Neunzehnter Datenschutz- und Informationsfreiheitsbericht

der

Landesbeauftragten für Datenschutz

und Informationsfreiheit

Nordrhein-Westfalen

Bettina Sokol

für die Zeit vom 1. Januar 2007

bis zum 31. Dezember 2008

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 2009

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorbemerkung

Leider ist bislang weder ein Silberstreif am Horizont noch Licht am Ende des Tunnels zu entdecken. Um die tatsächliche Gewährleistung des Datenschutzes in Nordrhein-Westfalen ist es objektiv schlecht bestellt. Das hat viele verschiedene Ursachen, nicht zuletzt aber auch diejenige, dass meine Dienststelle personell unzureichend ausgestattet ist. Damit keine Missverständnisse aufkommen: Meine Mitarbeiterinnen und Mitarbeiter sind hoch motiviert, engagiert und erledigen ihre Arbeit effizient. Dafür sei ihnen in diesem außergewöhnlich schwierigen Berichtszeitraum auch öffentlich ganz besonders herzlich gedankt. Denn sich die Arbeitsmotivation zu erhalten, ist angesichts der objektiven Umstände wahrlich nicht einfach.

Das Ergebnis einer Organisationsuntersuchung bestand 2002 in der Feststellung eines signifikanten personellen Mehrbedarfs für die Dienststelle, um überhaupt die Beratungs- und Kontrolltätigkeit betreffend den Datenschutz bei öffentlichen Stellen und in der Privatwirtschaft sowie die Sicherstellung der Informationsfreiheit gewährleisten zu können. Seitdem sind allein die schriftlichen Anfragen und Beschwerden um 35 Prozent gestiegen, vom sonstigen Arbeitsanfall ganz zu schweigen – telefonischer Service, Vorträge in öffentlichen Veranstaltungen, Podiumsdiskussionen, referierende Beteiligung an Fortbildungsmaßnahmen und dergleichen mehr sind hier zu nennen. Auch die Intensität und damit das Arbeitsaufkommen bei der Beratungstätigkeit, bei Projektbegleitungen, aber auch für Kontrolltätigkeiten ist deutlich angewachsen. Aller Orten werden im Datenschutz und bei der Datensicherheit Defizite und Missstände von einem Ausmaß erkennbar, dessen Beseitigung eigentlich keinen Aufschub duldet.

In einem Land mit 18 Millionen Einwohnerinnen und Einwohnern, 100.000 Vereinen sowie über 700.000 Unternehmen und einer kaum überschaubaren Anzahl von öffentlichen Stellen kann es nicht angemessen sein, für diese Aufgaben nur 45 Stellen im Haushaltsplan des Landes auszuweisen. 2006 waren es noch 50 Stellen. 2008 war das Jahr, in dem seit längerer Zeit die meisten Datenschutzskandale ans Licht der Öffentlichkeit gekommen sind: Ausspionierung von Beschäftigten im Einzelhandel bis in intimste Details, illegale Videoüberwachung am Arbeitsplatz, der Verdacht auf systematische Bespitzelung von Interessenvertretungen unter Verletzung des Fernmeldegeheim-

nisses und der kriminelle Handel von Kontodaten mit vermutlich weit mehr als 21 Millionen betroffener Opfer. Vor diesem Hintergrund ist die Stellenausstattung meiner Behörde für die Sicherstellung des Datenschutzes und der Informationsfreiheit in Nordrhein-Westfalen nicht ausreichend. Demgegenüber kann die Darstellung des Innenministeriums NRW, dass meine Dienststelle die bestausgestatteste in der Bundesrepublik sei, angesichts der tatsächlichen Verhältnisse nicht als sachlich zutreffend bezeichnet werden. Die Landesbeauftragten haben in den jeweiligen Ländern durchaus verschiedene Aufgaben: Manche sind nur für den Datenschutz im öffentlichen Bereich zuständig, manche auch für die Privatwirtschaft und manche – wie in Nordrhein-Westfalen – haben sich darüber hinaus um die Informationsfreiheit zu kümmern. Außerdem handelt es sich um höchst unterschiedliche Größenklassen betreffend die Zahl der Einwohnerinnen und Einwohner sowie der öffentlichen und privaten Stellen im jeweiligen Land. Dies ins richtige Verhältnis gesetzt, muss bei seriöser Betrachtung daher leider festgestellt werden, dass hinsichtlich der personellen Ausstattung Nordrhein-Westfalen mit Niedersachsen gemeinsam das Schlusslicht unter den Landesbeauftragten bildet. Inwieweit das die nach § 21 Abs. 4 Datenschutzgesetz NRW gesetzlich gebotene notwendige Personalausstattung für die Aufgabenerfüllung darstellt, mag jede oder jeder selbst beurteilen. Zweifel daran, ob mit einem Stellenabbau von 10 Prozent in den letzten Jahren und derzeit noch 45 Stellen eine auch nur ansatzweise wirksame Datenschutzkontrolle mit den mindestens notwendigen Stichprobenprüfungen stattfinden kann, sind nicht nur erlaubt, sondern offenkundig. Der Schutz des Persönlichkeitsrechts der Menschen in Nordrhein-Westfalen, des in der Landesverfassung verankerten Grundrechts auf Schutz der personenbezogenen Daten besitzt demnach, wenn es um eine angemessene Ausstattung geht, weder für die Landesregierung noch für die Landtagsmehrheit einen über bloßes Wortgeklingel hinausgehenden Stellenwert.

Auf der Seite der "Nachfrage" nach unseren Angeboten sind demgegenüber nicht nur die rasant gestiegene Arbeitsbelastung zu nennen, sondern auch die vielen positiven Rückmeldungen, die wir aus der Bevölkerung für unsere Arbeit erhalten. Zu den jährlich gemeinsam mit dem Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster veranstalteten Tagungen gab es zudem erfreulicherweise 2007 mit dem Thema "Persönlichkeit im Netz: Sicherheit – Kontrolle – Transparenz" und 2008 zum Be-

schäftigtendatenschutz mit dem Titel: "GPS, Internet und Video – Datenschutz am Arbeitsplatz" einen noch größeren Andrang als in den Jahren zuvor.

1 Zur Situation von Datenschutz und Informationsfreiheit

Datenschutzverstöße in Serie empören seit dem Frühjahr 2008 die Öffentlichkeit. Zur Erinnerung: Etliche Regionalgesellschaften eines großen deutschen Einzelhandelsunternehmens hatten Detekteien damit beauftragt, die eigenen Arbeitnehmerinnen und Arbeitnehmer des Unternehmens zu beobachten. Teilweise wurden die Beschäftigten sogar mit Kameras und Mikrofonen über intime Details ihres Privatlebens ausgeforscht. Berichtet wurde etwa über Gesundheitsprobleme, Aussehen, Verhaltensweisen, Liebesbeziehungen, Arbeitslosigkeit in der Verwandtschaft und Scheidungen. Respekt vor der Privatsphäre sieht anders aus. Auch ein Großbetrieb in der fleischverarbeitenden Branche fiel durch eine unverhältnismäßige Überwachung der eigenen Arbeitnehmerinnen und Arbeitnehmer auf. Hunderte von Videokameras hatten ständig "ein Auge auf die Beschäftigten" – selbst im Sozialraum. Die von der LDI NRW gegen die Unternehmen verhängten Bußgelder sind bestandskräftig.

