bezeichnung eines Grundstücks und dessen Eigentumsverhältnisse, sondern darüber hinaus in den Abteilungen II und III auch weitere sensible Daten, insbesondere über Grundschulden und Hypotheken, die auf den Grundstücken liegen. Der Blick in das Grundbuch lässt so Rückschlüsse auf die finanzielle Situation der Eigentümerinnen und Eigentümer zu. Das Grundbuch ist deshalb auch nicht öffentlich. Einblick nehmen und Auszüge erhalten kann nach § 12 Grundbuchordnung (GBO) nur, wer ein berechtigtes Interesse an den Informationen geltend machen kann. Dabei ist das berechtigte Interesse jeweils mit Blick auf die entsprechende Abteilung des Grundbuchs und die darin enthaltenen Informationen zu prüfen. Dies wird in der Praxis nicht immer ausreichend beachtet.

So auch im Fall der Beschwerdeführerinnen und Beschwerdeführer. Hier wurde das Grundbuchblatt für die Spielplatzfläche erst nach der Parzellierung der Nachbargrundstücke erstellt, und die jeweiligen Miteigentumsanteile wurden zugunsten der finanzierenden Banken verpfändet. Sodann übersandte das Grundbuchamt allen Käuferinnen und Käufern jeweils unter Missachtung des § 12 GBO vollständige Grundbuchauszüge einschließlich der in der Abteilung III eingetragenen Grundschulden und Hypotheken aller Miteigentümerinnen und Miteigentümer, obwohl keine dieser Personen ein berechtigtes Interesse an der Kenntnis der jeweils zulasten ihrer Nachbarinnen und Nachbarn eingetragenen Belastungen geltend gemacht hatte. Ursächlich dafür mögen nicht zuletzt technische Probleme gewesen sein, da die zur automatisierten Führung der Grundbücher derzeit im Einsatz befindlichen Programme nicht in der Lage sind, Teilgrundbuchauszüge zu erstellen.

Erfreulich ist, dass zunächst das Oberlandesgericht Düsseldorf und schließlich auch das Justizministerium des Landes Nordrhein-Westfalen die Thematik aufgegriffen und die Amtsgerichte beispielhaft auf die Verfahrensweise des Amtsgerichts Düsseldorf hingewiesen haben. Dort wird bei Miteigentümergemeinschaften nach Bruchteilen nur ein Ein-

sichtsrecht bezogen auf die betroffenen Miteigentumsanteile gewährt, soweit nicht im Einzelfall ein weitergehendes berechtigtes Interesse geltend gemacht wird. Die Einsichtnahme erfolgt – da das IT-Progamm Teilauszüge nicht erstellen kann – mittels Papierausdruck und Abdecken der nicht benötigten Grundbuchteile.

➧ Das Beispiel zeigt, dass unzureichende technische Lösungen – hier die fehlende Möglichkeit auf automatisiertem Weg Teilgrundbuchauszüge erstellen zu können – nicht zulasten des Datenschutzes gehen dürfen. Notfalls muss "von Hand" nachgearbeitet werden. Nach wie vor gilt der Grundsatz: Die Technik muss dem Recht folgen und nicht umgekehrt.

10.5 Paketversand an Gefangene

Zumindest in kleineren Ortschaften, in denen "man sich kennt", ist es problematisch, wenn bei der Paketaufgabe in der Post durch Aufkleber auf den Versandstücken erkennbar wird, dass sie an Inhaftierte einer Justizvollzugsanstalt gesandt werden.

So manche Eltern mögen sich daher die unangenehme Frage gestellt haben, ob nicht der Aufdruck "Haus X, HR Y" auf dem Geburtstagspaket für ihren Sohn die Postbeschäftigten darüber in Kenntnis setzt, dass dieser wohl eine Haftstrafe abzusitzen hat. Auf Bitten einzelner Gefangener wurde daher die in der Vergangenheit bereits über die obligatorische Verwendung von vorgedruckten Paketmarken für Pakete an Gefangene geführte Diskussion (siehe hierzu Bericht 1997 unter 10) mit dem Justizministerium erneut aufgegriffen und auf eine datenschutzgerechte Lösung gedrungen.

➧ Das Justizministerium hat daraufhin verfügt, dass an Stelle der bisher üblichen Paketmarken von den Justizvollzugsanstalten des Landes künftig nur noch Adressaufkleber mit einem unverfänglichen Zahlencode verwendet werden, aus dem Außenstehende nicht auf die Inhaftierung der Adressatin oder des Adressaten schließen können.

10.6 Missbräuchliche Akteneinsicht

Ermittlungsakten der Staatsanwaltschaft enthalten häufig eine Fülle von interessanten Informationen und personenbezogenen Daten. Nicht zuletzt auch zum Schutz des Grundrechts auf informationelle Selbstbestimmung hat der Gesetzgeber die Einsichtnahme in Ermittlungsvorgänge in der Strafprozessordnung (StPO) an strenge Voraussetzungen und Zweckbindungen geknüpft. Dies gilt auch für Rechtsanwältinnen und Rechtsanwälte.

Nach § 475 StPO kann einer Rechtsanwältin oder einem Rechtsanwalt Auskunft aus und Einsicht in Ermittlungsakten der Staatsanwaltschaft gewährt werden, wenn hierfür ein berechtigtes Interesse dargelegt wird. Es ist deshalb grundsätzlich zulässig, dass die Staatsanwaltschaft einer Rechtsanwältin oder einem Rechtsanwalt Einsicht in die wegen eines mutmaßlichen Immobilienbetrugs geführte Strafakte gewährt, damit die darin befindlichen Informationen genutzt werden können, um zivilrechtliche Ansprüche im Zusammenhang mit möglichen Betrügereien geltend machen zu können. Allerdings hatte der betreffende Rechtsanwalt aus den Strafakten nicht nur Daten erhoben, die seinem Mandanten zugutekommen sollten, sondern auch die Adressdaten einer Vielzahl weiterer mutmaßlich geprellter Anlegerinnen und Anleger notiert. Diese wurden im Folgenden von der gleichfalls anwaltlich vertretenen "Interessengemeinschaft" der Geschädigten angeschrieben und zum Beitritt zu der "Interessengemeinschaft" eingeladen, in der sich die betrogenen Anlegerinnen und Anleger zur Bündelung ihrer Interessen zusammenschließen sollten. Das legitime Recht der geschädigten Person – vertreten durch eine Anwältin oder einen Anwalt – auf Akteneinsicht in die Strafakte des mutmaßlichen Schädigers wurde auf diese Weise zu einem bequemen Verfahren der Mandantenakquise umfunktioniert.

Dies steht jedoch zu der ausdrücklichen Zweckbindungsvorschrift des § 477 Abs. 5 StPO im Widerspruch, wonach die aus einer Akteneinsicht gewonnenen Daten eben nur für den beantragten Zweck genutzt werden dürfen und ein Verarbeiten für weitergehende Zwecke nur dann zulässig ist, wenn die zuständige Behörde dies ausdrücklich erlaubt. Ebenso wenig besteht ein überwiegendes berechtigtes Interesse der betreffenden Anwaltskanzlei gemäß § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG), die im Strafverfahren erfassten Daten der

betroffenen Anlegerinnen und Anleger zugunsten eigener Geschäftszwecke zu verarbeiten. Ein von der "Interessengemeinschaft" angeschriebener Fondsanleger war über die ungebetene Werbung deshalb zu Recht mehr als irritiert. Im Rahmen des gegen den Rechtsanwalt durchgeführten Ordnungswidrigkeitenverfahrens hat die betroffene Kanzlei zugesagt, die durch Akteneinsicht in Strafverfahren erlangten Daten dritter Personen künftig nicht in zweckwidriger Weise zur Mandantenakquisition zu verwenden.

➡ Der Zweckbindungsgrundsatz verlangt, dass Daten, die im Rahmen einer Akteneinsicht bei Ermittlungsbehörden erlangt werden, nur für die angegebenen Zwecke, zum Beispiel die Geltendmachung von Schadensersatzansprüchen, verwendet werden. Eine darüber hinausgehende Nutzung der Daten kann den Bußgeldtatbestand des § 43 Abs. 2 Nr. 1 BDSG verwirklichen.

11 Kommunales

11.1 Der neue biometrische Reisepass – Charme verloren, Sicherheit gewonnen?

Seit November 2005 werden neue Reisepässe ausgegeben, auf denen das Gesichtsbild elektronisch auf einem RFID-Chip gespeichert wird. Ab November 2007 soll die Aufnahme von Fingerabdrücken folgen. Diese Neuerungen wurden in Deutschland sehr viel früher eingeführt, als es europarechtlich gefordert war.

"Lächeln verboten!" heißt es seit November 2005 für alle, die ein Passbild für ihren neuen Reisepass anfertigen lassen wollen. Denn in der in Ausgestaltung der europäischen Reisepassverordnung aus dem Jahr 2004 erlassenen neuen Passmusterverordnung ist nicht nur genauestens geregelt, wie der Kopf bei Aufnahme des Lichtbilds gehalten werden muss, sondern es werden Details bis hin zum Gesichtsausdruck festgelegt.

Dahinter steht die Einführung sogenannter "biometrischer Reisepässe". Biometrie ist nach dem Duden die Zählung und Körpermessung von Lebewesen. Doch anders, als es der neue Begriff vermuten lässt, besteht die Neuerung nicht in der Einführung biometrischer Merkmale in Reisepässen: Diese gab es auch bisher schon, denn hierzu zählen Gesichtsbild ebenso wie Körpergröße und Unterschrift. Neu ist hingegen – neben der Einführung des elektronischen Fingerabdrucks Ende 2007 – vor allem die Art der Speicherung: Das Gesichtsbild wird zusätzlich zu dem vom menschlichen Auge erkennbaren Foto elektronisch auf einem kontaktlos auslesbaren Chip gespeichert. Um die so gespeicherten Gesichtsbilder besser vergleichen und künftig auch Gesichtserkennungsprogramme darauf anwenden zu können, ist es erforderlich, sie zu standardisieren. Dafür muss das Gesicht aus einem ganz bestimmten Winkel, ohne störende Accessoires, weder durch Frisuren oder Kleidung bedeckt noch durch Grimassen oder eben ein Lächeln "verzerrt" aufgenommen werden. Das gewinnende Lächeln wurde somit dem vermessenen Gesicht geopfert. Warum?

Begründet wird die Einführung mit einer Verbesserung der Fälschungssicherheit der – ohnehin bereits höchst fälschungssicheren – deutschen Ausweispapiere und dem Sicherheitsgewinn, der darin liege, die

auf dem Chip gespeicherten Daten der Passinhaberin oder des Passinhabers künftig elektronisch mit der Person vergleichen zu können, die das Dokument im Rechtsverkehr verwendet. Biometrische Verfahren sollen so bei der Authentifizierung von Personen helfen, können aber auch als Überwachungs- und Kontrollinstrument, zum Beispiel für die Erstellung von Bewegungsprofilen, dienen (siehe hierzu Bericht 2003 unter 3.2). Die Datenspeicherung auf unbemerkt auslesbaren RFID-Chips (siehe hierzu Bericht 2005 unter 2.1) birgt darüber hinaus die Gefahr eines unbefugten Zugriffs auf die digitalen Daten. Hiergegen sollen zwar Verfahren zur Verschlüsselung der Daten und zur Authentifizierung der Lesegeräte schützen, Presseberichte aus jüngster Zeit über Hacker, die Chips kopieren, zeigen jedoch, dass diese Gefahr durchaus keine abstrakte ist, und angesichts der rasanten technischen Entwicklung könnten die Sicherheitsstandards im Laufe der zehnjährigen "Lebensdauer" der Pässe bald überholt sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben wiederholt vor einer überstürzten Einführung der biometrischen Pässe gewarnt, bevor die Technik inklusive der Schutzvorkehrungen gegen unberechtigte Zugriffe hinreichend ausgereift und erprobt ist (siehe Entschließungen im Anhang des Berichts 2003 sowie im Anhang dieses Berichts). Das neue Kontrollverfahren, für welches die Passkontrollstellen noch mit den erforderlichen Lesegeräten ausgerüstet werden müssen, ist für die Betroffenen mit erheblichen Nachteilen verbunden. Aufgrund der zu erwartenden Falschabweisungsraten, die die neue Technik mit sich bringt, wird ein nicht genau bestimmbarer Prozentsatz bei den Kontrollen "aussortiert" werden und sich einer genaueren Prüfung unterziehen müssen, so als ob ein Passmissbrauch vorläge. Diese diskriminierende Wirkung wird sich durch Einführung der Fingerabdrücke noch verstärken, da nach Schätzungen etwa 2% der Bevölkerung keine aussagekräftigen Fingerabdrücke besitzen oder die Fingerabdrücke sich nach Passausstellung durch Krankheit oder bestimmte körperliche Arbeiten verändert haben. Aber auch dort, wo das Verfahren funktioniert, birgt es zahlreiche Gefahren und Nachteile für die Betroffenen. Die ausschließliche Nutzung der Daten zur hoheitlichen Passkontrolle ist bisher nicht gewährleistet. Versuche wie das Pilotprojekt am Mainzer Hauptbahnhof zeugen zum Beispiel von Bestrebungen, digitale Gesichtsbilder mittels Gesichtserkennungsprogrammen zur elektronischen Überwachung von Menschenmassen mit Videokameras einzusetzen. Zur Erstellung von Bewegungsprofilen über

Einzelpersonen ist es dann ebenfalls nicht mehr weit. Die Dimension künftiger legaler und illegaler Verwendungsmöglichkeiten der Daten ist schon aufgrund der enormen Zahl autorisierter Lesegeräte, die weltweit zum Einsatz kommen werden, unübersehbar. Die Gefahr ist vor allem dann besonders groß, wenn Kontrollbehörden in Ländern mit niedrigem Datenschutzniveau Leseberechtigungen erhalten. Angesichts der großen Gefahren von Zweckänderung und missbräuchlicher Verwendung ist es besonders unglücklich, dass auf den Chips die vollständigen Rohdaten gespeichert werden, anstatt sie durch Verwendung von Templates und Einwegfunktionen so zu verfremden, dass kein Rückschluss auf das komplette Gesichtsbild oder den vollständigen Fingerabdruck möglich ist.

Da für die Passkontrolle nur ein Abgleich mit auf dem Chip gespeicherten Daten erfolgt, ist eine zusätzliche Speicherung der biometrischen Daten außerhalb des Passes nicht erforderlich. Die Errichtung einer zentralen externen Referenzdatei wäre nach deutschem Recht bisher auch nicht zulässig. Die Schaffung einer solchen Referenzdatei mit biometrischen Daten war von der Europäischen Kommission jedoch ursprünglich als ein Ziel der erwähnten Verordnung bezeichnet worden, so dass ihre Errichtung auf europäischer Ebene nicht auszuschließen ist. Damit wäre auch die Entwicklung der biometrischen Daten zu einheitlichen Personenkennzeichen, die eine Verknüpfung von personenbezogenen Informationen aus verschiedensten Bereichen ermöglichen, kein unrealistisches Szenario mehr. Derartige einheitliche Personenkennzeichen sind vom Bundesverfassungsgericht jedoch bereits in einem Grundsatzurteil aus dem Jahr 1983 (BVerfGE 65, 1/53) für verfassungswidrig erklärt worden.

- Mit den biometrischen Pässen und Personalausweisen werden weitere Bausteine zum Entstehen einer Überwachungsinfrastruktur geliefert. Der behauptete Sicherheitsgewinn durch die neuen Ausweisdokumente ist mehr als zweifelhaft, wohingegen der Verlust für unsere Freiheitsrechte sicher ist.

11.2 Was hat die SCHUFA mit der Gastfreundschaft zu tun?

Wer eine Ausländerin oder einen Ausländer nach Deutschland einlädt, muss sich häufig im Rahmen einer Verpflichtungserklärung nach § 68 Aufenthaltsgesetz (AufenthG) zur Sicherstellung des Unterhaltes der eingeladenen Person einer Bonitätsprüfung unterziehen. Die Ausländerbehörde einer großen Kommune ist dabei besonders "gründlich" vorgegangen und forderte in vielen Fällen neben anderen Unterlagen von den betroffenen Bürgerinnen und Bürgern auch eine Selbstauskunft der SCHUFA.

Nach § 5 AufenthG setzt die Erteilung eines Aufenthaltstitels für eine Person aus dem Ausland regelmäßig voraus, dass für die Dauer des Aufenthaltes deren Lebensunterhalt gesichert ist. Häufig kann der erforderliche Nachweis nur dadurch erbracht werden, dass sich die gastgebende Person gegenüber der Ausländerbehörde verpflichtet, die Kosten für den Lebensunterhalt der ausländischen Person zu tragen. Ob die einladende Person finanziell hierzu in der Lage ist, wird von der Ausländerbehörde im Rahmen einer Bonitätsprüfung festgestellt. Regelmäßig wird hierzu die Vorlage verschiedener Unterlagen über Einkünfte und Zahlungsverpflichtungen verlangt. Zu weit geht es allerdings, wenn die Ausländerbehörde regelmäßig ergänzend zu diesen Unterlagen auch die Vorlage einer SCHUFA-Selbstauskunft fordert. Im Rahmen einer SCHUFA-Selbstauskunft werden nicht nur "harte" Negativmerkmale, wie etwa eine titulierte Forderung oder die Abgabe der eidesstattlichen Versicherung mitgeteilt. Auch andere Hinweise wie etwa die Anzahl der unterhaltenen Giro- oder Kreditkartenkonten oder ein nicht ordnungsgemäß bedienter Kreditvertrag werden übermittelt. Solche weiteren Hinweise lassen indes kaum sichere Rückschlüsse auf das für eine Verpflichtungserklärung nach § 68 AufenthG allein maßgebliche gegenwärtige wirtschaftliche Leistungsvermögen der betroffenen Person zu. Die regelmäßige Vorlage von SCHUFA-Selbstauskünften würde deshalb in vielen Fällen zu einer überflüssigen und unverhältnismäßigen Datenerhebung führen.

Um sicherzustellen, dass die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit beachtet werden, wurde mit der Kommune vereinbart, dass erstens SCHUFA-Selbstauskünfte nur in begründeten Einzelfällen und ausschließlich bei längeren Aufenthalten, etwa bei Stu-

dienaufenthalten oder Sprachkursen, in Betracht kommen können, zweitens die Möglichkeit der Beibringung einer SCHUFA-Selbstauskunft in einem erforderlichen Beratungsgespräch mit den sich verpflichtenden Personen erörtert wird und drittens die Auskunft nach Abschluss der Prüfung der betroffenen Person wieder ausgehändigt wird und keine Speicherung der Daten bei der Ausländerbehörde erfolgt.

- Die Ausländerbehörde darf im Rahmen von Verpflichtungserklärungen SCHUFA-Selbstauskünfte nur in begründeten Einzelfällen zur Bonitätsprüfung verlangen. Eine Speicherung dieser besonders sensiblen personenbezogenen Daten bei der Ausländerbehörde ist in keinem Fall erforderlich.

11.3 Novellierung des Meldegesetzes

Eine Anpassung an die geänderten rahmenrechtlichen Vorgaben des Bundes hat das Meldegesetz für das Land Nordrhein-Westfalen (MG NRW) erfahren. Im Vordergrund der Novellierung stand die Schaffung rechtlicher Grundlagen für die Nutzung elektronischer Verfahren im Meldewesen.

Wesentliche Neuerungen des im April 2005 geänderten Meldegesetzes sind etwa die zusätzliche Speicherung der vom Bundesamt für Finanzen zu vergebenden steuerlichen Identifikationsnummern (siehe hierzu Bericht 2005 unter 19.1), der Verzicht auf die bisherigen Mitwirkungspflichten der Vermieterin oder des Vermieters bei der An- und Abmeldung sowie der Wegfall der Abmeldepflicht bei einem Wohnungswechsel im Inland. Künftig hat die für die neue Wohnung zuständige Meldebehörde von sich aus die Meldebehörde des Wegzugsortes im Wege der Rückmeldung zu informieren. Nach der Vorgabe des Melderechtsrahmengesetzes soll die Rückmeldung spätestens ab dem Jahr 2007 ausschließlich auf elektronischem Weg erfolgen.