Im weiteren Verlauf des Jahres riss die Kette der Datenskandale nicht ab: Die Staatsanwaltschaft nahm Ermittlungen gegen ein Unternehmen in der Telekommunikationsbranche auf, das im Verdacht steht, illegal Gesprächsverbindungen ausgewertet und Gesprächsinhalte belauscht zu haben. Genau diesem Unternehmen sind in seiner Mobilfunksparte vor etwa zweieinhalb Jahren mehr als 17 Millionen Datensätze gestohlen worden. Es ging um Adressen und Telefonnummern von ungefähr der Hälfte aller Kundinnen und Kunden des Unternehmens. Dies wirft Fragen nach der Datensicherheit auf, die sich nach denjenigen Pressemeldungen vermehren, nach denen es ohne großen Aufwand möglich gewesen sein soll, sich in das aktuelle Kundensystem des Unternehmens einzuloggen und dort Daten nicht nur lesen, sondern auch verändern zu können – zum Beispiel Bankverbindungen. Längere Zeit im Internet frei zugänglich waren aufgrund von Unachtsamkeiten auch die Meldedaten von möglicherweise einer halben Million Menschen. Der illegale Handel mit Kontodaten zog sich jedoch wie ein roter Faden durch den Rest des Jahres. Unautorisierte Kontoabbuchungen hatten die Republik aufgeschreckt. Mal ging es um 70.000 Datensätze, die auf dem Schwarzmarkt kursierten, mal um sechs Millionen und Anfang Dezember 2008 wurde darüber berichtet, dass die Bankverbindungen von 21 Millionen Menschen illegal im Um-

lauf seien. Es wäre nicht überraschend, wenn sich demnächst herausstellen sollte, dass praktisch mit den Daten aller Personen, die ein Konto besitzen, illegal gehandelt wird.

Kurz vor Redaktionsschluss des Berichts ging Mitte Dezember 2008 die Meldung von vagabundierenden Kreditkartendaten durch die Medien. Über Namen, Adressen und Kontoverbindungen hinaus stehen die Abrechnungsdaten des Kaufverhaltens zehntausender Menschen noch auf einer höheren Qualitätsstufe, da mit ihnen ein Teilprofil des Konsums der insoweit "gläsernen" Betroffenen gebildet wird. Wenn es zutreffen sollte, dass das Unternehmen, dem die Daten abhanden gekommen sein sollen, ebenfalls an der Erstellung und Einführung der elektronischen Gesundheitskarte beteiligt ist, verstärken sich die ohnehin vorhandenen Befürchtungen hinsichtlich der Sicherheit der hochsensiblen Gesundheitsdaten noch um ein Vielfaches.

Personenbezogene Daten sind zu einem Wirtschaftsgut geworden, mit dem sich – je nach Masse, Aussagekraft oder Identifikationsmöglichkeit – viel Geld machen lässt. Betrügereien und Identitätsdiebstähle sind bei sorglosem Umgang mit den eigenen Daten in der Online-, aber auch in der Offline-Welt inzwischen zu einem handfesten Risiko geworden. Dazu beigetragen hat die bisherige Rechtslage, die den Adresshandel dann legal ermöglicht, wenn die betroffenen Personen dem nicht ausdrücklich widersprochen haben. Darüber sind Datenschützerinnen und Datenschützer schon lange erzürnt. Denn es hat sich seit geraumer Zeit ein "Graubereich" des Datenhandels entwickelt, dem die Aufsichtsbehörden zum einen wegen der Rechtslage und zum anderen wegen der fehlenden personellen Kapazitäten nicht wirklich Einhalt gebieten können. So wurde schon im Bericht 2005 unter 5.2 der äußerst dubiose Umgang eines kontrollierten Call-Centers mit illegalen Kontodaten- und Adresslisten dargestellt. Der von der LDI NRW gegen das Unternehmen bereits 2004 gestellte Strafantrag führte jedoch lediglich dazu, dass die Staatsanwaltschaft 2008 – also immerhin vier Jahre später – ankündigte, das Verfahren aus prozesstaktischen Erwägungen gegen Zahlung einer geringen Geldbuße einstellen zu wollen. Dabei wurde von der Staatsanwaltschaft eingeräumt, dass bei den Ermittlungen der schwer nachzuweisende Betrugsvorwurf im Vordergrund stand. Dagegen wurde die Prüfung der von der LDI NRW in Betracht gezogenen datenschutzrechtlichen Strafnorm vernachlässigt.

Nach Jahren der Untätigkeit ist jetzt auch die Politik aufgewacht, hat aber leider die Dimension der Problematik nicht in voller Gänze erfasst. Der jetzt vorliegende Gesetzentwurf aus dem Bundesinnenministerium zur Novellierung des Bundesdatenschutzgesetzes nimmt die notwendigen Maßnahmen nur äußerst unzureichend und halbherzig in Angriff. Zwar wird endlich abgeschafft, dass die Menschen einem Handel mit ihren Daten ausdrücklich widersprechen müssen. Künftig soll der Adresshandel grundsätzlich nur noch mit der Einwilligung der Betroffenen erlaubt sein. Das Gesetz sieht aber erstens zu viele Ausnahmen vor – etwa für die Spendenwerbung karitativ tätiger Organisationen – und räumt zweitens den Unternehmen eine viel zu lange Übergangsfrist von drei Jahren zur Umstellung ihrer Geschäftsprozesse ein. Auch die im Falle von Datenpannen, also Datenlecks oder Datenklau vorgesehene Informationspflicht der Unternehmen gegenüber den Betroffenen und der jeweils zuständigen Aufsichtsbehörde greift nur, wenn bestimmte Daten betroffen sind, beispielsweise Daten zu Bank- oder Kreditkartenkonten oder die im Bundesdatenschutz als besonders sensibel eingestuften Datenarten. Die Benachrichtigungspflicht ist weiter daran geknüpft, dass neben der unrechtmäßigen Kenntnisnahme der Daten durch Dritte schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Nicht aufgenommen in den Gesetzentwurf ist die dringend erforderliche Kennzeichnungspflicht über die Herkunft der Daten: Wann sind sie von wem erstmals nachweislich mit der Einwilligung der betroffenen Personen erhoben worden und wohin sind sie dann gewandert? Nur wenn diese Informationen Pflicht sind, gibt es überhaupt eine aussichtsreiche Chance, den illegalen Datenströmen auf die Spur zu kommen und sie entsprechend zu ahnden. Auch viele andere geforderte Instrumente, die den Aufsichtsbehörden in ihrer täglichen Praxis sehr nutzen könnten, sind in dem Gesetzentwurf nicht berücksichtigt worden (mehr dazu unter 6.2). Besonders bedauerlich ist, dass es den Aufsichtsbehörden nach wie vor nicht möglich sein soll, unbefugte Datenverarbeitungen zu untersagen. Die bloße Verhängung von Bußgeldern reicht insoweit nicht aus. Nur am Rande erwähnt sei das ebenfalls im Entwurfspaket vorgesehene Auditgesetz, das diesen Namen im Grunde genommen nicht verdient, und das in dieser Form nicht verabschiedet werden sollte.

Darauf, dass dem allgegenwärtigen Misstrauen eine Präventionslogik folgt, der die Maßlosigkeit bezüglich der Datengier innewohnt, ist bereits in den Situationsbeschreibungen der Berichte 2005 und 2007 hingewiesen worden. Diese Tendenz hat sich verstärkt. Technische Maßnahmen werden insoweit als Allheilmittel gepriesen, sind jedoch häufig keine Lösung, sondern Teil des Problems. Dies gilt beispielsweise für die immer stärker ausufernde Videoüberwachung sowohl im öffentlichen wie auch im nicht-öffentlichen Bereich. Von der öffentlichen Diskussion eher unbemerkt entwickelt sich die Technik rasant weiter. Die maschinelle Analyse "auffälligen Verhaltens" macht ebenso Fortschritte wie die automatische Gesichtserkennung. In Kombination mit der Erfassung und Speicherung biometrischer Merkmale – etwa dem digitalen Foto in den neuen Ausweisdokumenten – eröffnen sich hier enorme Möglichkeiten der Personenkontrolle. Erst recht wenn schon Supermärkte, Videotheken oder gar Kindergärten auf biometrische Zugangs- oder Bezahlungsfunktionalitäten setzen, werden die Kundinnen und Kunden von morgen schon heute dazu erzogen und daran gewöhnt, Fingerabdruck, Gesichtserkennung und Irisscans als Selbstverständlichkeiten zu empfinden.

Mit der Speicherung kaum vorstellbar großer Bestände personenbezogener Daten, zunehmend in privater Hand, sind ebenso große Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Bei Kontrollen der Datensicherheit sind in öffentlichen wie in nicht-öffentlichen Stellen immer wieder teilweise schwerwiegende Mängel festzustellen. Nicht stattfindende Datenverschlüsselung, unzureichende Zugriffs- und Berechtigungsregelungen oder gar das komplette Fehlen eines Datensicherheitskonzepts sind leider keine Seltenheit. Darauf, ob dies aus Unkenntnis, aus Schlamperei oder aufgrund mangelnder Kapazitäten stattfindet, kann es dabei nicht ankommen, denn objektiv stellen Datensicherheitsmängel immer gleichsam eine Einladung zum Datenmissbrauch dar. Je größer und sensibler die Datenbestände sind, umso höher ist auch die Missbrauchsgefahr.

Es wächst aber ebenso das Risiko des vermeintlich oder tatsächlich legalen behördlichen Zugriffs auf solche Datenbestände. So hatte sich der Staat mit der Verpflichtung der Telekommunikationsanbieter zur anlasslosen Vorratsdatenspeicherung aller Telekommunikationsverkehrsdaten für die Dauer von sechs Monaten auch das Recht eingeräumt, auf diese Daten unter bestimmten Umständen zugreifen zu

können – und war dabei zu weit gegangen. Erstmals im März 2008 erließ das Bundesverfassungsgericht eine – mittlerweile verlängerte – einstweilige Anordnung, mit der der behördliche Zugriff auf diese Datenbestände vorläufig beschränkt wurde und derzeit den Strafverfolgungsbehörden nur bei der Ermittlung von schweren Straftaten nach dem Straftatenkatalog der Strafprozessordnung möglich ist, also wenn auch das Abhören der Telekommunikation erlaubt wäre. Im Bereich der Gefahrenabwehr ist der Datenabruf nach einem weiteren Eilbeschluss aus dem November 2008 nur zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zulässig. Auch den Befugnissen der Nachrichtendienste wurden engere Grenzen gezogen.

In solchen Eilverfahren entscheidet das Gericht allein aufgrund einer Folgenabwägung. Unjuristisch ausgedrückt, lässt es sich dabei von folgender Frage leiten: "Was ist schlimmer: Ein verfassungsmäßiges Gesetz, das nicht angewendet werden darf oder ein mit dem Gesetzesvollzug stattfindender verfassungswidriger Eingriff in die Grundrechte mit den damit verbundenen negativen Folgen für die Einzelnen und die Demokratie?" Die weit über 34.000 gegen die Vorratsdatenspeicherung anhängigen Verfassungsbeschwerden sind in der Hauptsache vom Gericht noch zu entscheiden. Mit den immer wieder – auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder – geltend gemachten verfassungsrechtlichen Bedenken gegen die anlasslose Bevorratung von Telekommunikationsverkehrsdaten wird sich das Bundesverfassungsgericht also noch befassen. Es hat der Vorratsdatenspeicherung in den Eilentscheidungen immerhin schon die Wirkung eines erheblichen "Einschüchterungseffekts" bescheinigt.

Im Februar 2008 hat das Bundesverfassungsgericht zudem die neue Regelung im nordrhein-westfälischen Verfassungsschutzgesetz zur so genannten "Online-Durchsuchung" für verfassungswidrig und nichtig erklärt. Damit sollte es dem Verfassungsschutz ermöglicht werden, wie ein "Hacker" mit Einsatz technischer Mittel heimlich auf gespeicherte Daten in Computern und in anderen informationstechnischen Systemen Zugriff nehmen zu können. Die bereits im Gesetzgebungsverfahren geäußerten und im Bericht 2007 unter 1 und 8 dargestellten verfassungsrechtlichen Bedenken gegen diese neue Befugnis waren vom Innenministerium NRW und von der Landtagsmehrheit unberücksich-

tigt geblieben. Das Bundesverfassungsgericht stellt in seinem Urteil fest, dass die betreffende Regelung nicht dem verfassungsrechtlichen Gebot der Normenklarheit genügt und unverhältnismäßig ist. Auch sind darin keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung getroffen worden. Für die Prüfung dieser altbekannten verfassungsrechtlichen Anforderungen hätte es im Grunde genommen keiner mündlichen Verhandlung mit der Anhörung etlicher, gerade auch technisch kundiger, sachverständiger Personen bedurft. Das Gericht nahm das Verfassungsschutzgesetz NRW jedoch zum Anlass, Maßstäbe für die bundesweit geführte Diskussion um die "Online-Durchsuchung" zu erarbeiten. 25 Jahre nachdem das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht und aus der Menschenwürde das Grundrecht auf informationelle Selbstbestimmung abgeleitet hatte, entwickelte es aus denselben Grundlagen eine Art "Schwester" für dieses Grundrecht, nämlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Im Ergebnis sind danach "Online-Durchsuchungen" nur in sehr engen verfassungsrechtlichen Grenzen überhaupt zulässig. Von besonderer Bedeutung ist außerdem, dass das Gericht den objektiv-rechtlichen Grundrechtsgehalt stark betont. Es stellt einen staatlichen Schutzauftrag fest, Vertraulichkeit und Integrität informationstechnischer Systeme so zu gewährleisten, dass auch die technisch nicht so versierten Nutzerinnen und Nutzer in ihrer grundrechtlichen Entfaltung gerade angesichts der künftigen technischen Entwicklung wirksam geschützt sind – wie etwa beim Cloud Computing, bei dem sich die Daten und Anwendungen nicht mehr auf dem lokalen Rechner befinden, sondern auf im Netz liegenden Servern. Hier ist der Gesetzgeber gefragt.