Besonders hervorzuheben ist die neu geschaffene Möglichkeit, die schon bisher nahezu voraussetzungslos zulässige einfache Melderegisterauskunft zu Name und Anschrift einer Person an private Stellen auch im Wege des automatisierten Abrufs über das Internet zu erteilen. Zur Gewährleistung der Datensicherheit müssen das Antragsverfahren und die Auskunftserteilung in verschlüsselter Form erfolgen. Die Abwicklung dieser Online-Melderegisterauskunft kann nach der

neu in das Meldegesetz eingefügten Regelung des § 34 Abs. 1c MG NRW sowohl über einen eigenen Zugang der Meldebehörde als auch über Portale erfolgen, die im Auftrag der Kommunen oder kommunaler Rechenzentren Meldedaten verarbeiten. Ein solches Portal darf die übermittelten Daten nur so lange speichern, wie es für die Abwicklung der Melderegisterauskunft erforderlich ist. Dem Portal überlassene Datenträger oder übermittelte Daten sind nach Erledigung des Antrags unverzüglich zurückzugeben, zu löschen oder zu vernichten.

Sofern eine Kommune die Möglichkeit der Online-Melderegisterauskunft eröffnet, hat sie dies öffentlich bekannt zu machen. Die Betroffenen können der Auskunftserteilung via Internet widersprechen. Auf das Widerspruchsrecht hat die Meldebehörde spätestens einen Monat vor der Eröffnung des Internetzugangs und danach mindestens einmal jährlich durch öffentliche Bekanntmachung sowie bei jeder Anmeldung hinzuweisen. Eine Reihe von Anfragen zeigen allerdings, dass solche Hinweise auf ein Widerspruchsrecht in der Praxis von vielen Bürgerinnen und Bürgern nicht wahrgenommen werden. Datenschutzfreundlicher wäre es deshalb gewesen, die neu geschaffene Online-Abfrage von der vorherigen schriftlichen Zustimmung der Betroffenen abhängig zu machen.

Erfreulich ist immerhin, dass das für den Gesetzentwurf federführende Innenministerium der Empfehlung der LDI ist, die Melderegisterauskünfte an Parteien und andere Träger von Wahlvorschlägen aus Anlass von Wahlen klarer zu fassen. Schon bisher war es zulässig, dass die Meldebehörden den Parteien und sonstigen Wahlvorschlagsträgern vor einer Wahl Auskunft über Namen und Anschriften von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Da das Meldegesetz keine näheren Bestimmungen über den Umfang der zu erteilenden Auskünfte traf, wurde die Regelung häufig überdehnt und in Einzelfällen den Parteien weit mehr als die Hälfte der Adressdaten aller Wahlberechtigten für Zwecke der Wahlwerbung überlassen. Der neugefasste § 35 Abs. 1 MG NRW begrenzt die Auskunftspflicht nunmehr auf zwei Gruppen von Wahlberechtigten, die ihrerseits nicht mehr als zehn Geburtsjahresgruppen umfassen dürfen. Die weitergehende Anregung der LDI, es bei zwei Gruppen mit jeweils maximal fünf Geburtsjahrgängen zu belassen, ist leider ebenso wenig aufgegriffen worden wie die Empfehlung, das auch für diese Datenübermittlung bereits beste-

hende Widerspruchsrecht der Betroffenen durch eine Einwilligungslösung zu ersetzen. Da – wie oben dargelegt – bloße Widerspruchsrechte der breiten Öffentlichkeit meist unbekannt bleiben, werden sich wohl bei den nächsten Wahlen wieder viele Bürgerinnen und Bürger verwundert fragen, woher die Parteien ihre Adressdaten erhalten haben.

- Das novellierte Landesmeldegesetz passt das Landesrecht an die veränderten Vorgaben des Melderechtsrahmengesetzes an und öffnet das Meldewesen für moderne Formen des eGovernment. Dabei hat der Gesetzgeber die Chance verpasst, die neu geschaffene Online-Melderegisterauskunft sowie die Übermittlung von Daten an Parteien für Zwecke der Wahlwerbung an die Einwilligung der Betroffenen zu knüpfen und damit das Grundrecht auf informationelle Selbstbestimmung zu stärken.

11.4 Bürgerschreiben weltweit abrufbar

Tagesordnungen der Räte und Ausschüsse, aber auch die zur Vorbereitung von der Verwaltung erstellten Vorlagen sind häufig nicht nur für die Mitglieder der kommunalen Vertretungen, sondern auch für die Öffentlichkeit von Interesse. Nicht selten erhalten die Mitglieder der kommunalen Vertretungen die Vorlagen nicht nur in Papierform, sondern Städte und Gemeinden stellen diese Informationen auch auf der Homepage ihrer Kommune zum Abruf im Internet bereit. Eine gute Sache, wenn dabei der Datenschutz nicht zu kurz kommt.

Das ist leider nicht immer der Fall, wie die zunehmende Anzahl von Beschwerden zeigt. So war ein Bürger sehr erstaunt, als er seinen Antrag, den er in einer verkehrsrechtlichen Angelegenheit an seine Stadtverwaltung gerichtet hatte, wenige Tage später eingescannt auf der Homepage seiner Kommune im Ratsinformationssystem wiederfand. Grundsätzlich gilt hier: Auch wenn die Bekanntgabe personenbezogener Daten für eine sachgerechte Beratung und Entscheidungsfindung der Rats- und Ausschussmitglieder im Einzelfall erforderlich ist (siehe hierzu Bericht 2003 unter 12.1), ist die Übermittlung personenbezogener Daten an Dritte oder sogar eine weltweite Veröffentlichung im Internet gemäß § 4 Datenschutzgesetz NRW (DSG NRW) nur zuläs-

sig, wenn sie entweder durch eine Rechtsvorschrift erlaubt ist oder die betroffene Person eingewilligt hat.

Eine Rechtsgrundlage, die generell eine Veröffentlichung der aus Anlass von Bürgeranträgen, Beschwerden, Einwendungen und ähnlichen Schreiben der Stadt bekannt gewordenen personenbezogenen Daten im Internet erlaubt, besteht nicht. Insbesondere dürften die strengen Voraussetzungen des § 16 DSG NRW, die ausnahmsweise eine Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs erlauben, nur in seltenen Einzelfällen vorliegen und noch weniger eine weltweite Veröffentlichung im Internet zulassen. Dies gilt in gleicher Weise auch für § 48 Abs. 3 Gemeindeordnung NRW (GO NRW). Der Anwendungsbereich des § 48 Abs. 3 GO NRW ist auf die Offenbarung personenbezogener Daten in der Sitzung des Rates beschränkt. Ebenso wenig kann eine generelle Veröffentlichung der aus Anlass von Bürgeranträgen der Stadt bekannt gewordenen personenbezogenen Daten im Internet aus den Regelungen des Informationsfreiheitsgesetzes NRW (IFG NRW) hergeleitet werden. Auch danach ist der Zugang zu personenbezogenen Daten nur gegeben, wenn die betroffene Person entweder eingewilligt hat, oder die Voraussetzungen eines der sonstigen in § 9 Abs. 1 und 3 IFG NRW genannten Ausnahmetatbestände vorliegen.

- Internetgestützte Ratsinformationssysteme können den schnellen und unbürokratischen Zugang zu Informationen sowohl für Rats- und Ausschussmitglieder als auch für die interessierte Öffentlichkeit wesentlich vereinfachen. Personenbezogene Daten dürfen aber regelmäßig nur nach vorheriger Einwilligung der betroffenen Personen veröffentlicht werden.

11.5 Suchfähigkeit von Daten im Internet ausschließen

Das Internet ist als weltweit zugängliche Informationsquelle aus unserem Alltag nicht mehr wegzudenken. Kaum eine öffentliche oder private Stelle lässt sich die Chance entgehen, auf einer eigenen Homepage auf sich aufmerksam zu machen. Die öffentliche Verwaltung nutzt das Internet zunehmend auch, um auf möglichst einfache und kostengünstige Weise gesetzlichen Veröffentlichungspflichten nachzukommen. Das folgende Beispiel macht allerdings deutlich, dass eine Veröffentlichung per-

sonenbezogener Daten im Internet mit besonderen Gefahren verbunden ist.

Das am 1. März 2005 in Kraft getretene Korruptionsbekämpfungsgesetz (KorruptionsbG) verpflichtet Ratsmitglieder dazu, eine Reihe sensibler Daten auch öffentlich bekannt zu machen. Dazu gehören nach § 17 KorruptionsbG etwa der ausgeübte Beruf oder Beraterverträge, die Mitgliedschaft in bestimmten Aufsichtsgremien oder auch Funktionen in Vereinen.

Auch wenn die gesetzlichen Regelungen dies nicht zwingend vorschreiben, wird in der Praxis häufig die Homepage einer Kommune als Medium für die Veröffentlichung genutzt. Eine suchfähige Veröffentlichung personenbezogener Daten im Internet birgt indes besondere Risiken für das Grundrecht auf informationelle Selbstbestimmung, deren sich häufig weder die veröffentlichende Stelle noch die Betroffenen bewusst sind. Dies gilt insbesondere dann, wenn über eine Person verschiedene Informationen in das Internet eingestellt sind, etwa über das politische Engagement in einer Partei und in Volksvertretungen, ehrenamtliche Tätigkeiten in Vereinen, Verbänden, Kirchen, Schulen oder über berufliche und wirtschaftliche Aktivitäten oder Freizeitaktivitäten in sportlichen oder sonstigen Bereichen. Interessierten Dritten, etwa potentiellen Arbeitgeberinnen oder Arbeitgebern, ist es dann ein Leichtes, die verschiedenen Informationen mit Hilfe gängiger Suchmaschinen zusammenzutragen, um sich in kürzester Zeit ein mehr oder weniger vollständiges, häufig aber auch verzerrtes Bild von der Persönlichkeit der betroffenen Person zu verschaffen, ohne dass diese auch nur Kenntnis davon erhält. Die damit einhergehende Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung geht regelmäßig weit über den Zweck einzelner gesetzlicher Veröffentlichungspflichten hinaus.

Schon im Bericht 2005 unter 17.3 ist deshalb mit Blick auf bereits bestehende Veröffentlichungspflichten in der Gemeindeordnung empfohlen worden, durch geeignete technische Maßnahmen eine suchfähige Veröffentlichung im Internet auszuschließen. Dies gilt nunmehr umso mehr für die weitergehenden Veröffentlichungspflichten nach dem Korruptionsbekämpfungsgesetz, aber auch generell für die Veröffentlichung personenbezogener Daten durch andere private oder öffentliche Stellen. Technisch bietet sich hierfür an, eine Datei zu erstellen, die Suchmaschinen dazu veranlasst, bestimmte Seiten, Dateien oder auch

ganze Verzeichnisse nicht aufzusuchen und zu indizieren. Eine solche Datei fußt auf dem Robots Exclusion Protocol und muss robots.txt (Kleinschreibung beachten) heißen. Ferner muss sie im Hauptverzeichnis des Servers stehen. Einzelheiten hierzu können auf der Homepage der LDI NRW abgerufen werden (www.ldi.nrw.de).

- Eine suchfähige Veröffentlichung personenbezogener Daten im Internet birgt besondere Gefahren für das Persönlichkeitsrecht der betroffenen Personen. Es wird deshalb empfohlen, eine Auswertung durch einfache technische Lösungen zu verhindern.

12 Soziales

12.1 Hartz IV zum Ersten – Behördliche Datenschutzbeauftragte

Mit der Zusammenführung der Sozialhilfe und Arbeitslosenhilfe in einer Stelle mit zwei Trägern endete für die Betroffenen die Transparenz der Datenverarbeitung. Erste Hilfe können häufig die behördlichen Datenschutzbeauftragten leisten.

Die ARGEn sind öffentliche Stellen des Landes. Als solche haben sie die Pflicht zur Bestellung eigener behördlicher Datenschutzbeauftragter. Hierbei können grundsätzlich auch die kommunalen Datenschutzbeauftragten als externe Beauftragte bestellt werden.

- Mit Hilfe der behördlichen Datenschutzbeauftragten können Anliegen der Betroffenen schon vor Ort verfolgt und die Mitarbeiterinnen und Mitarbeiter für die Problematik sensibilisiert werden.

12.2 Hartz IV zum Zweiten – Telefonaktionen durch Call-Center

Bei Telefonaktionen stellt sich die Frage nach der für den Datenschutz verantwortlichen Stelle. Ohne schriftliche Vorabinformation können Betroffene die Berechtigung und Identität der Anrufenden kaum kontrollieren.

Zwar hat der Gesetzgeber Instrumentarien zur Verfügung gestellt, die eine Call-Center-Tätigkeit grundsätzlich ermöglichen. Die Zulässigkeit solcher Aktionen hängt jedoch von ihrer konkreten Durchführung ab. So ist etwa noch unklar, inwieweit bei Einschaltung privater Dritter bloße Datenverarbeitung im Auftrag stattfindet. In dem bekannt gewordenen Fall sollte das Call-Center abschließend Änderungen im Datenbestand vornehmen.

- Die im Gesetz formulierte "umfassende Unterstützung durch einen persönlichen Ansprechpartner" gerät bei dieser Praxis zunehmend in den Hintergrund, zumal die ARGEn ihrerseits Dritte mit der Durchführung weiterer Aufgaben wie Profiling beauftragen. Dies führt

letztlich zumindest zu mangelnder Transparenz der Datenerhebung und -verarbeitung.

12.3 Hartz IV zum Dritten – Zulässigkeit von Hausbesuchen

Seit dem 1. August 2006 ist geregelt, dass Außendienste zur Bekämpfung von Leistungsmissbrauch eingesetzt werden sollen. Damit ist jedoch keine Änderung der rechtlichen Voraussetzungen verbunden, unter denen ein Hausbesuch zulässig ist.

Wenn berechtigte Zweifel an den Angaben einer Person im Einzelfall vorliegen, kann ein Hausbesuch ein taugliches Mittel zur Sachverhaltsaufklärung darstellen. Allerdings gilt auch hier der Erforderlichkeitsgrundsatz. Da ein Hausbesuch stets einen schwerwiegenden Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in das Grundrecht auf Unverletzlichkeit der Wohnung darstellt, sollten zuvor mildere Mittel zur Aufklärung des Sachverhalts geprüft werden. So kann in der Regel den Betroffenen zunächst Gelegenheit gegeben werden, ihre Antragsdaten und -unterlagen entsprechend zu korrigieren.

Der Außendienst darf die Wohnung von Hilfebedürftigen nur mit deren wirksamer Zustimmung betreten. Lässt sich ohne Hausbesuch der relevante Sachverhalt nicht aufklären, so muss bei einer Verweigerung des Betretens der Wohnung oder des Hauses durch den Außendienst das Risiko hingenommen werden, dass Anträge auf entsprechende Leistungen gekürzt oder abgelehnt werden.

- Die Betroffenen sind umfassend über die Rechtslage, den Grund für den Hausbesuch, die Freiwilligkeit der Gewährung des Zutritts zur Wohnung und über die möglichen Folgen bei einer Weigerung zu belehren.

12.4 Hartz IV zum Vierten – Verantwortungs- und Einstehensgemeinschaft

Für die Zukunft steht kurioserweise zu erwarten, dass erwerbsfähige Hilfebedürftige von sich aus Hausbesuche zur Sachverhaltsaufklärung anbieten werden. Grund dafür ist die zum 1. August 2006 in Kraft getretene gesetzliche Vermutung

für das Vorliegen einer Verantwortungs- und Einstehensgemeinschaft insbesondere in den Fällen, in denen Personen länger als ein Jahr zusammenleben.

Dann liegt es an den Betroffenen, die gesetzliche Vermutung zu widerlegen. In dem entsprechenden Vordruck der Bundesagentur für Arbeit wird um möglichst umfassende Darlegungen und Beifügung entsprechender Nachweise gebeten. Dies wird voraussichtlich in vielen Fällen zu nicht erforderlichen Datenerhebungen in einem sehr persönlichen Bereich führen. Bedenklich erscheint zudem die Aussicht, dass sich zukünftig Mitglieder bloßer Wohngemeinschaften faktisch gezwungen sehen werden, Sozialleistungsträgern gegenüber umfassend persönliche Angaben zu machen, mit denen sie eigentlich nichts zu tun haben.

➡ Die Regelung einer Beweislastumkehr, die bereits dann greift, wenn Personen länger als ein Jahr zusammenleben, erscheint deshalb insgesamt unverhältnismäßig und überarbeitungsbedürftig.

12.5 Hartz IV zum Fünften – DV-Anwendungen

Bereits im Oktober 2004 wurde auf die bestehenden datenschutzrechtlichen Mängel der Leistungsberechnungssoftware A2LL in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder hingewiesen (siehe Anhang). 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. An diesem Zustand hat sich bis heute nichts geändert.

Der fortwährende Verstoß gegen das Sozialgeheimnis ist zudem nicht auf die Anwendung von A2LL beschränkt. Auch hinsichtlich der DV-Anwendung coArb fehlt ein Zugriffsberechtigungskonzept. Tatsächlich konnten die Beschäftigten einer jeden ARGE bundesweit unbeschränkt über die DV-Anwendung coArb die zu jeder betroffenen Person gespeicherten Daten einsehen und bearbeiten.

Unrühmliche Bekanntheit hat dabei der Fall einer "Mutter aus dem Ruhrgebiet" erlangt: Eine arbeitslose Mutter sei nicht in der Lage gewesen, der zuständigen Sachbearbeitung den Namen des Kindesvaters

mitzuteilen. Auf Nachfrage der Stelle habe die Mutter mitgeteilt, dass das Kind Ergebnis einer flüchtigen Bekanntschaft bei einem Fußballspiel sei. In der Folge seien im Vermerkfeld des DV-Programms coArb zynische Anmerkungen zur Lebensführung der betroffenen Frau eingetragen worden. Auf diesen Eintrag hatten aufgrund des fehlenden Zugriffsberechtigungskonzeptes sämtliche Beschäftigte der Bundesagentur für Arbeit wie auch sämtlicher ARGEn und mithin rund 40.000 Personen ungehindert Zugriff. Innerhalb kurzer Zeit sei der entsprechende Vermerk zum bundesweiten "Witz des Tages" geworden.

Angesichts der besonderen Dringlichkeit ist die Geschäftsführung in den ARGEn gefordert, auf einen besonders verantwortungsvollen Umgang gerade mit den grundsätzlich bedenklichen Freitextfeldern hinzuwirken. Das Arbeits- und Sozialministerium hat die ARGEn aufgefordert, in den DV-Anwendungen nur Eintragungen vorzunehmen, die für die Aufgabenerfüllung notwendig sind.

- Es steht zu hoffen, dass die nunmehr genutzte DV-Anwendung VerBIS das angekündigte aufgaben- und rollenbezogene Zugriffskonzept auch tatsächlich aufweist.

12.6 Aus JobCard wird ELENA – und eine gigantische Zentraldatei

Zukünftig sollen Daten von Arbeitnehmerinnen und Arbeitnehmern, welche für die Bewilligung von Arbeitslosengeld sowie weiterer Sozialleistungen erforderlich sein können, den zuständigen Stellen in elektronischer Form zur Verfügung gestellt werden. Damit seien Kosteneinsparungen auf Arbeitgeberseite verbunden, weil die Archivierung und Ausstellung schriftlicher Bescheinigungen entfiele.

Um dieses Ziel zu erreichen, sollen 30 bis 40 Millionen Menschen in das Verfahren eingebunden werden. Die entstehende zentrale Datensammlung ist für die jeweils betroffene Person jedoch nur dann überhaupt von Relevanz, wenn sie tatsächlich einen Antrag auf Leistungen stellt. Die Gefahr des Missbrauchs dieser einzigartigen Datensammlung soll zur Verfahrensbeschleunigung hingenommen werden. Es bestehen aber grundsätzliche Bedenken an der Verhältnismäßigkeit dieser Verfahrensweise.