Mit großer Besorgnis ist das zügige Wachstum des Datenbestands in der DNA-Analysedatei zu sehen. Anfang Dezember 2008 betrug die Gesamtsumme der eingespeicherten Datensätze fast 750.000. Von Nordrhein-Westfalen aus erfasst waren 108.223 DNA-Identifizierungsmuster und die Profile von 27.021 Spuren. Es bedarf gründlicher Sorgfalt bei der Prüfung, ob die Voraussetzungen für die Aufnahme in die Datei tatsächlich vorliegen, auch und gerade wenn die Einspeicherung aufgrund einer Einwilligung der betroffenen Personen erfolgen soll. Bei jugendlichen Ersttätern im pubertären Alter hat die Prüfung nach der Rechtsprechung des Bundesverfassungsgerichts besonders streng zu sein und unter anderem auch die Erkenntnisse der Krimino-

logie über jugendtypische Delikte sowie die möglichen Auswirkungen einer Speicherung auf die weitere Entwicklung von Teenagern zu berücksichtigen. Das Gericht spricht insoweit sogar von einer möglicherweise drohenden "Brandmarkung" der Jugendlichen, die ihre Chancen für ein straffreies Leben einschränken kann. Es ist also Wachsamkeit geboten, damit sich die Verhältnisse hier nicht so entwickeln wie in Großbritannien. Dort sind mit 4,4 Millionen Personen ungefähr sieben Prozent der Gesamtbevölkerung registriert, davon über eine Millionen Minderjähriger, von denen 150.000 Kinder zum Speicherbeginn noch unter 13 Jahre alt waren und 700.000 Teenager zwischen 13 und 15 Jahren. Für eine unbefristete Speicherung in der Datei genügt der bloße Verdacht einer Straftat, selbst wenn die verdächtigte Person vor Gericht freigesprochen wurde. Der Umfang der wöchentlich um 15.000 Profile wachsenden Datenbank soll sich nach Prognosen bis 2012 verdoppelt haben und ein Sechstel der erwachsenen Bevölkerung erfassen. Es ist außerordentlich zu begrüßen, dass der Europäische Gerichtshof für Menschenrechte die britische Praxis betreffend Kinder und Freigesprochene im Dezember 2008 für menschenrechtswidrig erklärt hat.

Die schon im Bericht 2007 als alarmierend bezeichnete Tendenz zu Maßlosigkeit und zweifelhaftem Präventionsdenken auf Kosten des Datenschutzes hat sich sowohl im öffentlichen Bereich wie auch in der Privatwirtschaft weiter verstärkt. Nicht umsonst musste das Bundesverfassungsgericht 2008 den Gesetzgebern im Bund und in den Ländern gleich mehrfach die verfassungsrechtlichen Grenzen grundrechtsverletzender Gesetzgebung aufzeigen. Zu nennen sind nur die "Online-Durchsuchung", der anlasslose Abgleich von Kraftfahrzeugkennzeichen und die Vorratsdatenspeicherung. Es ist zu hoffen, dass die Reihe der verfassungsgerichtlichen Entscheidungen ebenso wie die Serie der eingangs genannten Datenskandale hier ein Umdenken bewirkt, dem Taten zur Stärkung des Datenschutzes folgen.

Generell ist im Bereich der Informationsfreiheit eine positive Entwicklung festzustellen. Dies gilt nicht nur für die Anwendung des Informationsfreiheitsgesetzes selbst, sondern auch für die wachsende Zahl bereichsspezifischer Informationszugangsgesetze. Die öffentlichen Stellen sind zunehmend bestrebt, die Zielsetzung des Informationsfreiheitsgesetzes Nordrhein-Westfalen zu verwirklichen, also eine transparente Verwaltung zu schaffen und insbesondere die Nachvollziehbar-

keit behördlicher Entscheidungen zu erhöhen. Hierzu ist allerdings eine Aktenführung unabdingbar, die eine rasche Umsetzung von Zugangsrechten ohne großen Aufwand ermöglicht. Mit zunehmender Sicherheit im Umgang mit dem Gesetz werden schon heute Informationsanträge selbstverständlicher entgegen genommen, in Betracht kommende Verweigerungsgründe sorgfältiger geprüft und Ablehnungen nachvollziehbarer als anfangs begründet. Gleichwohl bleibt die Zahl der hier eingehenden Anfragen und Beschwerden recht konstant. Hartnäckige Abwehr ist meist nur noch bei Einrichtungen und Organisationen zu verzeichnen, die im Selbstverwaltungsbereich tätig oder als Private mit öffentlichen Aufgaben betraut sind.

Inzwischen stützen nicht nur diverse Entscheidungen des Oberverwaltungsgerichts Münster die Anwendung und Umsetzung des Landesinformationsfreiheitsgesetzes. In zwei streitigen Fällen, die die Informationspflicht der Industrie- und Handelskammern und die Offenlegung kommunaler Rechnungsprüfungsunterlagen betrafen, hat auch das Bundesverwaltungsgericht die Anwendbarkeit dieses Gesetzes bejaht. Die Zielsetzung des allgemeinen Informationszugangsrechts findet sich inzwischen auch im neuen Umweltinformationsgesetz Nordrhein-Westfalen und im Verbraucherinformationsgesetz Das Agrar- und Fischereifonds-Informationen-Gesetz, in dem eine webgestützte Veröffentlichung von geleisteten Subventionen und deren Empfängerinnen und Empfängern bestimmt wird, ist ebenfalls eine konsequente Weiterentwicklung des Informationsfreiheitsrechts. Diesem Beispiel muss in anderen Subventionsbereichen gefolgt werden, um auch den bisher undurchsichtigen Teil der Leistungsverwaltung transparenter, also die Subventionsgewährung und die ihr zugrunde liegenden politischen Entscheidungen nachvollziehbarer zu machen. Eine Fortsetzung der positiven Gesamtentwicklung der Informationsfreiheit ist wünschenswert.

2 Technik

2.1 Internet der Dinge – Erfassung, Speicherung und Übermittlung von Daten durch Geräte des Alltags

Die elektronische Haustür mit biometrischem Zugangssystem, die über Handy und Internet regelbare Heizungssteuerung, mit Speicherchips ausgestattete Waren, Kühlschränke und Alarmanlagen mit Netzanschluss, mit Elektronik gespickte Autos, Handys mit Kamera und Navigation, überall haben vernetzbare, "intelligente" Geräte Einzug in unseren Alltag gehalten. Das Problem ist nur, sie wissen viel über unsere Gewohnheiten, wir wissen meistens wenig über ihre Speicher- und Kommunikationsmöglichkeiten.

Im Tagesablauf nutzen wir an den unterschiedlichsten Stellen technische Hilfsmittel, die durch unsere Einstellungen persönliche Profile besitzen. Sie kennen beispielsweise unsere Namen, Passwörter, Vorlieben und versuchen, uns zu beraten und zu unterstützen. Doch wissen wir immer, wie diese Geräte arbeiten? Was wird an Daten erfasst, gespeichert und weitergegeben?

Ein Beispiel hierfür ist die Energieversorgung. Sie soll zukünftig über intelligente Zähler und Messeinrichtungen transparenter werden. Kundinnen und Kunden wird es damit möglich werden, ihre Verbrauchswerte und das Verbrauchsverhalten regelmäßig und schnell abzurufen und zu bewerten. Grundlage dieser Umstellung ist die EG-Richtlinie 2002/91/EG. Hier ist festgelegt, dass ab dem 1. Januar 2010 in Gebäuden Messeinrichtungen bereitgestellt werden müssen, die in monatlichen Intervallen den Energieverbrauch und die Nutzungszeit an Energielieferanten, Netzbetreiber und Messstellenausstatter übermitteln und damit erweiterte Ablesemöglichkeiten und Auswertungen bieten. Die Übermittlung weiterer Leistungsmerkmale ist abhängig von den Angeboten der jeweiligen Unternehmen und mit Einwilligung der Verbraucherinnen und Verbraucher möglich. Zukünftig sollen die Verträge zwischen den Beteiligten auch Aussagen zur Verarbeitung und Übermittlung der Verbrauchsdaten enthalten. Kontroll- und Vorgabeinstanz ist die Bundesnetzagentur.