Die Einkommensdaten aller abhängig Beschäftigten oder Auszubildenden, unabhängig davon ob es sich um Beamtinnen und Beamte, Arbeiterinnen und Arbeiter oder Angestellte handelt, sollen bis zur Beendigung des Beschäftigungsverhältnisses Monat für Monat an eine zentrale Speicherstelle elektronisch übermittelt werden (elektronischer Einkommensnachweis, ELENA).

Das Problem dieses vormals JobCard genannten Projekts besteht in der Schaffung einer gigantischen Datensammlung, die in vielen Fällen für den gesetzlich vorgesehen Zweck nicht benötigt wird. Millionen von Daten würden monatlich übermittelt, gespeichert und wieder gelöscht werden, ohne dass während des Speicherzeitraums überhaupt ein Antrag auf Arbeitslosengeld oder auf eine der anderen erfassten Leistungen gestellt wurde.

➡ Der Gesetzgeber ist gefordert, sich mit den verfassungsrechtlichen Bedenken an der Verhältnismäßigkeit einer derartigen gigantischen Datensammlung und auch der Gefahr der nachträglichen Zweckerweiterung auseinander zu setzen.

12.7 Abrechnungskontrolle der Pflegedienste

Mit der Begründung, fehlerhaften Abrechnungen von Pflegediensten anders nicht auf die Spur zu kommen, haben die gesetzlichen Kranken- und Pflegekassen immer wieder Zugriff auf die Pflegedokumentation ihrer Versicherten genommen. Dabei ist eine Rechtsgrundlage für diese Vorgehensweise nicht vorhanden.

Die Nutzung der Pflegedokumentationen kann jedoch auch unter Wahrung der Datenschutzrechte der betroffenen Pflegebedürftigen erfolgen: Bei Zweifelsfragen hinsichtlich der vorgelegten Abrechnung eines Leistungserbringers wird dieser aufgefordert, einen Nachweis zu erbringen, der unter Nutzung der Angaben in der Pflegedokumentation erstellt wird. Die Richtigkeit der Angaben aus der Pflegedokumentation wird durch die Unterschrift der vor Ort eingesetzten Pflegekraft ausdrücklich bestätigt.

➡ Damit dürfte ein Auseinanderfallen der Angaben in der Pflegedokumentation und in den Unterlagen, die zur Erstellung der vorgelegten Rechnung gedient haben,

im Regelfall zu vermeiden sein. Ein Zugriff auf die Pflegedokumentation durch den jeweiligen Sozialleistungsträger ist danach nicht mehr erforderlich.

12.8 Mitgliederwerbung ja, aber legal!

Bei der Werbung neuer Mitglieder hat eine Krankenkasse die Grenzen der Legalität überschritten.

Eine große gesetzliche Krankenkasse hatte ihre Mitarbeiterinnen und Mitarbeiter eindringlich zu besonderer "Kreativität" bei der Werbung neuer Mitglieder aufgefordert. Die Beschäftigten sollten Adressen für potentielle Mitglieder unter anderem aus ihrem Verwandten- und Bekanntenkreis, aus Klassen- und Vereinslisten oder aus Wählerverzeichnissen beschaffen. Gegenstand der Eingabe war die Beschaffung und Verwendung einer Liste von Erstwählerinnen und -wählern, wie sie im Zusammenhang mit der Kommunalwahl von einer Stadt erstellt wurde.

➡ Die Krankenkasse konnte im Ergebnis dazu bewegt werden, von einer derartigen Datenerhebung zur Mitgliederwerbung Abstand zu nehmen.

13 Gesundheit

13.1 Die elektronische Gesundheitskarte – Fluch oder Segen?

Die elektronische Gesundheitskarte und die damit verbundene Telematikinfrastruktur werden von ihren Befürwortern und Befürworterinnen als ein Allheilmittel angepriesen. Mit ihr sollen Doppeluntersuchungen vermieden, die Behandlungsqualität durch schnell verfügbare Gesundheitsdaten verbessert, Arbeitsabläufe optimiert oder auch die Wirtschaftlichkeit verbessert werden. Gleichzeitig soll die elektronische Gesundheitskarte die Rechte und die Eigenverantwortung der Versicherten stärken. Aber ist das wirklich so? Oder gibt es vielleicht unerwünschte Nebenwirkungen?

Das elektronische Rezept ist die erste Anwendung, die auf Basis der elektronischen Gesundheitskarte realisiert werden soll. Ziel ist die Beseitigung des Medienbruchs in den Apotheken. Das Papierrezept, das Sie heute in der Apotheke einreichen, kann nämlich nicht so einfach abgerechnet werden. Da die Abrechnung mit den Krankenkassen elektronisch erfolgt, müssen die Apotheken die Rezepte zunächst an Apotheken-Rechenzentren schicken, die die Rezepte einscannen und dann als elektronische Dateien bereitstellen. Diese Vorgehensweise verursacht unnötige Kosten und ist zudem zeitintensiv. In Zukunft soll es nun so sein, dass Ihre Ärztin oder Ihr Arzt die Rezepte entweder direkt auf der elektronischen Gesundheitskarte abspeichert oder auf einem Server hinterlegt, verbunden mit einer auf der Karte gespeicherten Referenz auf den Speicherort des Rezepts. Mit der Gesundheitskarte gehen Sie dann in eine Apotheke, stecken sie dort in ein Kartenlesegerät und das Apothekenpersonal kann Ihre Rezepte einlösen. Da der Apotheke nun die Rezeptdaten in elektronischer Form vorliegen, kann sie unmittelbar mit den Krankenkassen abrechnen.

Soweit, so gut. Bei dieser Lösung ergeben sich allerdings zwei Probleme. Das erste Problem besteht in der Lösung der Frage, wie die Rechte der Betroffenen gewährleistet werden können. Durch das Recht auf informationelle Selbstbestimmung hat jede Person das Recht, den Inhalt eines sie betreffenden Rezepts zu erfahren und selbst zu bestimmen, welches verordnete Medikament von welcher Apotheke bezogen wird. Außerdem darf sie das Rezept löschen oder die Berichti-

gung von Rezeptdaten veranlassen. Beim Papierrezept ist dies alles kein Problem. Der Inhalt eines Papierrezepts ist lesbar. Löschen heißt, Sie zerreißen und entsorgen das Rezept. Wenn Sie Medikamente in verschiedenen Apotheken besorgen möchten, bitten Sie Ihre Ärztin oder Ihren Arzt, Ihnen für jedes Medikament ein separates Rezept auszustellen. Müssen Daten Ihres Rezepts korrigiert werden, können Sie das fehlerhafte oder unvollständige Rezept vorlegen und es wird Ihnen ein neues ausgestellt.

Wie geht das aber, wenn das Rezept in elektronischer Form auf der Gesundheitskarte oder einem Server gespeichert ist? Elektronische Daten sind mit den menschlichen Sinnen nicht unmittelbar wahrnehmbar. Hierfür werden technische Hilfsmittel benötigt. Solche Hilfsmittel sollen zukünftig Patiententerminals sein. Ein Patiententerminal ist in etwa vergleichbar mit einem Bankautomaten. Wenn Sie bei einem solchen Terminal Ihre Gesundheitskarte in den Leseschlitz einführen und die Ihnen zugewiesene PIN (wahrscheinlich eine sechsstellige Nummer) eingeben, werden Ihnen die für Sie aktuell vorliegenden Rezepte angezeigt und zwar für jedes verordnete Medikament ein separates Rezept. Löschen können Sie nun ein Rezept, indem Sie es mit den vom Terminal bereitgestellten Funktionen zunächst markieren und anschließend den Löschknopf drücken. Die Auswahl von Medikamenten für unterschiedliche Apotheken ist schon schwieriger. Hierfür müssen Sie zunächst diejenigen Medikamente markieren, die Sie nicht in der Apotheke einlösen wollen, die Sie zuerst aufsuchen wollen. Dann betätigen Sie den Knopf für das Verbergen von Rezepten. Die zuvor ausgewählten Rezepte sind damit nicht mehr sichtbar. Wenn Sie nun die erste Apotheke aufsuchen und dort Ihre Gesundheitskarte vorlegen, kann das Apothekenpersonal nur die Medikamente sehen, die Sie nicht verborgen haben. Möchten Sie anschließend die noch nicht eingelösten Medikamente in einer zweiten Apotheke abholen, müssen Sie vorher wieder ein Patiententerminal aufsuchen, um Ihre verborgenen Rezepte wieder sichtbar zu machen. Danach können Sie die Rezepte einlösen. Nun zur Rezeptkorrektur. Angenommen Sie schauen sich an einem Patiententerminal Ihre Rezepte an und stellen fest, dass Ihnen nur 50 Tabletten eines bestimmten Medikaments verschrieben wurden, obwohl Ihnen der Arzt oder die Ärztin eine Packung mit 100 zugesagt hat. Wie können Sie nun eine Berichtigung des Rezepts veranlassen? Zunächst müssten Sie doch Ihren Arzt oder Ihre Ärztin auf den Fehler hinweisen. Die gehen aber sicherlich nicht mit Ihnen zu einem Patien-

tenterminal, um sich von dem Fehler zu überzeugen. Wenn Sie Glück haben, ist das Rezept noch im Praxiscomputer gespeichert. Wird Ihnen nun ein neues Rezept mit der 100er Packung ausgestellt, ist das alte aber noch auf dem Server beziehungsweise auf Ihrer Gesundheitskarte. Sie könnten jetzt zwei Rezepte einlösen. Also wieder zum Patiententerminal und das fehlerhafte Rezept löschen. Woher wissen aber Ihr Arzt oder Ihre Ärztin, dass Sie es wirklich gelöscht haben? Sie sehen, es wird schwierig. Wie solche Probleme praktisch zu lösen sind, ist von denjenigen, die die Systemarchitektur entwerfen, noch nicht beantwortet worden.

Zurück zum Ausgangspunkt. Das Recht auf informationelle Selbstbestimmung ist nur dann gewährleistet, wenn es auch faktisch von allen ausgeübt werden kann. Glauben Sie, dass ein Patiententerminal ein geeignetes Mittel zur Gewährleistung der Patientenrechte sein kann? Was ist mit älteren Menschen, was mit Behinderten? Was ist mit Menschen, die aufgrund ihrer Erkrankung eingeschränkt sind? Kommen sie damit zurecht? Verschärfend kommt hinzu, dass das elektronische Rezept für etwa 60 Millionen Pflichtversicherte verbindlich sein wird. Darüber hinaus stellt sich die Frage, wie diejenigen, die solche Lösungen befürworten, zum Behindertengleichstellungsgesetz stehen? Sie erinnern sich, die elektronische Gesundheitskarte soll die Rechte und Eigenverantwortung der Versicherten stärken.

Abgesehen von diesen Aspekten bleibt noch das angesprochene zweite Problem. Die elektronische Gesundheitskarte ist nicht geeignet, alle in der Praxis vorkommenden Anwendungsfälle abzubilden. Elektronische Rezepte können bei Hausbesuchen nicht ausgestellt werden. Eine telefonische Bestellung eines Wiederholungsrezepts dürfte auch nicht möglich sein, da zur Abspeicherung der Daten Ihre Karte benötigt wird. Wie die Rezeptausstellung ablaufen soll, wenn Sie nicht selbst in die Praxis gehen, sondern Ihren Mann oder Ihre Frau schicken, ist auch noch nicht geklärt. Ebenso wenig ist klar, wie Rezeptausstellung und Einlösung für Patientinnen und Patienten in Pflegeheimen bewerkstelligt werden wird. Darüber hinaus muss immer mit Ausfällen der Technik gerechnet werden. Als Notfalllösung soll dann wieder auf das Papierrezept zurückgegriffen werden. Dies bedeutet aber, dass das elektronische Rezept das Papierrezept nicht ersetzen kann. Es werden immer zwei Verfahren parallel betrieben werden müssen: Das elektro-

nische Verfahren und das Papierverfahren. Ob dies eine sinnvolle und wirtschaftliche Lösung ist, bleibt fraglich.

Dabei gäbe es eine einfache Lösung. Das Papierrezept bleibt erhalten und es werden nur zusätzlich die abrechnungsrelevanten Daten in Form eines Barcodes auf das Rezept gedruckt. In der Apotheke kann der Barcode mit einem Barcodescanner eingelesen werden, so wie es zur Erfassung der Medikamentenpreise sowieso schon geschieht. Damit stünden die Abrechnungsdaten der Apotheke in elektronischer Form zur Verfügung, was ja der eigentliche Zweck des elektronischen Rezepts sein soll.

- Die elektronische Gesundheitskarte wird noch eine Reihe von Problemen nach sich ziehen. Es ist zu befürchten, dass die Nebenwirkungen stärker sind als die Heilungseffekte. Dies zeichnet sich bereits für die einfachste Anwendung, für das elektronische Rezept, ab. Die elektronische Patientenakte stellt bei weitem höhere Anforderungen. Es bleibt zu hoffen, dass die in den Testregionen durchzuführenden Tests die Schwächen ans Licht bringen. Akzeptabel kann eine technische Lösung nur dann sein, wenn sie praktikabel, datenschutzgerecht und allen barrierefrei zugänglich ist.

13.2 "Herrenlose" Patientenunterlagen

In Kellern, verlassenen Wohnungen und Containern gefundene Patientenunterlagen aus Arztpraxen, die aus verschiedenen Gründen ohne eine Nachfolgeregelung aufgegeben wurden, warfen in der Vergangenheit nicht nur in Nordrhein-Westfalen Probleme auf.

Nach Sicherstellung der Patientenakten durch die Ordnungsbehörden blieb die Frage nach der Verantwortung für eine sichere Verwahrung der höchstsensiblen Unterlagen mangels einer gesetzlichen Regelung zunächst offen. Nunmehr hat das Gesundheitsministerium klargestellt, dass die Ärztekammern in Nordrhein-Westfalen freiwillig Patientenunterlagen und –dateien von aufgegebenen Arztpraxen übernehmen und aufbewahren, wenn die bisherigen Praxisinhaberinnen und –inhaber sie nicht selbst aufbewahrt oder in gehörige Obhut gegeben haben.

➡ Ein gesetzlicher Regelungsbedarf ist mit dieser Zusage – zumindest vorläufig – nicht mehr gegeben.

13.3 Deine, meine, unsere Patientinnen und Patienten

Immer mehr Ärztinnen und Ärzte entscheiden sich für eine gemeinsame Berufsausübung, deren Formen in der Berufsordnung definiert werden. Den Zusammenschluss besiegelt meist ein umfangreiches Vertragswerk. Eine Vereinbarung, wie im Hinblick auf den Patientenbestand bei einer Auflösung der Gemeinschaft verfahren werden soll, ist allerdings selten vorgesehen.

Es ist zwingend notwendig, ein Datenschutz- und Sicherheitskonzept zu erstellen, das den Zugriff auf die jeweiligen Patientendaten regelt und den Zugriff auf einzelne Datensätze nachvollziehbar dokumentiert. Zu Schwierigkeiten bei der Auflösung von Berufsausübungsgemeinschaften kann es kommen, wenn sich in der gemeinsam genutzten EDV die Daten "deiner, meiner, unserer Patientinnen und Patienten" mischen. Erfolgt die Trennung nicht einvernehmlich, eindeutig und unter Wahrung der Datenschutzbelange der Betroffenen, müssen nicht selten Gerichte nachhelfen, wenn die Unterlagen der "eigenen" Patientinnen und Patienten aus den Datenbeständen der Berufsausübungsgemeinschaft herausgelöst werden sollen. Gelegentlich macht auch die verwendete Software Schwierigkeiten, getrennte Datenbestände zu erzeugen.

➡ Bei der Gründung einer gemeinsam geführten Praxis ist ein Datenschutz- und Datensicherheitskonzept unverzichtbar.

13.4 Aber ich bin mit meiner Krebsvorsorge zufrieden!

Für die Einladung zur freiwilligen Teilnahme am bundesweit angebotenen Mammographie-Screening übermitteln die Meldebehörden in Nordrhein-Westfalen den bei den Kassenärztlichen Vereinigungen dafür eingerichteten Zentralen Stellen monatlich personenbezogene Daten aller Einwohnerinnen, die an einem bestimmten Stichtag das 50. Lebensjahr vollendet und das 70. Lebensjahr noch nicht vollendet haben.

Das Angebot richtet sich in der Hauptsache an gesetzlich versicherte Patientinnen, da die Kosten für ein Mammographie-Screening von den gesetzlichen Krankenkassen bisher nicht erstattet wurden. Die Teilnahme ist im Übrigen im Hinblick auf die Vorsorgeuntersuchungen nach § 25 Abs. 2 Sozialgesetzbuch Fünftes Buch freiwillig.

Durch die pauschale Übermittlung der Datensätze erhalten auch Frauen eine Einladung, die privat versichert sind und an der gewohnten ärztlichen Behandlung und Betreuung festhalten wollen und Frauen, die diese Form der Untersuchung von vornherein ablehnen. Dies gilt auch für die gesetzlich versicherten Frauen, die sich mit der allgemeinen Krebsvorsorge begnügen wollen.

Die Möglichkeit, die in diesen Fällen nicht erforderliche Datenübermittlung von Anfang an zu unterbinden, hat dieser Personenkreis allerdings nicht. Die betroffenen Frauen müssen es vielmehr hinnehmen, dass ihre Meldedaten 20 Jahre lang regelmäßig der Zentralen Stelle übermittelt werden. Dieses überflüssige Verfahren verstößt nicht nur gegen den Erforderlichkeitsgrundsatz, sondern auch gegen den Grundsatz der Datenvermeidung und Datensparsamkeit.

Den betroffenen Frauen sollte daher entweder zunächst eine generelle Einwilligung in die vorgesehene Datenübermittlung von der Meldebehörde an die Zentrale Stelle abverlangt werden (die entsprechende Erklärung wäre von den jeweiligen Meldebehörden einzuholen) oder zumindest ein Widerspruchsrecht gegen die Übermittlung ihres Datensatzes an die Zentrale Stelle gegenüber den Meldebehörden eingeräumt werden.

Bis zur Schaffung ergänzender gesetzlicher Bestimmungen könnte bereits im Vorgriff durch öffentliche Bekanntmachung in den Kommunen auf ein solches Widerspruchsrecht hingewiesen werden. Von den Kommunen wäre weiter sicherzustellen, dass Widersprüche vor der nächstfolgenden Datenübermittlung berücksichtigt werden.

➧ Das Verfahren ist datenschutzkonform umzugestalten.

13.5 Datenerhebung für das Krebsregister – ärztliches Personal ist gefragt

Nach den Bestimmungen des Gesetzes zur Einrichtung eines flächendeckenden bevölkerungsbezogenen Krebsregisters in

Nordrhein-Westfalen sind Ärztinnen und Ärzte, die Krebserkrankungen diagnostizieren oder behandeln, verpflichtet, die Daten für das Krebsregister gemäß der gesetzlich bestimmten Meldewege zu übermitteln.

Eine Klinik sah in dieser Vorschrift eine unzumutbare Belastung des ärztlichen Personals und schlug folgende Lösung vor:

Die Ärztinnen und Ärzte holen die Einwilligungen der Erkrankten für eine Aufnahme in das Krebsregister ein und dokumentieren die Einwilligungen auf dem jeweiligen Aufklärungsbogen. Den Aufklärungsbogen erhält das Krankenhaus, das sich aus dem Krankenhausinformationssystem den dazu passenden Arztbrief heraussucht. Aus dem Arztbrief entnimmt es die Informationen, die anschließend zur Einstellung in das Krebsregister übermittelt werden.

Ein solches Vorgehen begegnet erheblichen datenschutzrechtlichen Bedenken: Die Meldepflicht obliegt nicht Krankenhäusern, Arztpraxen oder sonstigen Einrichtungen, sondern dem gesetzlich definierten meldepflichtigen Personenkreis, der damit auch in der Verantwortung für den Umgang mit den hochsensiblen Patientendaten und deren Schutz steht. Sobald diese Verantwortung an nicht-ärztliches Personal weitergegeben wird, fehlt dafür die erforderliche gesetzliche Grundlage.

➡ Die gesetzliche Regelung ist eindeutig: Die Meldepflicht ist nicht beliebig delegierbar. Derartige Planungen sind geeignet, die Akzeptanz der Datenerhebung für das Krebsregister bei den Betroffenen und damit auch Wert und Aussagefähigkeit des Registers in Frage zu stellen.

13.6 Ärztliche Fortbildung – und der Datenschutz?!

Im Rahmen der ärztlichen Fortbildung wurde ein Seminar angeboten, bei dem angekündigt wurde, dass die Bearbeitung der Themen unter anderem in Einzelgruppen an Fall- und Gutachtenvorlagen, praktischer Untersuchung und Befundung, Auswertung der Unterlagen und anderem mehr erfolgen solle.

Den Seminarteilnehmerinnen und Seminarteilnehmern waren dafür von einem Sozialleistungsträger stammende Unterlagen überlassen worden, in denen der Personenbezug nicht zuverlässig, etwa durch Schwärzen, beseitigt worden war. Dadurch war es den Seminarteil-

nehmerinnen und Seminarteilnehmern möglich, Daten des Sozialleistungsträgers und der betroffenen Sozialversicherten einzusehen, die durch das Sozialgeheimnis (§ 35 Sozialgesetzbuch Erstes Buch) besonders geschützt waren.

➡ Der Veranstalter hat zugesichert, zukünftig derartige Seminarunterlagen sicher zu anonymisieren und auch im Übrigen das Seminar datenschutzkonform durchzuführen.

14 Beschäftigtendatenschutz

14.1 Whistleblowing-Hotlines: Ein Beitrag zur Korruptionsbekämpfung

Unternehmen sind verstärkt daran interessiert, "Whistleblowing-Hotlines" einzusetzen, um frühzeitig an Informationen zu gelangen, die dem Unternehmensinteresse schaden könnten.

Der Begriff Whistleblower bezeichnet Personen, die ethisch motiviert "Alarm blasen" und ihre Arbeitgeberin oder ihren Arbeitgeber, aber auch dritte Stellen (etwa Behörden, Presse) auf illegale Praktiken und sonstige Verfehlungen hinweisen. Sie können gerade auch bei der Aufdeckung von Korruptionsdelikten erhebliche Bedeutung haben, weil das geschädigte Unternehmen ansonsten, wenn überhaupt, erst viel später vom Schadenseintritt erfährt und die Täterermittlung zu diesem Zeitpunkt erheblich schwieriger ist.

Mit der Meldung von Verstößen gegen Verhaltenspflichten gehen die Erhebung, Übermittlung und Speicherung von personenbezogenen Daten einher. Wenn diese Daten automatisiert oder in nicht automatisierten Dateien verarbeitet werden, müssen die Vorschriften des Datenschutzrechts eingehalten werden. Betroffene Personengruppen sind vor allem die Hinweisgeberinnen und Hinweisgeber sowie die Beschuldigten. Die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union haben die sich aus der europäischen Datenschutzrichtlinie ergebenden Ziele und Vorgaben in einer Stellungnahme zu Whistleblowing-Systemen zusammengefasst (abrufbar unter: www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf).

- Unter Zugrundelegung dieser Stellungnahme wird derzeit zusammen mit anderen Datenschutzaufsichtsbehörden ein Arbeitsbericht "Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz" abgestimmt. Darin werden die maßgeblichen datenschutzrechtlichen Zulässigkeitskriterien der automatisierten personenbezogenen Datenerhebung, -verarbeitung und -nutzung bei solchen Meldeverfahren dargestellt.

14.2 Lohnlisten mit Beschäftigtendaten an die Gewerkschaft?

Der Übergabe von Lohnlisten an Gewerkschaften, um deren Zustimmung zu Kostensenkungsmaßnahmen im Personalbereich zu erzielen, sind durch das Datenschutzrecht Grenzen gesetzt.

Nachdem die Belegschaft eines Unternehmens sich ganz überwiegend für die Kürzung der Jahressonderzahlung ausgesprochen hatte, entschloss sich die zuständige Gewerkschaft zu Verhandlungen über einen Firmentarifvertrag, in dem die angestrebten finanziellen Einschränkungen für die Belegschaftsmitglieder zumutbar und sozial verträglich gestaltet werden sollten. Zu diesem Zweck stellte das Unternehmen der gewerkschaftlichen Tarifkommission namentliche Listen über die Einkommenssituation der einzelnen Beschäftigten und deren sozialen Status (etwa Familienstand, Kinderzahl, Alter) zur Verfügung.

Das Unternehmen war der Ansicht, die Übermittlung auf die Regelung des § 80 Abs. 2 Satz 2 des Betriebsverfassungsgesetzes stützen zu können. Danach sind zur Einsichtnahme in die Listen über die Bruttolöhne und -gehälter bestimmte betriebliche Ausschüsse und Betriebsratsmitglieder, nicht aber gewerkschaftliche Tarifkommissionen befugt. Selbst wenn der Betriebsrat Mitglied der Tarifkommission geworden ist, muss die Zustimmung der jeweils betroffenen Beschäftigten zur Mitteilung ihrer personenbezogenen Daten durch den Betriebsrat in den Sitzungen der Tarifkommission eingeholt werden.

Überdies war die vorliegende Einsichtnahme in die Lohnlisten nicht erforderlich. Zwar benötigte die Gewerkschaft für die Entscheidung über den Abschluss des Firmentarifvertrages Angaben über die Verdienste der Beschäftigten und ihre sonstigen Daten. Allerdings hätte hierfür eine Überlassung von Daten ohne Personenbezug ausgereicht. Das Unternehmen will dies bei künftigen Verhandlungen beachten und hat die Löschung der übermittelten personenbezogenen Daten bei der Gewerkschaft veranlasst.

➡ Bei Verhandlungen über Firmentarifverträge dürfen grundsätzlich nur Lohnlisten ohne Namensnennung verwandt werden. Im Einzelfall kann die Pseudonymisierung der Beschäftigtendaten genügen.

14.3 Personalausgabenbudgetierung – nicht immer mit personenscharfen Bezügedaten

Mit der Personalausgabenbudgetierung soll überbordenden Haushaltslasten begegnet werden. Als Instrumentarium steht ein automatisierter Abruf der Bezügedaten der Beschäftigten durch die personal- und budgetbewirtschaftenden Stellen zur Verfügung.

Entsprechende Informationen dürften diese Stellen künftig häufiger benötigen, denn eine ungenaue Kalkulation der für das Haushaltsjahr zur Verfügung stehenden Personalmittel kann einer Realisierung der haushaltsgesetzlichen Ziele entgegenstehen. Es bedurfte in Nordrhein-Westfalen allerdings erst verschiedener Gespräche mit dem Finanzministerium, um die Notwendigkeit einer besonderen Rechtsgrundlage für den angestrebten Abruf von Bezügedaten beim Landesamt für Besoldung und Versorgung zu verdeutlichen. Diese ist nunmehr in haushaltsrechtlich verankert (vergleiche § 7 Abs. 4 Haushaltsgesetz 2006). Ausschließlich Bezügedaten und nicht etwa Aufwendungen für Beihilfeleistungen dürfen in eine Personalausgabenbudgetierung einfließen. Klarstellungsbedürftig ist allerdings noch, dass Abrufe von Bezügedaten nicht zum Regelfall werden dürfen.

- Falls der Zweck der Personalausgabenbudgetierung entweder unter Zugrundelegung von Personalkostendurchschnittsbeträgen oder durch Abruf aggregierter Personalkosten ebenso erreichbar ist, ist eine Verarbeitung personenscharfer Bezügedaten nicht erforderlich und auch nach dem Grundsatz der Datenvermeidung unzulässig. Die bereits für den Schulbereich erreichte Klarstellung sollte auch für die übrigen Ressorts erfolgen.

14.4 Rundfunkgebühren ohne Ende ...

Darf die Gebühreneinzugszentrale (GEZ) bei Dienststellen ermitteln, ob Landesbedienstete ihr Privatfahrzeug für Dienstreisen einsetzen und der Rundfunkgebührenpflicht unterliegen?

Dies war der Hintergrund einer Anfrage des Finanzministeriums. Das Ansinnen der GEZ, sich von Dienststellen zu diesem Zweck die

betroffenen Beschäftigten benennen zu lassen, war klar zu zurückzuweisen. Die Rechte und Pflichten der Beteiligten im Rahmen der Erhebung der Rundfunkgebühren sind im Rundfunkgebührenstaatsvertrag geregelt. Dieser enthält jedoch keine Ermächtigungsgrundlage für die GEZ, entsprechende Auskünfte von Dienststellen zu verlangen. Demnach kommt auch keine Verpflichtung von Dienststellen in Betracht, Auskünfte über Beschäftigte zur Feststellung des Vorliegens eines Rundfunkteilnehmerverhältnisses gegenüber der GEZ zu erteilen.

➡ Die GEZ hat mittlerweile von ihrem zweifelhaften Vorhaben Abstand genommen, nachdem auch das Finanzministerium auf die Rechtslage aufmerksam gemacht hat.

14.5 Qualitätsmanagement im Bereich der Beihilfe – so nicht!

Wie können Qualitätsmängel von Krankenhausrechnungen beihilfeberechtigter Personen untersucht werden? Hierzu lassen die Rechtsvorschriften gegenwärtig ausschließlich Überprüfungen durch das zuständige Gesundheitsamt zu.

Anders das Finanzministerium, das im Rahmen von Qualitätssicherungsmaßnahmen bei der Beihilfegewährung zunächst in einem Testverfahren Krankenhausrechnungen auf Übereinstimmung mit den rechtlichen Vorgaben prüfen ließ. Hierzu wurden Beihilfeberechtigte von ihrer Beihilfestelle aufgefordert, Unterlagen des Krankenhauses (Entlassungsberichte, Operationsberichte, Herzkatheder- oder Beatmungsprotokolle) beizubringen. Angekündigt wurde, dass die Festsetzung der Beihilfe bis zum Abschluss der innerhalb von drei Wochen zugesagten Prüfung zurückgestellt werde und das Krankenhaus um Gewährung von Zahlungsaufschub für vier Wochen gebeten werden solle. Falls dieser nicht eingeräumt werde, möge die Beihilfestelle benachrichtigt werden. Die Prüfung werde ein externes Dienstleistungsunternehmen übernehmen, dem die Rechnung und die angesprochenen Unterlagen anonymisiert zugeleitet würden.

Das Finanzministerium wurde darauf aufmerksam gemacht, dass weder beamtenrechtliche noch sonstige Vorschriften eine derartige Verfahrensweise erlauben. Die Aufforderung an die betroffenen Beihilfeberechtigten, die zu beschaffenden ärztlichen Behandlungsunterlagen

der Beihilfestelle zu dem beschriebenen Zweck zu überlassen, stellt einen Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung dar und beeinträchtigt den Anspruch auf Schutz ihrer personenbezogenen Daten, Art. 4 der Verfassung für das Land NRW (LV NRW). Die Beihilfeberechtigten können danach grundsätzlich und eigenverantwortlich selbst bestimmen, ob und gegebenenfalls in welchem Umfang ärztliche Behandlungsunterlagen, die von der behandelnden Ärztin oder dem behandelnden Arzt selbst nur auf Grund einer rechtswirksamen Schweigepflichtentbindungserklärung dritten Stellen überlassen werden dürften, dem öffentlich-rechtlichen Kostenträger zugänglich werden. Eingriffe in diese Rechtsposition der Betroffenen sind nach Art. 4 Abs. 2 LV NRW nur in überwiegendem Interesse der Allgemeinheit auf Grund eines Gesetzes zulässig.

Der Gesetzgeber hat die Durchführung allgemeiner Qualitätssicherungsmaßnahmen anders als in der gesetzlichen Krankenversicherung im Beihilferecht des öffentlichen Dienstes nicht vorgesehen. Unerheblich ist, dass die genannten Behandlungsunterlagen von den Beihilfeberechtigten nur an ihre Beihilfestelle übermittelt und sie von dort in anonymisierter Form einer beauftragten dritten Stelle weitergeleitet werden sollten. Ausschlaggebend ist allein der Zweck der Inanspruchnahme der Beihilfeberechtigten, der nicht von einer Rechtsvorschrift gedeckt ist. Ebenso ist es von der dienst- oder arbeitsrechtlichen Verpflichtung einer oder eines Beihilfeberechtigten nicht umfasst, zur Durchführung allgemeiner Qualitätssicherungsmaßnahmen an der Überprüfung von Krankenhausrechnungen – nach einem den Betroffenen zudem im Einzelnen nicht erläuterten Untersuchungssystem – durch Übersendung der ärztlichen Behandlungsunterlagen an die Beihilfestelle mitwirken zu müssen. Darüber hinaus bedürfte es nach § 4 Abs. 3 Satz 1 Datenschutzgesetz NRW bereits für die Testphase einer entsprechenden Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt sowie angemessene Garantien zum Schutz des Grundrechts auf informationelle Selbstbestimmung vorsieht.

Allenfalls im begründeten Einzelfall begegnete eine Aufforderung der Beihilfestelle gegenüber der beihilfeberechtigten Person keinen durchgreifenden datenschutzrechtlichen Bedenken, bestimmte ärztliche Behandlungsunterlagen etwa zur Prüfung einer unplausiblen Krankenhausabrechnung beizubringen. Mit der näheren Aufklärung wäre gegebenenfalls allein die Amtsärztin oder der Amtsarzt des zuständigen

Gesundheitsamtes im Rahmen der Aufgaben und Befugnisse nach § 24 Gesundheitsdatenschutzgesetz NRW zu betrauen.

Das Finanzministerium hält solche Qualitätssicherungsmaßnahmen auf der Grundlage von § 3 Abs. 2 Beihilfenverordnung für zulässig. Aus der Festsetzungsbefugnis der Beihilfestelle folge im Zweifelsfall auch die Berechtigung zur Erhebung zusätzlicher Angaben, wenn sich aus den vorgelegten Belegen nicht alle für eine Rechnungsprüfung notwendigen Tatbestände ergäben. Die testweise durchführte Maßnahme sei inzwischen beendet. Die angeforderten Unterlagen seien, wie ursprünglich vorgesehen, den Beihilfeberechtigten zurückgegeben worden.

Dem war mit dem Hinweis entgegenzutreten, dass zwar die Festsetzungsstelle über die Notwendigkeit und den angemessenen Umfang von Aufwendungen entscheidet, sie im Zweifelsfall jedoch nur zur Einholung eines amts- oder vertrauensärztlichen Gutachtens befugt ist. Die Beihilfenverordnung sieht allein diese Kompetenzen vor, so dass für eine Auslegung kein Raum ist, aus der Festsetzungsbefugnis der Beihilfestelle folge im Zweifelsfall auch die Erhebung zusätzlicher, überdies dem Arzt-Patientengeheimnis unterliegender Angaben. Abgesehen hiervon ist die Überprüfungsaktion nach den gleichlautenden Anschreiben der Beihilfestellen flächendeckend vorgenommen worden und hat sich damit nicht lediglich auf Zweifelsfälle erstreckt.

- Krankenhausbehandlungsunterlagen von Beihilfeberechtigten unterliegen dem Arzt-Patienten-Geheimnis. Die Übermittlung an Dritte ist grundsätzlich nur bei Vorliegen einer bereichsspezifischen gesetzlichen Grundlage zulässig. Dem Gesetz zuwider laufende Überprüfungen solcher Unterlagen wären im Wiederholungsfall förmlich zu beanstanden.

14.6 Bei Mitarbeiterbefragungen Anonymität gewährleisten

"Engagierte Mitarbeiterinnen und Mitarbeiter sind die Basis für zufriedene Kundinnen und Kunden und damit der Schlüssel des Erfolges", ist die Devise einer großen Discounterkette. Sie befragte deshalb ihre Beschäftigten zur eigenen Zufriedenheit mit

den Führungskräften und den Arbeitsabläufen, um hieraus Verbesserungsmaßnahmen abzuleiten.

Werden in Mitarbeiterbefragungen subjektive Einschätzungen und Bewertungen des Arbeitsumfeldes erfragt, besteht grundsätzlich keine arbeitsvertragliche Verpflichtung zur Teilnahme. Mitarbeiterbefragungen sind daher nur auf freiwilliger Basis zulässig. Hierauf ist bei der Erhebung eindeutig hinzuweisen. Darüber hinaus sind die Beschäftigten über Ablauf, Gegenstand und Zweck der Befragung zu informieren. Auch sollten sie darüber aufgeklärt werden, welche Auswertungen konkret vorgesehen sind.

Darüber hinaus muss die Anonymität der befragten Beschäftigten in der praktischen Umsetzung gewährleistet sein (§ 3 Abs. 6 Bundesdatenschutzgesetz). Das Gleiche gilt, wenn Mitarbeiterbefragungen Werturteile über andere Beschäftigte enthalten. Ansonsten ist die Einwilligung der von der Befragung Betroffenen erforderlich. Sollen kleine Organisationseinheiten ausgewertet werden, sind Daten zusammen zu fassen. Im Übrigen bietet sich an, die Auswertung der Fragebogen durch ein externes Institut durchführen zu lassen, das weder über das zu einer Reidentifikation erforderliche Zusatzwissen verfügt noch entsprechende Informationen erhält. Bei der Darstellung der Auswertungsergebnisse darf kein Rückschluss auf bestimmte Personen möglich sein.

➡ Bei Mitarbeiterbefragungen ist von zentraler Bedeutung, dass hieraus gewonnene Erkenntnisse keinesfalls mit anderen Personaldaten verbunden werden dürfen.

15 Finanzen

15.1 Kontenkontrollen – dokumentiert und transparent

Die Durchführung der durch das Steueränderungsgesetz 2003 eingeführten Möglichkeiten zu Kontenkontrollen wurde im Berichtszeitraum bei drei Finanzämtern stichprobenweise überprüft. Die Regelungen erlauben einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 und ursprünglich allein zum Zwecke der Terrorismusbekämpfung vorgehalten werden müssen.

Die überprüften Finanzämter hatten die ihnen obliegende Verpflichtung überwiegend nicht beachtet, die vor einem Kontenabrufersuchen nach § 93 Abs. 7 und 8 der Abgabenordnung an das Bundesamt für Finanzen (heute: Bundeszentralamt für Steuern) anzustellende Ermessensausübung in den Steuerakten zu vermerken. Auf Grund dieser Dokumentationsmängel konnte nicht nachvollzogen werden, ob die Kontenabrufe tatsächlich erforderlich waren. Auch die Darlegungen der Behördenleitungen, den Kontenabrufersuchen hätten in jedem Einzelfall Ermessensentscheidungen zugrunde gelegen, vermochten an der Notwendigkeit einer ordnungsgemäßen Dokumentation in den Steuerakten nichts zu ändern. In zahlreichen Fällen war außerdem der Transparenzgrundsatz nicht beachtet worden, weil die Betroffenen über die Kontenabrufersuchen nicht informiert worden waren. Nur vereinzelt waren Betroffene zuvor unterrichtet worden. In vielen Fällen konnte auch keine nachträgliche Unterrichtung festgestellt werden. Damit haben sich die mit solchen Abrufverfahren verbundenen datenschutzrechtlichen Risiken, wie sie bereits im Bericht 2005 unter 19.1 dargestellt wurden, bestätigt.

Das Finanzministerium hat die entsprechenden Empfehlungen zum Anlass genommen, alle Finanzämter über die datenschutzrechtlichen Erfordernisse zu unterrichten. Die bei den überprüften Finanzämtern festgestellten datenschutzrechtlichen Mängel sind zwischenzeitlich abgestellt.