Ein weiteres Beispiel sind die elektronischen Regelkreise zur Autosteuerung die immer weiter ausgebaut werden. Sie speichern Werte

über den Fahrzeugzustand, interne Fehler, gefahrene Kilometer, Geschwindigkeiten, Bremsaktivitäten, Querbeschleunigung oder ABS-Aktivitäten. Die gespeicherten statischen und dynamischen Messdaten erfüllen in erster Linie Hilfsfunktionen zur aktiven Unterstützung der Verkehrsteilnehmerinnen und -teilnehmer. Sie können aber auch zur Unfalldatenauswertung herangezogen, im Rahmen von Wartungen ausgelesen oder zur Profilanalyse verwendet werden. Teile der über vorhandene GPS-Systeme gewonnenen dynamischen Bewegungsdaten könnten auch von den Verkehrsleitstellen bei der Verkehrslenkung genutzt werden.

Mit den Herausforderungen dieses "Internet der Dinge", also der Verknüpfung von Sensoren und Steuergeräten über Funkschnittstellen und das Internet beschäftigt sich auch die EU-Kommission. Eine wesentliche Rolle hierbei spielt die RFID-Technologie. Mit derartigen Systemen kann es durch die Ansammlung unterschiedlichster Daten zu umfangreichen Profilbildungen ohne Wissen und Wollen der Betroffenen kommen. Transparenz und Widerspruchsmöglichkeiten für die Nutzenden sind deshalb zwingende Voraussetzungen. Weiter sind insbesondere datenschutzfreundliche Technologien zu bevorzugen, die auf Datenvermeidung, rechtzeitige Aggregierung sowie frühzeitige Anonymisierung und Pseudonymisierung setzen.

➡ Im "Internet der Dinge" können zahlreiche persönliche Daten zu aussagefähigen Profilen zusammengeführt werden. Um dies zu vermeiden, müssen datenschutzfreundliche Technologien zum Einsatz kommen.

2.2 Datenschutzförderndes Identitätsmanagement

Datenschutzförderndes Identitätsmanagement muss in erster Linie die Möglichkeit bieten, digitale Medien anonym oder pseudonym nutzen zu können. Der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren ist bereits seit langem vorhanden. Eine Umsetzung in geeignete Produkte, die eine breite Nutzung ermöglichen, steht allerdings noch aus.

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Ge-

währleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Nutzung digitaler Medien, insbesondere des Internet, führt derzeit zu einer mehr oder minder großen Preisgabe von Informationen zur Persönlichkeit. Möchte ich etwas kaufen, am Online-Banking teilnehmen, in Foren diskutieren oder Web 2.0-Communities beitreten, so ist jeweils die Angabe persönlicher Daten erforderlich. Dadurch, dass diese Daten auf den Plattformen der Anbietenden gespeichert werden, sind sie im Weiteren durch die Nutzenden nur begrenzt kontrollierbar. Datenschutzfördernde Identitätsmanagementsysteme sollen hier gegensteuern. Sie sollten so aufgebaut sein, dass eine anonyme oder pseudonyme Nutzung möglich ist. Ist die Angabe von Identitätsdaten erforderlich, sollte das informationelle Selbstbestimmungsrecht nicht aus der Hand gegeben werden müssen und es sollten eigenverantwortliche Schutzmöglichkeiten gegen die Bildung von Persönlichkeitsprofilen angeboten werden. In Abhängigkeit von den eingenommenen oder gewünschten Rollen sollten nur diejenigen Informationen preisgegeben werden, die zur Nutzung erforderlich sind.

In der Offline-Welt wird dieser Umgang mit persönlichen Daten intuitiv genutzt. Werden im Freundeskreis eher persönliche Dinge preisgegeben, geschieht dies im Berufs- und Geschäftsleben schon zurückhaltender und es werden nur die Angaben zu Namen, Funktionen und Umfeld gemacht, die erforderlich sind, um Tätigkeiten oder Geschäfte ausüben oder Kontakte knüpfen zu können. Diese Möglichkeiten müssen auch in der digitalen Welt vorhanden sein. Ist beispielsweise die Volljährigkeit nachzuweisen, so sollte hierzu die Angabe weiterer Personalien nicht erforderlich sein. Möglich wäre dies über die Verwendung so genannter Credentials – elektronischer Beglaubigungen –, die etwa die Volljährigkeit nachweisen, ohne weitere persönliche Daten preiszugeben.

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundesein-

heitlichen Steueridentifikationsnummer (Steuer-ID) oder der mit der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit faktisch solche Merkmale eingeführt. Auch mit dem neuen ePersonalausweis können die Bürgerinnen und Bürgern eine auf den Chip des Ausweises aufgebrachte elektronische Identität nutzen, mit der eine Identifikation gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten möglich wird. Zwar gilt in den jeweiligen Gesetzen das Grundprinzip, dass eine Verknüpfung von Daten aus mehreren Bereichen nicht erlaubt ist. So ist beispielsweise im Personalausweisgesetz geregelt, dass die Seriennummer des Ausweises nicht zum Abruf personenbezogener Daten oder zur Verknüpfung verwendet werden darf. Angesichts der stetig verbesserten technischen Möglichkeiten, Daten anwendungsübergreifend zu verknüpfen, werden allerdings die Begehrlichkeiten wachsen.

Ein datenschutzförderndes Identitätsmanagement kann die einzelne Person vor unangemessener Überwachung und Verknüpfung ihrer Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Es schließt Verknüpfungen nicht aus, wenn sie gewünscht oder gesetzlich vorgesehen sind. Es verhindert jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (zum Beispiel: Besteuerung) einer Person zugeordnet werden kann.

Datenschutzförderndes Identitätsmanagement ermöglicht im Idealfall eine einfache und leicht verständliche Nutzungskontrolle der Bedingungen, unter denen Aktionen wie Kommunikationsvorgänge, Handlungen oder Personen miteinander verknüpft werden können. Der operative Kernpunkt ist dabei die technische Unterstützung bei der Verwendung von Pseudonymen. Es ist absehbar, dass es noch lange dauern wird, bis kulturell dem technisch gestützten Benutzen von Pseudonymen im Alltag nichts Anrüchiges, Unaufrichtiges, Feiges mehr anhaftet, sondern der Umgang mit Pseudonymen zur alltäglichen Selbstverständlichkeit geworden ist. Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteilig-

ten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert in einer Entschließung vom 3./4. April 2008 (Abdruck im Anhang) die Entwicklung und den Einsatz entsprechender Produkte. EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) verfolgen diese Ziele und werden im Rahmen des europäischen Forschungsprogramms "Technologien für die Informationsgesellschaft" gefördert.

- Die öffentliche Verwaltung und die Wirtschaft sollten die Einführung datenschutzfördernder Identitätsmanagementsysteme vorantreiben. Entwicklungen müssen künftig die Anforderung des Identitätsmanagements von vornherein in die Betriebssysteme, Kommunikationssoftware, Bürgerportale oder Public-Key-Infrastrukturen integrieren.