➡ Gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder wurde ein Muster-Formular entwickelt, das sicherstellen kann, die bisherigen Voll-

zugsdefizite zu vermeiden. Es ist für die Finanzämter mittlerweile verbindlich.

15.2 Zweitwohnungssteuer – zuviel geschnüffelt?

Bei der Datenerhebung zur Festsetzung der Zweitwohnungssteuer hat eine Großstadt die Mitwirkungspflichten von Bürgerinnen und Bürgern an der Aufklärung des steuerlich erheblichen Sachverhalts zu arg strapaziert.

Anlass verschiedener Beschwerden war die Aufforderung der Stadt in einem Rundschreiben an Eigentümerinnen und Eigentümer von Grundstücken und Wohnungen, Mieterinnen und Mieter zu benennen, die Wohnungen als Zweitwohnungen nutzen. Dabei wurde den Angeschriebenen der Eindruck vermittelt, sie seien hierzu gesetzlich verpflichtet und ihnen drohe im Falle der Nichtmitwirkung ein Bußgeld.

Der Stadt war bekannt, dass § 12 Abs. 1 Nr. 3 lit. a des Kommunalabgabengesetzes in Verbindung mit § 93 der Abgabenordnung (AO) für Eigentümerinnen und Eigentümer von Grundstücken und Wohnungen keine Verpflichtung enthält, den steuererheblichen Sachverhalt bei ihren Mieterinnen oder Mietern selbst zu ermitteln. Sie haben allein ihrer in der Zweitwohnungssteuersatzung der Stadt verankerten Mitwirkungspflicht (als Erklärungspflichtige) zu genügen, über die bestehenden Mietverhältnisse über Wohnraum Auskunft zu erteilen und jede Beendigung, jeden Neuabschluss, jede Einbeziehung weiterer Personen in das Mietverhältnis oder das Ausscheiden von Personen aus dem Mietverhältnis mitzuteilen. Darüber hinaus zielte die Anschreibeaktion auf eine rasterfahndungsähnliche Totalerfassung aller Steuerpflichtiger der Stadt ab. Nach der Rechtsprechung des Bundesfinanzhofs bietet § 93 AO keine Rechtsgrundlage für Auskunftsverlangen im Rahmen sogenannter Rasterfahndungen oder ähnlicher Ermittlungen ins Blaue hinein (BFH, Urteil vom 18.02.1997, Az: VIII R 33/95). Die Datenerhebungen dürften bereits unter diesem Gesichtspunkt rechtswidrig gewesen sein. Darüber hinaus bestanden auch deshalb Bedenken, weil es den Vermieterinnen und Vermietern in der Regel nicht möglich oder zumindest nicht zumutbar war, inhaltlich zutreffende Auskünfte zu geben. Zudem erfordert die Angabe, ob Personen ein Wohnobjekt als Zweitwohnung nutzen, Kenntnisse der steuerrechtlichen Voraussetzungen einer solchen Nutzung. Solche sind allenfalls von den nach

der kommunalen Satzung Erklärungspflichtigen, nicht jedoch von den Adressatinnen und Adressaten des Rundschreibens zu erwarten, die insoweit selbstverständlich auch keinen Rechtsrat einzuholen brauchen. Vor diesem Hintergrund sind die in der kommunalen Satzung verankerten Mitwirkungspflichten bewusst auf die Mitteilung von Tatsachen beschränkt, die allein die Stadt zu bewerten hat. So muss davon ausgegangen werden, dass die Antworten, ob benannte Personen eine Wohnung als Zweitwohnung nutzen, in nicht quantifizierbarem Umfang spekulative oder invalide Bewertungen enthalten.

Der Stadt wurde empfohlen, die erhobenen Daten zur Wahrung des Folgenbeseitigungsanspruchs der Betroffenen zu löschen und bei künftigen vergleichbaren Erhebungen über die Mitwirkungspflicht und die zu beachtenden sonstigen gesetzlichen Vorschriften korrekt zu unterrichten.

➧ Die Kommunen sind bei der Steuererhebung gut beraten, die Betroffenen über ihre Mitwirkungspflichten richtig zu informieren. Erhebungen bei Dritten sind dabei auf Ermittlungen von Tatsachen beschränkt, deren steuerrechtliche Bewertung allein durch die zuständige Stelle in der Gemeinde vorzunehmen ist.

16 Behördliche und betriebliche Datenschutzbeauftragte

16.1 Datenschutzbeauftragte bei öffentlichen Stellen

Im Jahr 2000 wurde das nordrhein-westfälische Datenschutzgesetz (DSG NRW) grundlegend novelliert. Unter anderem wurde die Berufung einer oder eines behördlichen Datenschutzbeauftragten für alle Behörden verpflichtend. Auch wenn seither sechs Jahre vergangen sind, gibt es nach wie vor noch Unklarheiten über die Bestellpflicht.

Vor allem die kleineren öffentlichen Stellen im Lande tun sich manchmal noch etwas schwer, geeignete Datenschutzbeauftragte zu finden. Die gesetzliche Pflicht zur Bestellung von Datenschutzbeauftragten trifft unabhängig von ihrer Größe ausnahmslos alle öffentlichen Stellen im Lande. Spielräume, die auch den Bedürfnissen kleiner Behörden gerecht werden, bestehen aber bei der Umsetzung der Verpflichtung.

Der Bestellung von Datenschutzbeauftragten an Schulen ist im Kapitel Bildung und Wissenschaft unter 5.3 ein eigener Abschnitt gewidmet. Lösungen für Studienämter, die zum Teil nicht mehr als drei Beschäftigte haben, konnten über Datenschutzbeauftragte bei den Bezirksregierungen als Aufsichtsbehörden realisiert werden. Das Gesetz lässt die Bestellung einer oder eines Datenschutzbeauftragten für mehrere Behörden auch bei einer Aufsichtsbehörde grundsätzlich zu.

Öffentlich bestellte Vermessungsingenieurinnen und -ingenieure hingegen, die als Beliehene ebenfalls öffentliche Stellen des Landes sind, hatten den Wunsch, Datenschutzbeauftragte bei ihrem Bundesverband zu bestellen. Dies war nicht mehr mit dem DSG NRW vereinbar, weil der Bundesverband selbst ein privater Verein und damit keine öffentliche Stelle des Landes ist.

- Kleine öffentliche Stellen sollten die gesetzlichen Spielräume ausschöpfen. So wurde den Vermessungsingenieurinnen und –ingenieuren empfohlen, sich regional zusammenzuschließen und Datenschutzbeauftragte gemeinsam bei einem ihrer Büros zu bestellen.

16.2 Betriebliche Datenschutzbeauftragte – Konsequenzen aus der Änderung des Bundesdatenschutzgesetzes

Was die betrieblichen Datenschutzbeauftragten betrifft, war im Berichtszeitraum besonders einschneidend die Änderung der gesetzlichen Voraussetzungen für die Bestellpflicht.

Mit Inkrafttreten des "Ersten Gesetzes zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft" am 26. August 2006 haben sich die Voraussetzungen für die Bestellung betrieblicher Datenschutzbeauftragter im Bundesdatenschutzgesetz verändert. Nun sind Daten verarbeitende Stellen verpflichtet, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu bestellen, wenn in der Regel mehr als neun Personen personbezogene Daten automatisiert verarbeiten. Zuvor lag die Grenze für die Bestellpflicht bei mehr als vier Beschäftigten. Ob das im Gesetzestitel formulierte Ziel durch diese Maßnahme erreicht wird, darf bezweifelt werden. Die inhaltlichen Anforderungen an den Datenschutz bei Unternehmen der Privatwirtschaft, bei Handel, Handwerk und freien Berufen gelten unverändert in vollem Umfang fort. Es fehlt nun bei den kleineren Unternehmen die kompetente Beratung durch eigene Datenschutzbeauftragte.

Besonderes Augenmerk müssen Unternehmen ohne eigene Datenschutzbeauftragte der Meldepflicht schenken. Verarbeiten diese Unternehmen automatisiert personenbezogene Daten und geschieht dies nicht ausschließlich für eigene Zwecke oder ist die Grundlage für die Verarbeitung weder die Einwilligung der betroffenen Personen noch die Erfüllung eines Vertragsverhältnisses, dann sind die Datenverarbeitungsverfahren der LDI NRW als Aufsichtsbehörde zu melden. Eine versäumte Meldung kann als Ordnungswidrigkeit verfolgt werden.

- Die Meldung ist gerade bei kleineren Unternehmen für die Aufsichtsbehörde ein wichtiges Instrument, um die nach der Gesetzesänderung fehlende interne Datenschutzkontrolle durch betriebliche Datenschutzbeauftragte zu kompensieren.

16.3 Betriebliche Datenschutzbeauftragte – Interessenkollision

Die Datenschutzaufsichtsbehörden haben eine gemeinsame Rechtsposition in Bezug auf eine mögliche Interessenkollision bei der Wahrnehmung der Datenschutzbeauftragtenfunktion durch IT-Dienstleistungsunternehmen bezogen.

Eine den Datenschutzaufsichtsbehörden sehr häufig gestellte Frage lautete, ob Systemhäuser, die die Netzwerkstruktur eines Unternehmens betreuen, gleichzeitig die Funktion einer Datenschutzbeauftragten oder eines Datenschutzbeauftragten bei ihrer Kundschaft übernehmen können. Das ist nicht selbstverständlich, denn die Datenschutzbeauftragten dürfen bei ihrer Tätigkeit keiner Interessenkollision ausgesetzt sein. Zu ihren Aufgaben gehört unter anderem auch die Kontrolle der Datensicherheit im Unternehmen. Wer etwa die Netzwerkstruktur in einem Unternehmen installiert, kann dabei nicht gleichzeitig die Kontrollfunktion über die eigene Arbeit ausüben.

Andererseits ist es in kleineren mittelständischen Unternehmen oft so, dass diese nicht über eigene im Datenschutz sachkundige Beschäftigte verfügen. Das externe IT-Dienstleistungsunternehmen, das die Rechnerinfrastruktur im Unternehmen betreut, hat aber häufig Beschäftigte, die fachlich als Datenschutzbeauftragte geeignet sind. Die Datenschutzaufsichtsbehörden haben für diese Sachlage eine Lösung aufgezeigt:

- Ein IT-Dienstleistungsunternehmen kann durch sein Personal die Funktion einer oder eines Datenschutzbeauftragten bei der Kundschaft wahrnehmen lassen, wenn es hierzu Personen einsetzt, denen es arbeitsvertraglich Unabhängigkeit im Sinne von § 4 Abs. 3 Bundesdatenschutzgesetz in Bezug auf die Datenschutzberatung garantiert.

17 Internationaler Datenverkehr

17.1 Antiterrorliste – Rechtsweg ausgeschlossen

Der Sanktionsausschuss der Vereinten Nationen ebenso wie der Rat der Europäischen Union erstellen Listen über terrorverdächtige Personen und Organisationen. Dabei werden rechtsstaatliche Prinzipien nicht allzu genau genommen.

Die Aufnahme in die Antiterrorlisten greift nicht nur tief in das informationelle Selbstbestimmungsrecht der betroffenen Personen ein, sondern hat in vielen Lebensbereichen gravierende Folgen. Wer auf die Liste terrorverdächtiger Personen der Vereinten Nationen oder des Rates der Europäischen Union gerät, unterliegt umfangreichen wirtschaftlichen und finanziellen Beschränkungen und sonstigen Sanktionen. Den Betroffenen wird beispielsweise die Einreise in die Länder der Europäischen Union verweigert, ihre Konten werden gesperrt, Vermögenswerte eingefroren, eine Eintragung in öffentliche Register, etwa das Grundbuch, ist nicht mehr zulässig. Die Sanktionen reichen bis zur Sperrung von Hilfen der Sozialämter und Arbeitsagenturen. Häufig sind die betroffenen Personen nicht eindeutig bezeichnet. Kommt es dann zu Verwechselungen, treffen die schwerwiegenden Folgen, die ein normales Leben nahezu unmöglich machen und die berufliche oder geschäftliche Existenz vernichten können, völlig unschuldige Personen. Auch deutsche Staatsangehörige stehen auf dieser Liste.

Umso wichtiger wäre es, diese gravierenden Folgen an ein rechtsstaatlich zweifelsfreies Verfahren zu knüpfen. Genau daran fehlt es aber: Die Aufnahme in die Antiterrorliste der Vereinten Nationen, die von der Europäischen Gemeinschaft durch die Verordnung (EG) Nr. 881/2002 des Rates umgesetzt wird, erfolgt auf Initiative einzelner Mitgliedstaaten durch den Sanktionsausschuss der Vereinten Nationen. Nur auf diesem Weg kann ein Mensch auch wieder von der Liste gestrichen werden. Ein individuelles Klagerecht der Betroffenen oder zumindest die Möglichkeit, ein unabhängiges Gremium um eine Überprüfung bitten zu können, existiert nicht. Das Gericht erster Instanz der Europäischen Gemeinschaften hat in seinem Urteil vom 21. September 2005 (T-206/01) die völkerrechtliche Verpflichtung der Europäischen Union zur Umsetzung der Vorgaben der Vereinten Nationen in den Vordergrund gestellt. Das Gericht meinte, die Rechte der von Sanktionen

betroffenen Personen auf ein rechtsstaatliches Verfahren nach den in der Europäischen Union geltenden Maßstäben angesichts dieser völkerrechtlichen Verpflichtung nicht durchgreifen lassen zu können.

Auf Basis der Verordnung (EG) Nr. 2580/2001 des Rates wird ergänzend eine eigene Terroristenliste der Europäischen Union durch Entscheidung des Rates erstellt. Bezüglich dieser Liste hat das Gericht erster Instanz der Europäischen Gemeinschaften allerdings am 12. Dezember 2006 ein Urteil (T-228/02) gefällt, in dem es die Aufnahme einer Organisation in die Liste wegen rechtsstaatlicher Verfahrensmängel für nichtig erklärt hat. Nach diesem Urteil haben vor allem die Mitgliedstaaten, auf deren Vorschlag der Rat einzelne Personen oder Organisationen auf die Liste setzt, ein rechtsstaatliches Verfahren sicherzustellen. Das bedeutet, dass den Betroffenen unmittelbar nach Aufnahme in die Liste die Möglichkeit zu rechtlichem Gehör gegeben werden muss und dass ein gerichtliches Verfahren zur Überprüfung der Entscheidung zur Verfügung stehen muss. Die angegebenen Urteile können im Internet unter http://curia.europa.eu abgerufen werden.

- In ihrer Entschließung vom 16./17. März 2006 (abgedruckt im Anhang) fordern die Datenschutzbeauftragten des Bundes und der Länder die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung rechtsstaatlicher Standards zu dringen. Dazu gehören ein transparentes Verfahren, Entscheidungen auf gesicherter Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

17.2 Reisen ist verdächtig

Die Angst vor terroristischen Anschlägen führt ganz besonders im internationalen Reiseverkehr zu überzogenen Überwachungsmaßnahmen. Datenschutz und rechtstaatliche Grundsätze werden teilweise außer Acht gelassen, insbesondere im transatlantischen Flugverkehr.

Zur Übermittlung von Reservierungsdaten der Flugreisenden an das US Bureau of Customs and Border Protection (CBP) enthält bereits der Bericht 2005 unter 6.1 eine ausführliche Darstellung. In der Zwischen-

zeit ist die Vereinbarung außer Kraft getreten, die die EU-Kommission mit den US-Behörden über Mindestanforderungen des Datenschutzes getroffen hatte. Der Europäische Gerichtshof hatte auf eine Klage des Europäischen Parlaments hin festgestellt, dass das Abkommen Fragen der Sicherheitspolitik regele und deswegen alleine der Rat der Europäischen Union ein solches Abkommen hätte abschließen können.

Das Parlament, das über die Klage mehr Datenschutz für die Flugpassagiere erreichen wollte, hat damit einen Pyrrhussieg errungen. Zwar wurde die angefochtene Vereinbarung beendet, inzwischen hat aber der zuständige EU-Rat das Abkommen im Wesentlichen inhaltsgleich erneuert. Gemeinsam mit dem neuen Abkommen wurde ein Brief des US-Heimatschutzministeriums veröffentlicht, der die getroffenen Vereinbarungen über die Datenschutzgarantien in einer Weise auslegt, die sich nachteilig für die Fluggäste auswirkt. So behält sich die US-Seite nun vor, durch einseitige Erklärung die Zahl der zu übermittelnden Datensätze zu erweitern. Die Übermittlung von Daten an andere Sicherheitsbehörden in den USA soll ebenso erleichtert werden wie die Weitergabe von Passagierdaten an Gesundheitsbehörden für Zwecke der Seuchenbekämpfung. Das laufende Abkommen gilt längstens bis Ende Juli 2007 und soll durch eine längerfristige Vereinbarung ersetzt werden. Ein hochrangiger Vertreter des US-Heimatschutzministeriums hat für die Verhandlungen über das Folgeabkommen bereits weitere Verschlechterungen bei den Datenschutzgarantien angekündigt. Insbesondere soll die Dauer der Datenspeicherungen über die nun schon festgelegten drei Jahre und sechs Monate ausgeweitet werden.

Neben der Auswertung der Reservierungsdaten nutzen die US-Sicherheitsbehörden zur Überwachung der Passagiere außerdem bestimmte Listen. Ausgewählte Sicherheitskräfte der Fluggesellschaften erhalten täglich eine aktualisierte No-Fly-Liste und eine Selectee-Liste aus den USA. Auf der No-Fly-Liste sind Personen vermerkt, die nicht in die USA einreisen dürfen. Auf der zweiten Liste befinden sich Daten von Personen, die einer eingehenden Leibesvisitation und Gepäckkontrolle unterzogen werden müssen und erst nach Rücksprache mit den US-Sicherheitsbehörden über das Ergebnis der Kontrolle in die USA einreisen dürfen. Auf beiden Listen sind jeweils mehrere 10.000 Personen verzeichnet. Die Fluggesellschaften führen beim Einchecken ihrer Fluggäste einen Datenabgleich mit den Listen durch, weil sie ansonsten Gefahr laufen, dass ihre Maschinen nach dem Start zurückfliegen

müssen. Denn sie erhalten in den USA keine Landeerlaubnis, wenn sich gelistete Personen an Bord befinden. Mittelfristig planen die US-Behörden, diesen Datenabgleich selbst zu übernehmen und nicht mehr den Fluggesellschaften zu überlassen. Die Fluggesellschaften senden bereits spätestens 15 Minuten nach dem Start die Passdaten und weitere Angaben zum Reiseziel der eingecheckten Fluggäste an die US-Sicherheitsbehörden. Zukünftig sollen die Daten bereits vor dem Start ausgetauscht werden. Auf dieser Basis würden dann Weisungen an die Fluggesellschaften erteilt, welche Fluggäste in die USA geflogen werden dürfen und welche nur nach eingehender Untersuchung an Bord dürfen.

Die Reisenden erfahren regelmäßig über den Datenabgleich nichts. Personen, die auf einer der Listen vermerkt sind, stehen keine Verfahren zur Verfügung, in denen sie ihre Rechte auf Auskunft, Löschung oder Berichtigung geltend machen könnten. Es gibt keine Möglichkeit, die Gründe nachzuvollziehen, warum die Personen gelistet sind. Für die Selectee-Liste gibt es lediglich die Vermutung, dass sie ein Produkt der systematischen Auswertung der Reservierungsdaten sein könnte. So scheint eine sehr kurzfristige Buchung oder die Barzahlung des Fluges ein Kriterium für die Aufnahme auf die Selectee-Liste zu sein. Beides sind Informationen, die sich aus den Reservierungsdaten ablesen lassen.