2.3 Datenschutz im IT-Grundschutz

Neben der neuen Bezeichnung "IT-Grundschutzkataloge" erhielt das seit vielen Jahren bewährte IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auch einen Baustein "Datenschutz", eine Gemeinschaftsproduktion des BSI, der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzaufsichtsbehörden. Der Baustein ist so angelegt, dass Datenschutzverantwortliche aus dem öffentlichen und dem nicht öffentlichen Bereich ihn nutzen können.

Kernstück dieses seit Herbst 2007 zur Verfügung stehenden Kapitels 1.5 ist der "Datenschutzprozess", der analog zum Datensicherheitsprozess zyklisch angelegt ist, also nicht terminiert, sondern immer wieder durchlaufen werden muss. Er gehört zur übergreifenden Aufgabe des Datenschutzmanagements und ist auf der gleichen Ebene wie das Datensicherheitsmanagement angesiedelt. Folgerichtig sollte sein Ergebnis ein Datenschutzkonzept sein. Es muss die einschlägigen Gesetze und Vorschriften des Datenschutzes, die Rechte der Betroffenen, die möglichen Gefährdungen und die entsprechenden Schutz-

maßnahmen enthalten. Zur besseren Übersicht ist es genau wie beim Datensicherheitskonzept möglich, Gefährdungen und Maßnahmen tabellarisch gegenüberzustellen und schnell einen Überblick über das Datenschutzniveau eines IT-Verfahrens zu erhalten.

Obwohl der Baustein "Datenschutz" nun integrativer Bestandteil der IT-Grundschutzkataloge ist, bleiben die unterschiedlichen Blickwinkel auf Datenschutz und Datensicherheit bestehen. Im Datenschutzkonzept wird festgeschrieben, welche Daten verarbeitet werden dürfen und welche Anforderung an deren Verarbeitungen direkt aus gesetzlichen Grundlagen abgeleitet werden müssen. Der Inhalt des Bausteins "Datenschutz" wird also direkt vom Status und Standort der für die Verarbeitung verantwortlichen Stelle abgeleitet. In Abhängigkeit hiervon sind beispielsweise das Sozialgesetzbuch, das Bundesdatenschutzgesetz oder die Landesdatenschutzgesetze anzuwenden. Das Datensicherheitskonzept hingegen beschreibt, wie die Daten verarbeitet werden und welche Schutzmaßnahmen getroffen wurden.

- Ein in der Entwurfsphase parallel mit dem Sicherheitsmanagement aufgesetztes Datenschutzmanagement gewährleistet, dass Aspekte des Datenschutzes wie die Gewährleistung der Rechte Betroffener oder auch die Zweckbindung in einem bestimmten Kontext erhobener Daten bereits in frühen Entwicklungsphasen von IT-Verfahren berücksichtigt werden können und Datenschutzverstöße vermieden werden.

2.4 Sicherheitskonzepte, notwendige Grundlage für einen sicheren Betrieb

Öffentliche Stellen betreiben eine Vielzahl von Verfahren, in denen personenbezogene Daten verarbeitet werden. Um diese Verfahren ordnungsgemäß ablaufen zu lassen, sind nach dem Datenschutzgesetz NRW Sicherheitskonzepte zu erstellen und Vorabkontrollen durchzuführen. In nicht wenigen Fällen mangelt es an der Qualität des Inhalts und an der Vollständigkeit.

Bei Kontroll- und Informationsbesuchen wurden immer wieder Mängel in der Dokumentation der den nach den Datenschutzgesetzen zu treffenden technischen und organisatorischen Maßnahmen sichtbar. Teil-

weise war es nicht möglich, Kontrollen durchzuführen, da die Unterlagen gar nicht oder nur mit erheblichen Lücken vorhanden waren. In zwei Fällen mussten Beanstandungen erfolgen, weil trotz mehrfacher Aufforderungen das Sicherheitskonzept, die Vorabkontrollen und das Verfahrensverzeichnis nicht geliefert wurden.

Ein ordnungsgemäßer, sicherer Betrieb von Verfahren ist nur dann möglich, wenn transparent ist, auf welchen Systemen welche Verfahren ablaufen, welche Daten wo und wie lange gespeichert werden, wer Zugriff über welche Übertragungswege auf diese Daten hat und welche Sicherheitsmaßnahmen zum Schutz der Daten getroffen wurden. § 10 des Datenschutzgesetzes NRW stellt hier den Rahmen über die zu treffenden technischen und organisatorischen Maßnahmen. Lücken in der IT-Sicherheit können nur erkannt werden, wenn aussagefähige Dokumentationen erstellt wurden. Beispiele, wie der über die Presse bekannt gewordene unbefugte Zugriff auf Einwohnerdaten zeigen, dass Missbrauchsszenarien durchaus realistisch sind und ein Schutz nur möglich ist, wenn eine umfassende Sicherheitsanalyse durchgeführt wurde.

➡ Die seit 2000 bestehende gesetzliche Verpflichtung zur Erstellung von Sicherheitskonzepten und Verfahrensverzeichnissen sowie zur Durchführung von Vorabkontrollen wird bisher nur unzureichend umgesetzt. Es ist dringend nötig, dass öffentliche Stellen hier ihren Verpflichtungen besser nachkommen.

2.5 Auslagerung der Datenverarbeitung

Erfolgt eine Auslagerung der Datenverarbeitung, so bleiben alle Verpflichtungen aus den Datenschutzgesetzen bei der beauftragenden Stelle bestehen. Sie trägt weiterhin die Verantwortung für die Verarbeitungen.

In der Verwaltung ist die Tendenz zu beobachten, die Datenverarbeitung für Verfahren, in denen personenbezogene Daten verarbeitet werden, immer häufiger und umfangreicher auszugliedern und sie bei Eigenbetrieben oder Verbundrechenzentren durchführen zu lassen. Die Verarbeitungskapazitäten von Rechnersystemen und die Übertragungsleistungen der Netze lassen diese Entwicklung aus technischer

Sicht zu. Ausschlaggebend sind die wirtschaftlichen Vorteile: Neben den Einsparungen für eigene IT-Systeme muss auch keine eigene IT-Abteilung und damit ebenfalls nur geringe IT-Kompetenz vorgehalten werden. Aus datenschutzrechtlicher Sicht ist dieser Konzentrationsprozess kritisch zu bewerten, weil mit ihm häufig auch die Verantwortung im vorgeschriebenen Umfang nicht mehr wahrgenommen wird. Da es sich bei der Verlagerung datenschutzrechtlich im Regelfall um eine Datenverarbeitung im Auftrag handelt, ist auf die getroffenen Vertragsvereinbarungen ein besonderes Augenmerk zu richten. Entsprechend § 11 Datenschutzgesetz NRW (DSG NRW) ist jede Auftragsdatenverarbeitung schriftlich festzulegen. Damit ist insbesondere die Verpflichtung verbunden, alle in § 10 DSG NRW angeführten Sicherheitsziele und die zu treffenden technischen und organisatorischen Maßnahmen eindeutig zu regeln sowie eine Kontrolle und Transparenz sicher zu stellen.