Neben den USA erhält aktuell Kanada ebenfalls Reservierungsdaten von Flugreisenden. Der Datensatz, der den kanadischen Behörden zur Verfügung gestellt wird, ist allerdings deutlich kleiner als im Fall der USA. Er enthält keine sensitiven Daten und wird über eine sogenannte "Push-Lösung" technisch begrenzt auf die Reservierungsdaten, die für Sicherheitszwecke gefordert werden. Das CBP in den USA erhält demgegenüber nach wie vor den Zugriff auf die gesamten Reservierungsdaten der größeren europäischen Fluggesellschaften, also auch auf Daten für Flüge ohne Bezug zu den USA. Die Umsetzung einer Push-Lösung ist ein wichtiges Instrument, um den Datenzugriff auf Flüge mit US-Bezug zu beschränken. Leider haben die USA sich in ihrem Interpretationsschreiben zum laufenden Abkommen vorbehalten, einseitig die Regeln für eine solche Push-Lösung vorzugeben. Daran kann deren Realisation scheitern.

Außerdem fordern aktuell Australien und Indien Reservierungsdaten. Innerhalb Europas zeigt sich ein uneinheitliches Bild. Zur Verhinderung

illegaler Einwanderung waren auf Grundlage einer EG-Richtlinie in den Mitgliedstaaten Regelungen umzusetzen, wonach die Fluggesellschaften im Wesentlichen zur Personenidentifizierung geeignete Passagierdaten an die Grenzbehörden übermitteln sollen. Bei der Umsetzung sind einzelne Mitgliedstaaten deutlich über das Ziel der Richtlinie hinaus gegangen und fordern umfangreichere Datensätze von den Fluggesellschaften auch zu allgemeinen Sicherheitszielen.

➡ Es muss ein einheitlicher internationaler Standard für Maßnahmen der Sicherheit im Flugverkehr gefunden werden. Dabei sind einzelstaatliche sicherheitspolitische Regelungen auf das erforderliche Maß zurückzuführen. Es müssen rechtsstaatliche Kontrollmechanismen dieser Maßnahmen vorgesehen und Transparenz für die Fluggäste geschaffen werden.

17.3 US-amerikanische Finanz- und Sicherheitsbehörden werten europäische Finanzdaten aus

Wer eine Überweisung ins Ausland veranlasst, um beispielsweise die Hotelrechnung am Urlaubsort zu bezahlen, muss damit rechnen, dass die Daten aus der Überweisung gegebenenfalls auch dem US-Geheimdienst in die Hände fallen und dort für Zwecke der Terrorismusbekämpfung ausgewertet werden.

Das belgische Unternehmen SWIFT (Society for Worldwide Interbank Financial Telecommunications), eine internationale Genossenschaft der Finanzinstitute, betreibt ein Telekommunikationsnetzwerk zum automatisierten Austausch von Zahlungsverkehrsnachrichten zwischen Kredit- und Finanzinstituten im internationalen Zahlungsverkehr. Um einen internationalen Zahlungsauftrag ausführen zu können, leiten die Banken bestimmte Daten, zum Beispiel die Namen der Zahlungsauftraggebenden und Zahlungsempfangenden, den Überweisungsbetrag sowie den Verwendungszweck an SWIFT weiter. Weltweit wickeln ungefähr 7.800 Banken in über 200 Staaten ihren internationalen Zahlungsverkehr über SWIFT ab.

Für die Zwecke der Datensicherung speichert SWIFT über einen Zeitraum von 124 Tagen den gesamten Datenbestand aus den abgewickelten Transaktionen stets in zwei Rechenzentren, von denen sich das eine in den Niederlanden, das andere in den USA befindet. Selbst die

Daten für eine Überweisung ohne Bezug zu den USA, wie etwa von Aachen ins benachbarte niederländische Vaals, werden daher auch bei SWIFT/USA gespeichert.

Nach den Terrorangriffen vom 11. September 2001 begannen US-amerikanische Behörden damit, von SWIFT Zugang zu den im Rechenzentrum in den USA gespeicherten Daten zu verlangen. Grundlage bildeten behördliche Beschlagnahmeanordnungen nach US-amerikanischem Recht. Zwar konnte SWIFT in der Vergangenheit einige Einschränkungen aushandeln, gab den Forderungen nach einer Herausgabe der Daten jedoch im großen und ganzen immer nach. Erst durch die Presseberichterstattung vor einigen Monaten wurde die Öffentlichkeit über die Vorgänge um SWIFT informiert. Auch die meisten beteiligten Banken erfuhren erstmals aus der Zeitung, dass Daten ihrer Kundinnen und Kunden regelmäßig Gegenstand von Beschlagnahmen US-amerikanischer Behörden bei SWIFT/USA sind. Lediglich die im Aufsichtsrat von SWIFT vertretenen Kreditinstitute, darunter zwei deutsche Banken, sowie die nationalen Zentralbanken waren zuvor von SWIFT über die in den USA erlassenen Beschlagnahmeanordnungen informiert.

SWIFT unterliegt als in Belgien gegründetes Unternehmen belgischem Recht und der Aufsicht der zuständigen belgischen Datenschutzaufsichtsbehörde. Die europäischen Banken, die sich der Dienstleistungen von SWIFT bedienen, unterliegen dagegen der Aufsicht der in den einzelnen Ländern jeweils zuständigen Behörden. Sowohl bundesweit unter Vorsitz der LDI NRW als auch auf europäischer Ebene setzten sich die Aufsichtsbehörden in Arbeitsgruppen eingehend mit dem Sachverhalt und seiner rechtlichen Bewertung auseinander, um ein abgestimmtes Vorgehen aller Aufsichtsbehörden zu erreichen.

Der "Düsseldorfer Kreis" als bundesweites Gremium der obersten Aufsichtsbehörden für Datenschutz im nicht-öffentlichen Bereich stellte im November 2006 fest, dass die gegenwärtige Übermittlung von Datensätzen an das SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe der gespeicherten Daten von dort an US-amerikanische Behörden sowohl nach deutschem Recht als auch nach europäischem Datenschutzrecht unzulässig sind. Als rechtlich verantwortlich sind sowohl die in Belgien ansässige SWIFT als auch die deutschen Banken anzusehen, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiter-

hin der Dienstleistungen von SWIFT bedienen. Die Banken wurden von den Aufsichtsbehörden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Behörden künftig ausgeschlossen ist. Der einstimmig gefasste Beschluss des Düsseldorfer Kreises ist im Anhang abgedruckt.

Nach Ansicht der Aufsichtsbehörden könnte eine Lösung in der Verlagerung des zurzeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau liegen. Eine weitere Möglichkeit könnte in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen bestehen. Dabei wäre auszuschließen, dass die US-amerikanischen Behörden die auf dem dortigen Server gespeicherten Daten dechiffrieren. Gegebenfalls kann auch durch ein völkerrechtliches Abkommen zwischen der EU und den USA ein Rechtsrahmen für die Übermittlung von Transaktionsdaten mit internationalem Bezug in die USA geschaffen werden. Allerdings muss ein solches Abkommen inhaltlich hinreichende Garantien für den Schutz der personenbezogenen Daten der Bankkundinnen und Bankkunden enthalten. Zudem würde ein in unbestimmter Zukunft liegender Abschluss auch den gegenwärtigen Handlungsbedarf nicht beseitigen. Die Banken sind daher in der Pflicht, auch für die Zwischenzeit geeignete Maßnahmen vorzuschlagen.

Unabhängig davon müssen die Banken ihre Kundinnen und Kunden unverzüglich darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges Rechenzentrum von SWIFT übermittelt werden. Diese Unterrichtung ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA.

Die deutschen Aufsichtsbehörden befinden sich mit ihren Forderungen in Übereinstimmung mit den übrigen europäischen Aufsichtsbehörden. Nach europaweit einheitlicher Ansicht lassen die gegenwärtig im SWIFT-Verfahren stattfindenden Datenübermittlungen in die USA die durch die Europäische Datenschutzrichtlinie definierten Garantien für einen Datentransfer in einen Drittstaat in wesentlichen Punkten unberücksichtigt.

- Die gegenwärtig noch stattfindenden Übermittlungen von Zahlungsverkehrsdaten an SWIFT/USA sind unzulässig. Die nationalen Banken sind verpflichtet, geeignete Maßnahmen zu treffen, um den Zugriff US-amerikanischer Behörden auf die im Rechenzentrum von SWIFT/USA befindlichen Datensätze wirksam auszuschließen. Die deutschen und europäischen Banken müssen ihre Kundinnen und Kunden unverzüglich darüber informieren, dass Daten aus ihren internationalen Zahlungsaufträgen stets auch in die USA übermittelt werden.

17.4 Globale Datenverarbeitung ohne Risiko

Verunsicherung herrscht in der Wirtschaft noch immer darüber, unter welchen Voraussetzungen Daten ins Ausland übermittelt werden dürfen. Dabei steht inzwischen eine ganze Reihe von Instrumenten zur Verfügung, die Datenübermittlungen auch in Länder ermöglichen, die kein angemessenes Datenschutzniveau besitzen.

Wenn die Übermittlung von personenbezogenen Daten durch ein Gesetz oder die Einwilligung der Betroffenen grundsätzlich erlaubt ist, sind unter Umständen dennoch weitere Vorkehrungen zu treffen, wenn die Daten empfangende Stelle in einem Staat ohne angemessenes Datenschutzniveau liegt. Es gibt verschiedene Instrumente, mit denen dann gesetzlich vorgeschriebene Datenschutzgarantien für die von einer solchen Übermittlung betroffenen Personen erreicht werden können. Einen Überblick über diese Instrumente bietet der Bericht 2003 unter 4. Neu hinzugekommen ist ein weiterer Standardvertrag für die Übermittlung an eine verantwortliche Stelle im sogenannten Drittstaat, den die EU-Kommission mit ihrer Entscheidung vom 27. Dezember 2004 eingeführt hat (veröffentlicht im Amtsblatt der Europäischen Union unter L 385/74). Dieser Vertrag wird allgemein als Alternativer Standardvertrag bezeichnet. Wird er originalgetreu für Datenübermittlungen in einen Drittstaat eingesetzt, bedarf diese Übermittlung in Deutschland nicht der Genehmigung gemäß § 4c Abs. 2 Bundesdatenschutzgesetz. Eine Kombination einzelner Klauseln aus den verschiedenen Standardverträgen ist nicht ohne weiteres möglich. Wer Elemente aus den Standardverträgen nach eigenen Vorstellungen

kombiniert, erstellt damit einen individuellen Vertrag. Wird ein Individualvertrag eingesetzt, bedarf die Datenübermittlung in den Drittstaat der Genehmigung durch die Datenschutzaufsichtsbehörde.

Sehr aktiv haben die Datenschutzbeauftragten und -behörden in Europa daran gearbeitet, den Weg für das Instrument der "verbindlichen Unternehmensregelung zum Datenschutz" (Binding Corporate Rules = BCR) als Grundlage für Datenübermittlungen in Drittstaaten zu ebnen. Insbesondere international agierende Konzerne sind daran interessiert, die Datenschutzregelungen im Konzern weltweit einheitlich festzulegen. Wenn diese Festlegungen rechtlich verbindlich gemacht werden und zugleich ausreichende Datenschutzgarantien gewährleisten, können sie einen Rahmen für Datenübermittlungen in Drittstaaten bilden.

Allerdings müssen die Inhalte der BCR von den Datenschutzaufsichtsbehörden aller EU-Mitgliedstaaten anerkannt sein, aus denen Datenübermittlungen stattfinden. Um den Ablauf zu vereinfachen, wurde ein koordiniertes Verfahren entwickelt, das es den Unternehmen ermöglicht, zunächst nur mit einer Datenschutzbehörde zu verhandeln. Diese Behörde bemüht sich ihrerseits um die Abstimmung mit den anderen Datenschutzaufsichtsbehörden. Unternehmen, die dieses koordinierte Verfahren für ihre BCR anstreben, können sich in dem Arbeitspapier (WP 107) der Art. 29-Arbeitsgruppe bei der EU-Kommission informieren, welche Datenschutzaufsichtsbehörde sie wegen der Koordinierung ansprechen sollten. In einem weiteren Arbeitspapier (WP 108) ist beschrieben, welche Unterlagen in jedem Fall für das Verfahren einzureichen sind. Die Arbeitspapiere können unter folgender Adresse abgerufen werden: http://ec.europa.eu/justice_home/fsj/privacy/ workinggroup/wpdocs/2005_de.htm.

Ein erstes koordiniertes Verfahren wurde vom britischen Information Commissioner für die Datenschutzregelungen des US-Konzerns General Electric erfolgreich abgeschlossen. Weitere Konzerne wie Philipps und DaimlerChrysler befinden sich mit ihren Unternehmensregelungen ebenfalls im koordinierten Verfahren. Das Verfahren dient dazu, Einigkeit über die notwendigen Inhalte der Unternehmensregelungen zu erzielen. Nach den jeweils nationalen Gesetzen bestimmt sich, ob für die Datenübermittlung selbst noch Genehmigungen beantragt werden müssen. In diesen Genehmigungsverfahren würde der Inhalt der Unternehmensregelung dann aber von den Datenschutzbehörden, die im

Koordinierungsverfahren der Regelung zugestimmt haben, nicht mehr in Frage gestellt.

- Bei der Wahl des passenden Instruments für eine Übermittlung personenbezogener Daten an Stellen außerhalb des Europäischen Wirtschaftsraumes kommt es auf die individuellen Bedürfnisse im Unternehmen an. Im Zweifel hilft eine Beratung durch die Datenschutzaufsichtsbehörde bei der Entscheidungsfindung.

18 Informationsfreiheit

18.1 Fortschritte mit Stolpersteinen

Die Erfahrungen mit dem nordrhein-westfälischen Informationsfreiheitsgesetz (IFG NRW) sind überwiegend positiv. Der verfahrensunabhängige und voraussetzungslose Anspruch auf Zugang zu Informationen bei öffentlichen Stellen hat sich gut bewährt. Dennoch gibt es immer wieder auch Informationssackgassen, die den Informationssuchenden Frust bereiten.

Das 2002 in Kraft getretene IFG NRW wurde nach den ersten zwei Jahren seiner Existenz auf seine Auswirkungen hin überprüft. Der im Oktober 2004 vorgelegte Bericht (LT-Drs. Vorlage 13/3041) benennt eine Zahl von etwa 1.000 Informationsanträgen pro Jahr, verteilt auf alle öffentlichen Stellen des Landes. Zwischen 2004 und Ende 2006 wurde zwar keine Statistik mehr geführt, aber die in etwa gleichgebliebene Zahl der Anfragen und Beschwerden bei der LDI lässt im Rückschluss die Vermutung zu, dass sich die Antragszahlen auf diesem Niveau verstetigt haben könnten. Auch wenn der Schwerpunkt der Informationsanträge im kommunalen Bereich liegt, hat sich die im Zuge des Gesetzgebungsverfahrens geäußerte Sorge einer erheblichen Belastung der Kommunalverwaltungen nicht bestätigt. Viele Auslegungs- und Anwendungsfragen des IFG NRW sind inzwischen durch Rechtsprechung geklärt. Zudem hat das Innenministerium mittlerweile einen Anwendungserlass veröffentlicht, der ebenfalls Antworten auf offene Fragen gibt und außerdem die Pflicht wieder einführt, ab 2007 erneut eine Statistik zu Anzahl und Gegenstand der Informationsanträge sowie zu den Gebührenerhebungen zu führen.

➡ Der Anwendungserlass des Innenministeriums ist ein weiterer Schritt nach vorne. Seine Weiterentwicklung bleibt jedoch ständige Aufgabe.

18.2 Kammern können sich ihrer Informationspflicht nicht entziehen

Die in Nordrhein-Westfalen bislang streitige Frage, ob das Informationsfreiheitsgesetz NRW (IFG NRW) auch auf die Industrie- und Handelskammern Anwendung findet, wurde inzwi-

schen durch das Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW) geklärt.

Die Landesregierung ging bislang davon aus, dass ein Informationsanspruch gegen die Kammern nicht aus dem IFG NRW hergeleitet werden könne. Es solle vor allem das Gesetz über die Industrie- und Handelskammern (IHKG) vorrangig anwendbar sein und das IFG NRW vollständig verdrängen. Dieser Auffassung ist die LDI immer mit dem Argument entgegengetreten, dass auch bundesrechtlich verfasste Körperschaften als öffentliche Stellen des Landes informationspflichtig sind und dem Anwendungsbereich des IFG NRW unterfallen. Dieser Streit dürfte nach dem Urteil des OVG NRW vom 9. November 2006 (Az: 8 A 1679/04, www.nrwe.de) beigelegt sein.

Das OVG NRW bestätigt in dieser Entscheidung, dass die Industrie- und Handelskammer (IHK) als Körperschaft des öffentlichen Rechts der Aufsicht des Landes untersteht und damit grundsätzlich unter den Anwendungsbereich des IFG NRW fällt. Der Landesgesetzgeber hat auch die Gesetzgebungskompetenz zur Regelung eines allgemeinen Informationszugangsrechts gegenüber der IHK, da keine verdrängende Gesetzgebungskompetenz des Bundes besteht. Selbst wenn eine mögliche Gesetzgebungskompetenz des Bundes im Hinblick auf die Regelung von Verwaltungsverfahrensvorschriften oder Kraft Sachzusammenhangs mit der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft angenommen wird, hat der Bund jedenfalls von einer solchen Kompetenz keinen Gebrauch gemacht. Weder im IHKG noch im Bundesinformationsfreiheitsgesetz ist ein allgemeiner Informationsanspruch gegenüber der nordrhein-westfälischen IHK geregelt.

- Das OVG NRW hat mit seinem Urteil nunmehr auch die bereits seit langem von der LDI vertretene Auffassung bestätigt, dass das IFG NRW ebenfalls auf die nordrhein-westfälischen Industrie- und Handelskammern anwendbar ist.

18.3 Informationszugang auch bei privatisierter Aufgabenerfüllung?

Es bestehen immer noch Unklarheiten bei der Anwendung des Informationsfreiheitsgesetzes NRW (IFG NRW) auf juristische

Personen des Privatrechts. Die Klärung der Auslegung des § 2 Abs. 4 IFG NRW ist daher weiterhin erforderlich.

Sinn und Zweck des IFG NRW ist, die Transparenz und Akzeptanz behördlichen Handelns zu erhöhen sowie das Mitspracherecht und – mittelbar – auch die Kontrollmöglichkeiten der Bürgerinnen und Bürger in Bezug auf das Handeln staatlicher Organe zu verbessern. Diese Zielsetzung würde angesichts der den öffentlichen Stellen zunehmend eröffneten Möglichkeiten, bei der Erfüllung öffentlicher Aufgaben auf privatrechtliche Organisations- und Handlungsformen zurückzugreifen, weitgehend verfehlt, wenn sich der Anwendungsbereich des Gesetzes nicht auch auf eben diese Personen des Privatrechts erstreckte.

Die Auskunftspflicht natürlicher und juristischer Personen des Privatrechts richtet sich nach § 2 Abs. 4 IFG NRW. Nach dieser Bestimmung gelten natürliche oder juristische Personen des Privatrechts als Behörden im Sinne des Gesetzes und sind damit im gleichen Umfang wie öffentliche Stellen informationspflichtig, sofern sie öffentlich-rechtliche Aufgaben wahrnehmen. Zu der Auslegung dieser Regelung werden jedoch nach wie vor unterschiedliche Meinungen vertreten.

Die Auffassung, dass die Vorschrift lediglich Beliehene in den Anwendungsbereich mit einbeziehe, kann nicht überzeugen, da Beliehene ohnehin den gesetzlich definierten Behördenbegriff erfüllen und auf sie das Gesetz bereits nach § 2 Abs. 1 IFG NRW anwendbar ist. Daher liegt es nahe, dass die in § 2 Abs. 4 IFG NRW geregelte Fiktion den Anwendungsbereich des § 2 Abs. 1 IFG NRW erweitert.