Bei der Festlegung der technischen und organisatorischen Maßnahmen ist besonders darauf zu achten, dass im Rahmen der Konzentration von Verfahren auf wenige Rechenzentren die Eigenständigkeit von Datenbeständen auch beim Zusammenführen bei einem Auftragnehmer erhalten bleibt. So müssen beispielsweise die Daten des Einwohnerwesens einer Kommune von denen weiterer Kommunen getrennt gehalten werden. Die Auslagerung darf nicht dazu führen, dass über die vorher eigenständigen Datenbestände nunmehr insgesamt Datenabgleiche oder übergreifende Auskunftsersuchen möglich werden.

➡ Mit der Auslagerung einer Datenverarbeitung ist die Pflicht verbunden, konkrete Verarbeitungsregeln vorzugeben und diese zu kontrollieren.

2.6 Überprüfung der ePass-Verfahren

Mit der Beantragung eines elektronischen Passes werden bei den Kommunen sensible biometrische Daten erhoben und gespeichert. Kontroll- und Informationsbesuche haben ergeben, dass die Kommunen ihrer Verantwortung besser gerecht werden müssen.

Basis der Kontrollbesuche bei drei Kommunen waren die Verfahrensverzeichnisse nach § 8 Datenschutzgesetz (DSG NRW), die funktionale

Programmbeschreibung sowie das Sicherheitskonzept und die Vorabkontrolle nach § 10 Abs. 3 DSG NRW. Zu den Ergebnissen sind folgende Feststellungen zu treffen:

- In einem Fall konnten die geforderten Prüfunterlagen nicht geliefert werden und es musste eine Beanstandung ausgesprochen werden. Im zweiten Fall mussten die Unterlagen speziell für den Besuch erstellt werden.
- Funktionen, Abläufe und Technik des Übermittlungsverfahrens der Antragsdaten an die Bundesdruckerei waren teilweise unvollständig oder nicht in den Unterlagen enthalten. Insbesondere fehlten Regelungen, die Auskunft darüber geben, wer welche Funktionen bei den Kommunen im Zusammenhang mit der Übermittlung der Daten und beim Einsatz der Chipkarten für die Signatur der Passanträge übernimmt.
- Zur Überprüfung der Pässe durch die Bürgerinnen und Bürger sind in den Antragsstellen Terminals vorhanden. Über diese können die digital gespeicherten Passbilder angesehen werden. Die Fingerabdrücke können derzeit jedoch nur an wenigen Terminals dargestellt werden. Es ist aber erforderlich, dass möglichst bald alle Terminals Fingerabdrücke darstellen können und zusätzlich ein Vergleich der digital gespeicherten Fingerabdrücke mit echten Abdrücken möglich ist. Nur hierdurch können die Bürgerinnen und Bürger die Korrektheit der gespeicherten Daten prüfen.
- Die Verfahren besitzen gestufte Berechtigungskonzepte. Formale Zuweisungen der Berechtigungen an die Beschäftigten für das Passantragsverfahren werden aber nicht immer vorgenommen. Dies ist jedoch erforderlich. Hierzu sollte eine Übersicht darüber vorliegen, welche Berechtigungen für die jeweiligen Funktionsbereiche vergeben worden sind.
- Im Hinblick auf die Protokollierung im ePass-Verfahren erfolgt teilweise eine mehrjährige Speicherung der Anwendungsdaten. Hier sind Revisionssicherheit und Datensparsamkeit gegeneinander abzuwägen und kürzere Speicherzeiten anzustreben. In jedem Fall sind aber konkrete Regeln für den Umgang mit den Protokolldateien festzulegen. Insbesondere ist darauf zu ach-

ten, dass eine Löschung der biometrischen Fingerabdrücke nach der Ausgabe der Pässe zeitnah auch in allen Sicherungsbeständen erfolgt und die Daten nicht in den Protokolldateien erhalten bleiben.

➡ Beim ePass-Verfahren sind insbesondere für die sensiblen biometrischen Daten die Löschungsfristen einzuhalten und die Überprüfungsmöglichkeiten für Bürgerinnen und Bürger zu verbessern.

2.7 Heimliche E-Mail-Lesebestätigungen

Lesebestätigungen von E-Mails sollen den Absendenden signalisieren, dass ihre Nachricht zur Kenntnis genommen wurde. Erfolgt eine Rückmeldung allerdings versteckt und heimlich, also ohne Kenntnis der Nutzenden, grenzt dies an Ausspähung.

Bei den im Office-Bereich eingesetzten E-Mail-Programmen können über standardmäßig vorgegebene Funktionen Empfangs- und/oder Lesebestätigungen angefordert werden. Diese Funktion ist vielen Nutzenden vertraut. Sie ist transparent und nach eigenen Vorstellungen einstellbar oder deaktivierbar. Häufig nicht bekannt hingegen sind die Möglichkeiten, versteckt im E-Mail-Text Lesebestätigungen über aktive Inhalte einzubringen und diese so zu nutzen, dass ohne Wissen und für die Empfängerinnen und Empfänger unsichtbar beim Öffnen der E-Mails oder auch bei der Anzeige des Lesebereichs im Vorschaufenster der absendenden Person eine "Lesebestätigung" gesandt wird. Die häufigste Nutzung besteht darin, bei Newslettern oder SPAM-Mails Bestätigungen darüber zu erhalten, ob E-Mail-Adressen tatsächlich existieren und diese dann für weitere Versendungen zu verwenden. Außerdem kann über diese Bestätigungen das Nutzungsverhalten ausgespäht werden. Technisch ist in derartige E-Mails in der Regel ein Script implementiert, das bei bestehender Internetverbindung einen Link zum Server der versendenden Person aktiviert. Gewöhnlich wird dies über den Download einer kleinen, für unerfahrene Nutzende unsichtbaren Grafik ausgelöst. Über die Protokolldateien erhält die versendende Person somit die Bestätigung, wann und wie oft E-Mails von bestimmten Personen geöffnet worden sind. Da die Implementierung des Scripts im HTML-Code erfolgt, kann eine Aktivierung auch nur in dieser Darstellung erfolgen.

➧ Grundsätzlich besteht bei den im HTML-Format geschriebenen E-Mails die Gefahr, dass sie Programmcodes oder Skripte mit einer Schadfunktion enthalten. E-Mail-Programme sollten aus Gründen der Datensicherheit so eingestellt sein, dass eingehende Nachrichten nur im Textformat dargestellt werden.

2.8 Umgang mit persönlicher Post im Dienstverkehr

Sollen Postsendungen Beschäftigte einer Dienststelle oder eines Unternehmens persönlich erreichen, sind sie so zu adressieren, dass der private Charakter zweifelsfrei erkannt werden kann.

Gegenstand von Anfragen ist immer wieder die Adressierung von Postsendungen mit persönlichem Inhalt. Sind Postsendungen so adressiert, dass der Name vor dem Firmennamen oder der Dienststelle in der Anschrift genannt ist oder der Zusatz "persönlich" oder "vertraulich" im Adressfeld enthalten ist, so ist die Sendung als persönliche Post zu behandeln und daher ungeöffnet an die Empfängerin oder den Empfänger weiterzuleiten. Um dies sicher zu stellen, sollte eine entsprechende Anweisung vorhanden sein, die allen Beschäftigten insbesondere denen der Poststelle bekannt gegeben wird. Sollte die Empfängerin oder der Empfänger feststellen, dass privat zugestellte Schreiben dienstliche Mitteilungen enthalten, ist dafür Sorge zu tragen, dass diese Schreiben in den Geschäftsgang gegeben werden. Auf diese Verantwortungspflicht sollte in der Anweisung hingewiesen werden. Weiter sollte geregelt sein, dass versehentlich geöffnete Privatpost direkt in einem verschlossenen Umschlag an die Empfängerin oder den Empfänger weiterzuleiten ist. Entsprechende Regelungen müssen auch für die Zusendung von privaten E-Mails getroffen werden. Weitere Informationen zum Umgang mit privaten E-Mails finden sich auf der Homepage www.ldi.nrw.de.