So wird immer häufiger vertreten, dass auch diejenigen Personen des Privatrechts von dem Anwendungsbereich umfasst sind, die Aufgaben wahrnehmen, die der Verwaltung gesetzlich zugewiesen sind. Aus der Verwendung des Begriffs "öffentlich-rechtliche" Aufgaben folge eine Eingrenzung auf die staatlichen Aufgaben, die sich eindeutig aus einer öffentlich-rechtlichen Norm ableiten ließen. Hiernach wäre etwa der Zugang zu Informationen bei einem privaten Abfall- und Abwasserunternehmen möglich, nicht aber Informationen betreffend die Wasser- und Energieversorgung. Diese Differenzierung führt allerdings für die informationssuchenden Personen häufig zu nicht nachvollziehbaren unterschiedlichen Ergebnissen.

Wieder andere Stimmen sind der Auffassung, dass "öffentlich-rechtlich" in § 2 Abs. 4 IFG NRW nicht enger zu verstehen ist als "öffentlich"

in § 2 Abs. 1 Satz 2 IFG NRW. In beiden Fällen handelt es sich nämlich um die Wahrnehmung von im öffentlichen Recht wurzelnden Verwaltungsaufgaben. Hieraus ergibt sich, dass eine juristische Person des Privatrechts schon dann von dem Anwendungsbereich erfasst ist, wenn sie eine gemeinwohlerhebliche Aufgabe wahrnimmt, die die öffentliche Hand aufgrund ihrer Wahrnehmungskompetenz zur öffentlichen Aufgabe gemacht hat. Demnach sind auch kommunale Unternehmen bei ihrer Wahrnehmung von Aufgaben im Bereich der freiwilligen Selbstverwaltung insbesondere der Daseinsvorsorge jedenfalls dann nach dem IFG NRW auskunftspflichtig, wenn die kommunale Gebietskörperschaft einen maßgeblichen oder gar beherrschenden Einfluss ausübt. Kriterien für einen bestimmenden Einfluss der öffentlichen Hand sind Kapitalanteile sowie die Zusammensetzung des Aufsichtsgremiums.

Für diese Wertung spricht auch die Rechtsprechung des Bundesgerichtshofes (BGH) zum niedersächsischen Pressegesetz. Darin führt der BGH aus, dass überall dort, wo zur Wahrnehmung staatlicher Aufgaben öffentliche Mittel eingesetzt werden, auch ein Informationsbedürfnis der Bevölkerung begründet wird. Auf dieses Bedürfnis hat es keinen Einfluss, ob sich die Exekutive zur Wahrnehmung öffentlicher Aufgaben im Einzelfall einer privatrechtlichen Organisationsform bedient (BGH, Urteil vom 10.02.2005, Az: III ZR 294/04).

- Es gibt gute Argumente dafür, dass diejenigen Privaten von dem Anwendungsbereich des Gesetzes erfasst sind, die öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen und zugleich von der öffentlichen Hand kontrolliert werden, sei es über Kapitalanteile, Stimmrechte oder über die Bestellung von Mitgliedern der Verwaltungs-, Leitungs- oder Aufsichtsorgane.

18.4 Klare Worte des Gerichts zum Konkurrenzverhältnis

Seit Anfang 2005 kann auch das besonders umstrittene Verhältnis des Informationsfreiheitsgesetzes zu § 29 VwVfG NRW und § 25 SGB X als gerichtlich geklärt angesehen werden. Beide Normen schließen ein Zugangsrecht nach dem IFG NRW nicht aus, so dass die Vorschriften nebeneinander zur Anwendung kommen können.

Inzwischen entspricht es schon fast ständiger Rechtsprechung, dass § 29 Verwaltungsverfahrensgesetz NRW (VwVfG NRW) und § 25 Sozialgesetzbuch Zehntes Buch (SGB X) das allgemeine Informationszugangsrecht nach dem Informationsfreiheitsgesetz NRW (IFG NRW) nicht generell verdrängen können (vgl. OVG NRW, Beschluss vom 31.01.2005, Az: 21 E 1487/04, abgedruckt in NJW 2005, 2028 f; VG Köln, Urteil vom 25.11.2005, Az: 27 K 6171/03).

Nach § 4 Abs. 2 Satz 1 IFG NRW treten die Vorschriften des IFG NRW zurück, soweit besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht bestehen. Schon das Tatbestandsmerkmal "soweit" zeigt, dass jedenfalls nur solche Vorschriften als vorrangig in Betracht zu ziehen sind, die denselben Sachverhalt abschließend – sei es identisch, sei es abweichend – regeln. Konkurrenzfragen sind in jedem Einzelfall durch eine systematische, an Sinn und Zweck des Gesetzes orientierte Auslegung der jeweiligen Informationszugangsrechte zu klären. Eine Vorrangigkeit im Sinne einer Ausschließlichkeit ist nur anzunehmen, wenn ein umfassender Informationsanspruch dem Schutzzweck des Spezialgesetzes zuwider laufen würde. Lässt sich derartiges nicht feststellen, gelangt der Anspruch aus § 4 Abs. 1 IFG NRW zur Anwendung.

Während das IFG NRW allen Bürgerinnen und Bürgern einen voraussetzungslosen Informationszugangsanspruch gewährt, räumen § 29 VwVfG NRW und § 25 SGB X ein Akteneinsichtsrecht nur den an einem Verwaltungsverfahren Beteiligten und dies auch nur für die das jeweilige Verwaltungsverfahren betreffenden Akten und nur für die Zeit des laufenden Verwaltungsverfahrens ein. Die Beteiligten müssen im Rahmen dieser Zugangsrechte zwar einerseits ein besonderes Interesse geltend machen. Andererseits unterliegen sie aber nicht den Einschränkungen, wie sie für einen Anspruch auf der Grundlage des IFG NRW in den §§ 6 ff. IFG NRW geregelt sind. Die Einschränkungen, denen der allgemeine Informationszugangsanspruch unterliegt, stellen zudem hinreichend sicher, dass private Belange der am Verwaltungsverfahren Beteiligten oder unbeteiligter Dritter in ausreichender Weise geschützt werden.

➡ Die früher oft behauptete Systemwidrigkeit des informationsrechtlichen Zugangsanspruchs im Verfahrensrecht besteht nicht. Das allgemeine Informations-

zugangsrecht ist vielmehr neben § 29 VwVfG NRW und § 25 SGB X anwendbar.

18.5 Wie der Wille gebildet wird...

Informationen über den Prozess der Willensbildung innerhalb, von und zwischen öffentlichen Stellen sollen nicht offen gelegt werden. Dies hat seinen guten Grund. Für manche öffentlichen Stellen zählt aber allzu viel zum Willensbildungsprozess.

Kein anderer Verweigerungsgrund wird nach den bisherigen Erfahrungen mit dem Informationsfreiheitsgesetz NRW (IFG NRW) so häufig missverstanden wie derjenige nach § 7 Abs. 2 Buchstabe a) IFG NRW, der dem Schutz des Willensbildungsprozesses dient. Der entsprechende Verweigerungsgrund erfasst nicht automatisch alle Informationen, die mit einem solchen Prozess in irgendeiner Weise in Zusammenhang stehen. Geschützt sind vielmehr nur Informationen, die einen Willensbildungsprozess tatsächlich inhaltlich wiedergeben. Diese enge Auslegung wurde inzwischen auch durch das Oberverwaltungsgericht NRW bestätigt (OVG NRW, Urteil vom 09.11.2006, Az: 8 A 1679/04, www.nrwe.de).

Der Ausschlussgrund kann nach Auffassung des OVG NRW lediglich für Anordnungen, Äußerungen und Hinweise gelten, die die Willensbildung steuern sollen. Es könne nicht bereits jede Stellungnahme oder jeder Vorschlag für eine zu treffende Entscheidung hierunter fallen, da ansonsten zu sämtlichen internen Vorbereitungsmaßnahmen innerhalb einer Verwaltung kein Informationsanspruch bestünde. Zudem würde der Ausschlussgrund des § 7 Abs. 1 IFG NRW, der einen Zugangsanspruch nur für Arbeiten und Beschlüsse zur unmittelbaren Vorbereitung von Entscheidungen ausschließe, nahezu leer laufen. Wenn die zu schützenden Unterlagen aber selbst interne Meinungsverschiedenheiten oder unterschiedliche Auffassungen innerhalb einer oder zwischen verschiedenen Behörden erkennen lassen, sind diese nach Maßgabe des § 7 Abs. 2 Buchstabe a) IFG NRW auch über den Abschluss einer Entscheidung hinaus zu schützen (siehe S. 26 und 28 f. des oben genannten Urteils).

Hiervon zu unterscheiden sind die Mitteilung von Tatsachen oder Hinweise auf die Rechtslage, die im Rahmen der Willensbildung herangezogen werden. Dient beispielsweise einer öffentlichen Stelle ein Gut-

achten oder eine interne Stellungnahme dazu, sich zu einem bestimmten Sachverhalt eine Meinung zu bilden und gegebenenfalls weitere Maßnahmen einzuleiten, stellen diese Unterlagen als solche nur eine Grundlage des behördlichen Entscheidungsbildungsprozesses dar, bilden die Willensbildung aber selbst nicht unmittelbar ab. Diese Unterlagen sind daher – soweit nicht ein anderer Verweigerungsgrund eingreift – als Sachinformation zugänglich.

- Zum Schutz des Willensbildungsprozesses sind nur solche Informationen grundsätzlich gesperrt, die einen Willensbildungsprozess unmittelbar widerspiegeln, nicht aber Sachinformationen, die einem Willensbildungsprozess lediglich dienen oder dessen Grundlage bilden.

18.6 Geschäftsgeheimnis bei rechtswidrigem Verhalten?

Werden in den Medien Skandale nach Kontrollen von örtlichen Überwachungsbehörden berichtet, redet alle Welt davon, wie wichtig Transparenz für Verbraucherinnen und Verbraucher sei. Wollen sie dann tatsächlich wissen, welcher Lebensmittelbetrieb, welche Gaststätte oder welches Restaurant mit welchem Ergebnis kontrolliert wurde, wird schnell der Riegel des vermeintlichen Geschäftsgeheimnisses vorgeschoben.

Das Informationsfreiheitsgesetz NRW tritt neben das Lebensmittel- und Futtermittelgesetzbuch sowie neben das Geräte- und Produktsicherheitsgesetz mit seinen besonderen Regelungen für die behördliche Informationstätigkeit. Es findet dann Anwendung, wenn Kontrollbehörden in Bereichen tätig sind, die durch die genannten Spezialregelungen nicht abgedeckt oder nicht abschließend geregelt sind. Der Zugang zur gewünschten Information, etwa welche Betriebe mit welchem Ergebnis überprüft worden sind, darf nur verweigert werden, wenn ein gesetzlicher Ablehnungsgrund vorliegt. Der jeweilige Ablehnungsgrund ist eng auszulegen. Wenn also ein Informationsantrag abzulehnen wäre, weil die Offenbarung eines Betriebs- oder Geschäftsgeheimnisses drohte, reicht die schlichte Prüfung nicht aus, ob etwa ein Geschäftsgeheimnis nach der wettbewerbsrechtlichen Definition zu bejahen ist. Neben den bekannten Merkmalen, nach denen Tatsachen im Zusammenhang mit dem Geschäftsbetrieb stehen müssen, die nur einem begrenzten Personenkreis bekannt, also nicht offenkundig sein

dürfen und nach dem Willen des Unternehmens geheim zuhalten sind, ist vor allem festzustellen, ob an der Geheimhaltung ein objektiv schutzwürdiges wirtschaftliches Interesse besteht. Fehlt es an einem dieser Merkmale, gibt es kein geheim zu haltendes Geschäftsgeheimnis. Liegt ein Geschäftsgeheimnis vor, muss im nächsten Schritt geprüft werden, ob durch die Offenbarung ein wirtschaftlicher Schaden eintreten würde, und weiter, ob nicht das Allgemeininteresse an der Offenlegung überwiegt.

Besteht ein objektiv schutzwürdiges wirtschaftliches Interesse an der Geheimhaltung, wenn Informationen darüber begehrt werden, mit welchem Ergebnis planmäßige Füllmengenprüfungen von Fertigpackungen durchgeführt worden sind? Die Kontrollen fanden nicht im Rahmen von Ordnungswidrigkeitenverfahren, sondern als präventive Maßnahmen der Eichämter bei verschiedenen Betrieben statt. Die Frage wird höchst unterschiedlich beantwortet.

Das Oberverwaltungsgericht Schleswig-Holstein hat ein wirtschaftliches Interesse an der Geheimhaltung der Prüfungsergebnisse auch dann angenommen, wenn die Abfüllpraxis rechtswidrig war. Nicht schon jedes rechtswidrige Verhalten schließe den Schutz des Betriebs- oder Geschäftsgeheimnisses aus (OVG Schleswig-Holstein, Beschluss vom 22.06.2005, Az: 4 LB 30/04). Ein einfacher Verstoß gegen Rechtsvorschriften könne nicht den Schutz des aus der Eigentumsgarantie von Art. 14 des Grundgesetzes resultierenden Geschäftsgeheimnisses aufheben. Aufgrund dieser Rechtsauffassung hat der Landesbetrieb Mess- und Eichwesen NRW auch die Einsichtnahme in die Niederschrift über eine Kontrolle der Gasdruckregelgeräte von Gasversorgungsunternehmen abgelehnt.

Demgegenüber verpflichtete das Verwaltungsgericht Berlin das dortige Landesamt für Mess- und Eichwesen, Auskunft über die festgestellten Füllmengenunterschreitungen zu erteilen, weil die betroffenen Unternehmen kein berechtigtes wirtschaftliches Interesse an der Geheimhaltung von Verstößen gegen die gesetzlich vorgeschriebene Füllmenge hätten (VG Berlin, Urteil vom 10.05.2006, Az: VG 2 A 72.04). Diese Auffassung wird auch in der informationsrechtlichen Literatur vertreten (vergleiche Rossi, Informationsfreiheitsgesetz, Handkommentar 2006, Rdnr. 77 zu § 6 mit weiteren Nachweisen).

➧ Wer in seinem Geschäftsgebaren gegen Gesetze verstößt, hat nicht automatisch einen Anspruch auf Geheimhaltung.

18.7 Subventionen sind grundsätzlich offen zu legen

Auf der einen Seite will die Transparenzinitiative der EU-Kommission eine Veröffentlichung aller europäischen Subventionsleistungen erreichen. Andererseits werden einer Veröffentlichung besonders aus dem Wirtschaftsbereich mögliche Geschäftsgeheimnisse entgegen gehalten.

Jede staatlich geleistete Subvention steht zwar im Zusammenhang mit den Geschäften der die Subvention erhaltenden Stelle und legt damit die Annahme eines Geschäftsgeheimnisses nahe. Dennoch stellt sich die Frage, ob ein objektiv schutzwürdiges wirtschaftliches Interesse eines Unternehmens daran bestehen kann, die Offenlegung staatlicherseits erhaltener Subvention zu verhindern. Das wäre jedenfalls dann so, wenn die bloße Angabe der Subventionssumme schon Aufschluss über weitere zur objektiven Gegebenheit eines Geschäftsgeheimnisses gehörende Umstände wie Kalkulation, Marktstrategie oder Marktchancen eines Geschäfts- oder Produktionsbetriebes geben würde. Kann ein im Wettbewerb stehendes Unternehmen aus der Kenntnis der geleisteten Subvention bereits die Marktstellung des genannten Subventionsempfängers erkennen und sich daraus einen Wettbewerbsvorteil verschaffen? In der Regel dürfte die Kenntnis der Subventionssumme zu keinem Wettbewerbsvorteil führen. In Großbritannien und Dänemark werden Subventionsdaten im Agrarbereich regelmäßig im Internet veröffentlicht, ohne dass dagegen Geschäftsgeheimnisse ins Feld geführt werden.

Selbst wenn ein objektiv schutzwürdiges wirtschaftliches Interesse an der Geheimhaltung der Information anzunehmen wäre, muss aber das Allgemeininteresse an der Kenntnis solcher Informationen berücksichtigt werden. Wohin die zum Teil erheblichen Subventionen fließen, sind allgemeine die Öffentlichkeit interessierende Informationen. An diesen Informationen lässt sich ablesen, welche Sektoren der Wirtschaft überwiegend und in welchem Umfang und welche weniger gefördert werden. Die Bedeutung, die das Wissen um diese Umstände für die Öffentlichkeit besitzt, lässt das wirtschaftliche Interesse des einzelnen Betriebes dahinter zurücktreten. Dass dem Betrieb durch die Offenle-

gung der erhaltenen Subvention ein unmittelbarer wirtschaftlicher Schaden entstehen könnte, ist ebenfalls regelmäßig nicht erkennbar.

- Es ist nicht ersichtlich, dass die Offenlegung von Subventionen Geschäftsgeheimnisse beeinträchtigen könnte. Daher sollten, wie Agrarsubventionen in Großbritannien und Dänemark, geleistete Subventionen veröffentlicht werden.

18.8 Seltene Fälle: Herausgabe personenbezogener Informationen

Dem Schutz personenbezogener Angaben wird im Rahmen des Informationsfreiheitsgesetzes NRW (IFG NRW) großes Gewicht beigemessen, das dem Niveau der übrigen landesrechtlichen Datenschutzbestimmungen in Nordrhein-Westfalen zumindest gleichwertig ist.

Es kommt vergleichsweise selten vor, dass Informationswünsche auch auf Daten zielen, die personenbezogener Art sind. Ist dies dennoch ausnahmsweise der Fall, ist die Offenbarung personenbezogener Daten Dritter nach § 9 Abs. 1 erster Halbsatz IFG NRW grundsätzlich unzulässig. Informationsanträge sind zwingend abzulehnen, wenn nicht einer der im Gesetz abschließend aufgezählten und eng zu verstehenden fünf Ausnahmetatbestände erfüllt ist (siehe insoweit Bericht 2003 unter 22.5.5).

Neben der Einwilligungserteilung geht es in der Praxis insbesondere um den Ausnahmetatbestand des § 9 Abs. 1 zweiter Halbsatz Buchstabe e) IFG NRW. Nach dieser Vorschrift müssen personenbezogene Angaben ausnahmsweise dann herausgegeben werden, wenn die informationssuchende Person an der Kenntnis der Informationen ein rechtliches Interesse geltend machen kann und nicht überwiegende schutzwürdige Belange der betroffenen Person der Offenbarung entgegen stehen. Ein solches rechtliches Interesse ist gegeben, wenn es der informationssuchenden Person eine qualifizierte Rechtsposition verschafft. Sie muss daher aufgrund der Kenntnis der begehrten Informationen ein gerade ihr zustehendes subjektives Recht geltend machen können. Hierunter fällt zum Beispiel ein mit einer Grunddienstbarkeit belastetes Eigentumsrecht an einem Grundstück. In diesem Fall kann ein rechtliches Interesse an der Kenntnis des Inhalts einer

Bauakte bestehen, um den Inhalt und Umfang dieser Grunddienstbarkeit nach dem Wortlaut und Sinn der Grundbucheintragung auslegen zu können. Der Umfang einer Dienstbarkeit kann nämlich mit der baulichen und nutzungsmäßigen Entwicklung der Grundstücke wachsen (VG Köln, Urteil vom 25.11.2005, Az: 27 K 6171/03).

Ist ein rechtliches Interesse an der Kenntnis der personenbezogenen Daten geltend gemacht, dürfen dem Informationszugang keine schutzwürdigen Belange der Betroffenen entgegen stehen. Solche schutzwürdigen Belange können nach der Systematik der Regelungen im IFG NRW lediglich Belange der Betroffenen sein, die über ihr Recht auf informationelle Selbstbestimmung hinausgehen, da dieses Recht bereits zum grundsätzlichen Ausschluss der Informationsweitergabe führt.

➧ Personenbezogene Angaben Dritter dürfen auch im Rahmen des IFG NRW nur in wenigen Ausnahmefällen herausgegeben werden.

18.9 Nicht jeder Aufwand darf in Rechnung gestellt werden

Hin und wieder tauchen einzelne Fälle auf, in denen öffentlichen Stellen nicht klar ist, ob und gegebenenfalls in welcher Höhe sie für eine gewährte Information eine Gebühr festsetzen sollen.

Nach dem Gebührentarif der Verwaltungsgebührenordnung zum Informationsfreiheitsgesetz NRW (VerwGebO IFG NRW) ist die Erteilung einer mündlichen oder einfachen schriftlichen Auskunft sowie einer Akteneinsicht in einem einfachen Fall gebührenfrei. Erst bei einem tatsächlich angefallenen erheblichen Vorbereitungsaufwand oder einem umfangreichen Verwaltungsaufwand dürfen Gebühren erhoben werden.

Als gebührenrelevanter Verwaltungsaufwand können etwa Recherchen oder Vorgespräche angesehen werden, die für den Informationszugang erforderlich sind. Auch das Abfassen eines schriftlichen Antwortschreibens, durch welches die begehrte Auskunft erteilt wird, zählt hierzu. Der Aufwand, der dadurch entsteht, dass eine öffentliche Stelle im Hinblick auf einen Informationsantrag die Anwendbarkeit des IFG NRW

zu prüfen hat, kann hingegen insoweit nicht berücksichtigt werden. Denn es obliegt einer Behörde von Amts wegen, sich im Rahmen ihres Verwaltungshandelns des jeweils anwendbaren Rechts zu vergewissern. Die hierfür entwickelten Bemühungen können der Bürgerin oder dem Bürger nicht entgeltlich angelastet werden (vgl. VG Arnsberg, Urteil vom 25.06.2004, Az: 11 K 1254/03, www.nrwe.de).

Nur ein erheblicher Verwaltungsaufwand kann eine Gebührenfolge auslösen. Im Rahmen des § 7 Gebührengesetz NRW (GebG NRW) wird darauf abgestellt, dass ein Verwaltungsaufwand bis zur zeitlichen Grenze von 15 Minuten als unerheblich zu qualifizieren ist. Gleiches gilt, wenn die durch die Informationsgewährung entstehenden Kosten nicht messbar oder so gering sind, dass sie den Verwaltungsaufwand der Gebührenerhebung nicht lohnen.

Für die Festsetzung der Höhe der Gebühr ist § 9 Abs. 1 GebG NRW maßgeblich. Danach sind bei der Festsetzung einer Gebühr, für die – wie hier – Rahmensätze vorgesehen sind, einerseits der mit der Amtshandlung verbundene Verwaltungsaufwand, andererseits der wirtschaftliche Wert oder sonstige Nutzen der Amtshandlung zu berücksichtigen. Für die Berechnung des zeitlichen Aufwands kann auf die Richtwerte für die Berücksichtigung des Verwaltungsaufwandes bei der Festlegung der nach dem GebG NRW zu erhebenden Verwaltungsgebühren in dem entsprechenden Runderlass des Innenministeriums zurückgegriffen werden. Hat die informationssuchende Person lediglich ein persönliches Interesse an der Kenntnis der Informationen, sollte sich dieser Umstand auf die Festsetzung gebührenmindernd auswirken. Außerdem ist die Billigkeitsklausel des § 2 VerwGebO IFG NRW zu berücksichtigen.

- Der allgemeine Informationszugang ist als subjektives Recht ausgestaltet und darf die Bürgerin oder den Bürger daher nicht unangemessen viel kosten.

18.10 Bei Nachfragen keine Nachforderungen

Sie wollen etwas wissen und stellen einen Informationsantrag. Eine Woche später haben Sie mehr Erkenntnisse zum Thema und stellen Zusatzfragen. Einige Tage später fallen Ihnen noch Ergänzungen ein. Für die Gebührenhöhe darf das nicht ausschlaggebend sein.

Gefragt worden war nach Einzelheiten im Zusammenhang mit der Abwasserbeseitigung und den dafür zu berechnenden Gebühren. Nachdem zunächst eine gebührenfreie Auskunft erteilt worden war, richteten die antragstellenden Eheleute innerhalb von drei Wochen drei Schreiben mit weiteren Nachfragen zu demselben Themenkomplex an die öffentliche Stelle. Nachdem die drei im Zusammenhang stehenden Schreiben bei der öffentlichen Stelle eingegangen waren, fertigte die Stadt zur Beantwortung drei separate Antwortschreiben mit drei Gebührenfestsetzungen und zwar in Höhe von 250, 100 und 200 Euro. Dies war nicht rechtens. Da die Anfragen jeweils Teilaspekte eines einheitlichen Themas innerhalb des begrenzten Zeitraums von nur drei Wochen betrafen und damit in einem unmittelbaren thematischen und zeitlichen Zusammenhang standen, handelte es sich der Sache nach nur um eine Anfrage, für deren Beantwortung auch nur eine einzige Gebührenfestsetzung hätte erfolgen dürfen, und zwar in dem dafür vorgesehenen Gebührenrahmen von 10 bis 500 Euro. Erst wenn in diesen Fällen ein Informationsantrag abschließend bearbeitet ist, handelt es sich bei einer erneuten Anfrage – auch wenn diese dasselbe Thema betrifft – um einen neuen Antrag, dessen Bearbeitung gegebenenfalls erneut eine Verwaltungsgebühr auslösen kann (VG Düsseldorf, Urteil vom 18.06.2004, Az: 26 K 6685/02).

➡ Werden mehrere in einem zeitlichen und thematischen Zusammenhang stehende Informationsanträge bearbeitet, darf lediglich eine einzige Gebührenfestsetzung im dafür vorgesehenen Gebührenrahmen erfolgen.

18.11 Umweltinformationsgesetz

Der Zugang zu Umweltinformationen soll jetzt auch in Nordrhein-Westfalen auf landesrechtlicher Ebene geregelt werden.

Dazu ist im Berichtszeitraum der Entwurf eines Gesetzes über den Zugang zu Umweltinformationen im Land Nordrhein-Westfalen (UIG NRW) in den Landtag eingebracht worden. Durch eine neue europäische Umweltinformationsrichtlinie war die Novellierung des Umweltinformationsgesetzes des Bundes notwendig geworden. Dieses Gesetz gilt jedoch nur für Bundesbehörden. Die Länder müssen daher für den Zugang zu Umweltinformationen bei den Landesbehörden eigene landesrechtliche Regelungen nach den Vorgaben der europäischen Richt-

linie treffen. Ein gemeinsamer Runderlass der Landesregierung vom 17. September 2005 bestimmt, dass für die Übergangszeit jedenfalls zum größten Teil die Zugangsregelungen unmittelbar aus der europäischen Umweltinformationsrichtlinie herzuleiten sind (MBl. NRW Nr. 46/2005 S. 1216 ff.).

Im landesrechtlichen Gesetzentwurf blieben bislang zwei Vorschläge der LDI unberücksichtigt. Um Missverständnisse zu vermeiden, sollte die überflüssige Klausel gestrichen werden, nach der es keiner Darlegung eines rechtlichen Interesses für einen Informationsantrag bedarf. Etwas wissen zu wollen, ist nach dem Gesetz nicht begründungsbedürftig. Das UIG NRW sollte unter Verständlichkeitsgesichtspunkten insoweit keine andere Formulierung wählen als das Informationsfreiheitsgesetz NRW (IFG NRW), das ohne eine solche Klausel auskommt. Außerdem soll das grundsätzliche Recht auf Wahl der Art des Informationszugangs (beispielsweise Akteneinsicht oder Auskunft) aufgeweicht werden können, wenn die öffentliche Stelle eine andere Art des Informationszugangs für angemessen hält. Sowohl das UIG des Bundes und das IFG des Bundes als auch das IFG NRW lassen eine Einschränkung des Wahlrechtes dagegen nur zu, wenn ein wichtiger Grund vorliegt. Davon sollte im UIG NRW nicht abgewichen werden.

- Zugangsanspruch und Art und Weise des Informationszugangs sollten im UIG NRW dem IFG NRW entsprechen.

Anhang

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Entschließung zwischen den Konferenzen

Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck! (15.02.2005)

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z.B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments "DNA-Analyse", weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung be-

jaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

69. Konferenz am 10./11. März 2005

Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Entschließung zur Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisa-

torischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind. Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Entschließung zwischen den Konferenzen

Zur Einführung biometrischer Ausweisdokumente (01.06.2005)

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützer Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

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

- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

70. Konferenz am 27./28. Oktober 2005

Eine moderne Informationsgesellschaft braucht mehr Datenschutz

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

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

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

cherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

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

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

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

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

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

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

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

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

Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

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

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

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

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

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

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

Keine Vorratsdatenspeicherung in der Telekommunikation

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

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

dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

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

Die von einigen Regierungen (z.B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten ("Einfrieren" auf Anordnung der Strafverfolgungsbehörden und "Auftauen" auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

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

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

Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

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

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

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

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

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

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

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

Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

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

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

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

Telefonieren mit Internettechnologie (Voice over IP – VoIP)

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

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

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbe-

zogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

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

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

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

Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

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

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

Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

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

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

Entschließung zwischen den Konferenzen

Sicherheit bei eGovernment durch Nutzung des Standards OSCI (15.12.2005)

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

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

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

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

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

71. Konferenz am 16./17. März 2006

Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

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

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

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

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

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshal-

ber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

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

Keine kontrollfreien Räume bei der Leistung von ALG II

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

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

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

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

Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

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

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

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

Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

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

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

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

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

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

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

Entschließung zwischen den Konferenzen

(bei Enthaltung von Schleswig-Holstein)

Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren (11.10.2006)

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

gangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

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

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

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

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

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,

- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,

- wird den Nutzenden keine "Warnfunktion" mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und

- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

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

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,

- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,

- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

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

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

72. Konferenz am 26./27. Oktober 2006

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

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

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

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

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

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

Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte "Schulleben" ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so

genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

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

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

Im übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.

- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.

- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

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

Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise,

Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

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

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

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

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

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

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

- Keine heimliche Profilbildung
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der

Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

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

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

Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

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

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

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

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum inter-

nationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Entschließungen der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)

Jetzt nicht kneifen – das Informationsfreiheitsgesetz endlich verabschieden! (27.05.2005)

Nachdem die zweite und dritte Lesung des Entwurfs für das Informationsfreiheitsgesetz im Deutschen Bundestag auf Anfang Juni 2005 verschoben wurde, fordert die Arbeitsgemeinschaft der Informationsbeauftragten, die Verabschie-

dung des Gesetzes nicht länger hinauszuzögern. Mit seinem überkommenen Amtsgeheimnis bleibt Deutschland sonst europäisches und internationales Schlusslicht in Sachen Transparenz.

Seit die Bundesregierung 1998 angekündigt hatte, ein Informationsfreiheitsgesetz für Bundesbehörden auf den Weg zu bringen, haben die Gegnerinnen und Gegner einer transparenten Verwaltung das Gesetzesvorhaben kontinuierlich torpediert. Jüngst befürchteten die Krankenkassen unter anderem Wettbewerbsverzerrungen durch Offenlegungspflichten und Überschneidungen mit bestehenden Informationsansprüchen. Die berechtigten Interessen der Krankenkassen an der Geheimhaltung ihrer Geschäftsgeheimnisse sowie der Sozialdaten ihrer Patientinnen und Patienten werden von dem vorgelegten Gesetzentwurf jedoch wirksam geschützt; ebenso regelt der Entwurf das Verhältnis zu vergleichbaren Informationsansprüchen klar und eindeutig. Es gibt also keinen Grund für eine Verschiebung der Diskussion im Parlament. Die Informationsbeauftragten fordern daher, dass der Deutsche Bundestag – trotz der aktuellen Debatte um vorgezogene Neuwahlen – dieses wichtige Gesetz noch verabschiedet, damit es spätestens Anfang 2006 in Kraft treten kann. Das Informationsfreiheitsgesetz soll den Bürgerinnen und Bürgern endlich freien Zugang zu öffentlichen Informationen auch bei Bundesbehörden verschaffen.

Offenlegung von Aktivitäten und Bezügen der Mitglieder öffentlicher Organe und Gremien (15.11.2005)

Ob ein Mitglied einer kommunalen Vertretung oder einer Landesregierung den Vorsitz in einer bestimmten Organisation führt oder in einem Aufsichtsrat eines Unternehmens sitzt, kann von erheblichem Einfluss auf die Entscheidungsfindung der Kommune oder des Landes sein. Ohne Kenntnis solcher Aktivitäten öffentlicher Entscheidungsträger ist Verwaltungshandeln häufig gar nicht nachvollziehbar. Insbesondere Informationen über die Höhe der zusätzlichen Vergütung können Aufschluss über die Motivation für ein bestimmtes Abstimmungs- oder Entscheidungsverhalten geben. Derzeit werden solche Informationen allerdings noch geheim gehalten.

Die Transparenz von "nebenamtlichen" Aktivitäten und Bezügen öffentlicher Entscheidungsträger ist ein wichtiges Kontrollinstrument, das auch in Geschäftsordnungen von Landtagen, in Haushaltsordnungen oder Gemeindeordnungen sowie in Korruptionsbekämpfungsgesetzen mehr und mehr Eingang findet. Die Verpflichtung, solche Aktivitäten und Bezüge offen zu legen, erhöht zudem die Akzeptanz der Entscheidungen öffentlich Bediensteter.

Die Arbeitsgemeinschaft der Informationsbeauftragten fordert daher die Gesetzgeber in den Ländern auf, eine allgemeine Offenlegungspflicht für "nebenamtliche" Aktivitäten und Vergütungen öffentlicher Entscheidungsträger gesetzlich festzulegen.

Transparenz in öffentlichen Unternehmen gefordert (15.11.2005)

Private, börsennotierte Aktiengesellschaften sind seit kurzem verpflichtet, die Vergütungen der Vorstandsmitglieder offen zu legen. Aktionärinnen und Aktionäre können somit erfahren, ob der Vorstand einer Aktiengesellschaft ange-

messene Bezüge erhält. Dieselben Rechte sollen auch Bürgerinnen und Bürger gegenüber öffentlichen Unternehmen geltend machen können.

Die Bürgerinnen und Bürger haben einen Anspruch darauf, zu wissen, wie hoch die Vergütungen für die einzelnen Mitglieder der Verwaltungsräte, Aufsichtsräte und Geschäftsführungen von privatrechtlichen Gesellschaften sind, die sich mehrheitlich aus Vertretern des Bundes, der Länder oder der Kommunen zusammensetzen. Eine Veröffentlichung der Bezüge in den Jahresabschlüssen und in den Beteiligungsberichten der öffentlich-rechtlichen Körperschaften verbessert die Transparenz über die Verwendung von Steuergeldern und stärkt die Akzeptanz öffentlicher Unternehmen.

Die Arbeitsgemeinschaft der Informationsbeauftragten fordert die Gesetzgeber des Bundes und der Länder daher auf, eine entsprechende Offenlegungspflicht auch für öffentlich kontrollierte Unternehmen festzulegen. Die Regelungen des jüngst verabschiedeten Vorstandsvergütungs-Offenlegungsgesetzes für private Aktiengesellschaften können hierfür als Maßstab dienen.

Verbraucherinformationsgesetz nachbessern (26.06.2006)

Die Informationsfreiheitsgesetze im Bund und in einigen Ländern stellen einen wichtigen Beitrag zu mehr Transparenz, Bürgerbeteiligung und gesellschaftlicher Offenheit dar. Folgerichtig bedarf es auch einer größeren Transparenz im Bereich des Verbraucherschutzes. Unter bestimmten Voraussetzungen sollte ein unmittelbarer Informationsanspruch gegen private Unternehmen gesetzlich verankert werden. Auch Daten, die in Unternehmen gespeichert werden, berühren unmittelbar Rechte der Bürgerinnen und Bürger und damit ihr Lebensumfeld. Dies gilt insbesondere bei verbraucherschutzrelevanten Produkten sowie Produkten des Energiemarktes. Die Transparenzrechte der Bürgerinnen und Bürger sollten deshalb in diesem Bereich ebenfalls durch Auskunftsansprüche gesetzlich geregelt werden.

Der Entwurf des Verbraucherinformationsgesetzes, der derzeit im Deutschen Bundestag beraten wird, schafft aber nur unzureichende Transparenzregelungen, die außerdem die Unternehmen nicht ausreichend zur Offenlegung der verbraucherschutzrelevanten Daten verpflichten. Die Informationsfreiheitsbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Verbraucherinformationsschutzgesetz erste Schritte für mehr Transparenz in der Wirtschaft umzusetzen.

Dazu gehören zumindest folgende Verbesserungen:

- die Erweiterung des Gesetzes über Lebens- und Futtermittel hinaus auf sonstige Produkte und Dienstleistungen,
- die Schaffung eines unmittelbaren Rechtsanspruchs auf Informationszugang gegenüber Unternehmen,
- die Schaffung einer Abwägungsregelung zwischen den unterschiedlichen Interessen, die unter Beachtung der tatsächlichen Betriebs- und

Geschäftsgeheimnisse der Unternehmen den Betroffenen den Informationsanspruch sichert; amtlich festgestellte Verstöße der Unternehmen gegen verbraucherschutzrelevante Regelungen dürfen dabei nicht als Betriebs- und Geschäftsgeheimnis geltend gemacht werden,

- die Reduzierung der Ausnahmen vom Informationszugang auf wesentliche Ausnahmen und eine verbraucherschutzfreundliche Ausgestaltung des Verfahrens,

- Höchstgrenzen bei der Regelung von Gebühren für die Beauskunftung durch die Betroffenen.

Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 08./09. November 2006

SWIFT: Datenübermittlung im SWIFT-Verfahren in die USA

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFTRechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zur Zeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US–Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.

Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen – zum Beispiel mit Hilfe von Hintergrundsystemen – später einer konkreten Per-

son zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird – insbesondere wegen der geringen Größe der RFID-Chips – künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereichhalten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz / Benachrichtigungspflicht

Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht

Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung "hinter dem Rücken" der Betroffenen darf es nicht geben.

Deaktivierung

Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr er-

forderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit

Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Verschlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung

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

Stichwortverzeichnis

Datum: .....

Absender/in:

.....
(Vorname, Name)

.....
(ggf. Behörde)

.....
(Straße, Hausnummer)

.....
(PLZ, Ort)

Landesbeauftragte
für Datenschutz und Informations-
freiheit Nordrhein-Westfalen
Kavalleriestr. 2–4

40213 Düsseldorf

E-Mail: pressestelle@ldi.nrw.de

Betr.: Informationsmaterial

Hiermit bitte ich um Übersendung folgender Broschüren:

_____ Aufkleber zum Adressenhandel

_____ Datenscheckheft

_____ den neuesten Datenschutzbericht

_____ den ..... Datenschutzbericht

_____ Datenschutzgerechtes eGovernment

_____ Faltblatt "Achtung Kamera – Videoüberwachung durch private Stellen"

_____ Faltblatt "Adressenhandel und unerwünschte Werbung"

_____ Faltblatt "Datenschutz im Verein"

_____ Faltblatt zum Informationsfreiheitsgesetz NRW: "Informieren – Einmischen – Mitreden"

_____ Faltblatt "Handels- und Wirtschaftsauskunfteien"

_____ Handys – Komfort nicht ohne Risiko

_____ Living by numbers – Leben zwischen Statistik und Wirklichkeit

_____ Total transparent – Zukunft der informationellen Selbstbestimmung?

_____ Die Gedanken sind frei – Hirnforschung und Persönlichkeitsrechte

_____ Orientierungshilfe "Behördliche Datenschutzbeauftragte"

_____ Orientierungshilfe "Datenschutz im Personalrat"

_____ Orientierungshilfe "Datenverarbeitung im Auftrag"

_____ Orientierungshilfe "Datenschutz und Datensicherheit beim Betrieb von IT-Systemen"

_____ Orientierungshilfe "Schützen Sie Ihre Daten"

_____ Orientierungshilfe "Telefax"

_____ Orientierungshilfe "Unterlagenvernichtung"

_____ Orientierungshilfe "Ich sehe das, was Du auch tust!– Videoüberwachung an und in Schulen"

_____ Orientierungshilfe "Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz"

Mit freundlichen Grüßen