➧ Zur Vermeidung von Verstößen gegen das Brief- und Fernmeldegeheimnis müssen klare Regelungen getroffen werden, wie mit persönlicher Post umzugehen ist.

3 Medien

3.1 Datenschutz beim digitalen Rundfunk und Fernsehen

Das analoge Fernsehen wird in absehbarer Zeit nicht mehr angeboten werden und durch das digitale Fernsehen abgelöst. Gleichzeitig werden neue Infrastrukturen aufgebaut, mit deren Hilfe grundsätzlich auch der Fernsehkonsum der Einzelnen beobachtet werden kann.

Aufbauend auf eine leistungsfähige Kabel-, Internet- und terrestische Infrastruktur könnte zukünftig mit der Einführung des digitalen Rundfunks und Fernsehens auch eine Registrierung des individuellen Nutzungsverhaltens möglich sein. So werden beispielsweise mit der Einführung des IP-Fernsehens auch Verbindungs- und Nutzungsdaten anfallen, mit denen problemlos das Nutzungsverhalten analysierbar ist. Gleiche Möglichkeiten könnten auch für den terrestischen und den Kabelbereich realisiert werden. Hinzu kommt, dass individuell zugeschnittene Programmpakete wie Video/TV on Demand und deren Abrechnung diesen Trend verstärken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert in einer Entschließung vom 8./9. März 2007 (Abdruck im Anhang), dass die Inanspruchnahme von Rundfunk und Fernsehen sowie deren Abrechnung weiterhin anonym möglich ist und frei empfangbare Programme nicht zu Lasten von Geschäftsmodellen verdrängt werden, die eine personenscharfe Registrierung erfordern.

➡ Die Entwicklung des digitalen Rundfunks und Fernsehens muss weiterhin kritisch daraufhin beobachtet werden, dass der seit jeher selbstverständliche anonyme Empfang von Sendungen möglich bleibt.

3.2 TK-Überwachung mit WLAN-Catcher

Ermittlungsbehörden behaupten einen Bedarf für die Überwachung breitbandiger Internetzugänge über WLAN-Technik. Hierzu setzen sie spezielle PC-Systeme ein, die eine Überwachung des Funkverkehrs ermöglichen. Die Überwachung des

Funkverkehrs bedeutet aber auch, dass unbescholtene Bürgerinnen und Bürger in ihrem Recht auf unbeobachtbare Kommunikation beeinträchtigt werden können.

Wireless-LAN-Technologie findet immer größere Verbreitung. Sie ist selbst für Laien leicht zu installieren und ermöglicht den mobilen Einsatz von Endgeräten wie Laptops oder PDA. Zur Technik und zur sicheren Nutzung dieser Zugänge wurde bereits im Bericht 2003 unter 3.4 und im Bericht 2007 unter 2.1 Stellung genommen. WLAN-Zugänge werden heute sowohl privat als auch kommerziell genutzt. Über so genannte Hotspots beispielsweise an Flughäfen, in Hotels oder Call-Shops können sich Berechtigte leicht einwählen und haben somit auch auf Reisen leistungsfähige Internetzugänge. Da auch Tatverdächtige mobil sind, sehen Ermittlungsbehörden den Bedarf, die Funkstrecken zu den Hotspots überwachen zu können. Hier liegt allerdings auch gleich das Problem. Über einen Hotspot kommunizieren in der Regel mehrere Nutzende, die sich im Allgemeinen nur kurze Zeit an bestimmten Orten aufhalten. Wird nun eine Funkstrecke zum Hotspot überwacht, sind alle eingewählten Nutzenden erkennbar und damit grundsätzlich auch überwachbar. Identifizierbar sind die eingewählten Teilnehmenden über die MAC-Adressen (eindeutige Kennung einer Netzwerkkarte) ihrer Endgeräte. Liegt eine Anordnung zur Überwachung vor, ist diese dann auf die angegebene MAC-Adresse zu fokussieren. Hinzuweisen ist aber darauf, dass die MAC-Adresse als eindeutiges Merkmal nur begrenzt tauglich ist, weil sie sich durch die Nutzenden ändern lässt. Für eine Überwachung ist es ein zusätzliches Hindernis, wenn die Funkstrecke mit einer starken Verschlüsselung gesichert ist.

- Überwachungssysteme wie der WLAN-Catcher, die unbeteiligte Dritte in ihren Rechten beeinträchtigen, sind datenschutzrechtlich bedenklich und somit abzulehnen.

3.3 Bewertungsportale – Recht auf freie Meinung oder Pranger?

Bewertungsportale ermöglichen es, nach einer Registrierung andere Personen wie Lehrkräfte, Ärztinnen oder Ärzte sowie Personen, die ein Handwerk ausüben, zu bewerten – und zwar

nicht immer sachlich. Der Umgang mit diesen Internetportalen wird deshalb mit vielen Emotionen diskutiert.

Der Fall spickmich.de hat bundesweit die Gemüter erhitzt. Das Portal, von Studierenden in Nordrhein-Westfalen gegründet, ermöglicht es, dass Schülerinnen und Schüler ihren Lehrkräften Noten geben. Hierbei können alle, die sich bei diesem Dienst für eine bestimmte Schule angemeldet haben, die Lehrkräfte an dieser Schule bewerten und "deren Zensuren" einsehen. Noten gibt es zu den unterschiedlichsten Kriterien. Ab zehn Bewertungen wird das Ergebnis veröffentlicht. Die Anmeldung zu dem Dienst ist ohne großen Aufwand und überprüfbare Identifikation möglich. Aus der Sicht des Datenschutzes stellt sich hierbei nicht die Frage, ob Schülerinnen und Schüler ihre Lehrkräfte öffentlich benoten dürfen, sondern ob die Veröffentlichung von personenbezogenen Daten der Betroffenen im Internet zulässig ist. Das Landgericht Köln und das Oberlandesgericht Köln kamen zu dem Ergebnis, dass die Benotung von Lehrkräften im Internet vom Grundrecht der Meinungsfreiheit aus Art. 5 Grundgesetz (GG) gedeckt und somit rechtens sei.

Die Datenschutzaufsichtsbehörden haben dazu eine ganz andere Meinung. Die Meinungsfreiheit kann durch allgemeine Gesetze eingeschränkt werden und dazu gehört auch das Datenschutzrecht, welches selbst ja Ausfluss des Grundrechtes auf informationelle Selbstbestimmung ist. Ob die anonyme Notenvergabe an Lehrerinnen und Lehrer und die Veröffentlichung der Durchschnittsnote als mathematisches Ergebnis von mindestens zehn Bewertungen in den Schutzbereich der Meinungsfreiheit nach Art. 5 GG fällt, ist zweifelhaft, zumal die Noten auch beispielsweise von Kolleginnen, Partnerinnen, Nachbarinnen sowie auch den Betroffenen selbst vergeben werden können, denn eine Registrierung unter einem frei erfundenen Namen ist wegen der unzureichenden Identifikation jederzeit möglich.

Aber auch wenn in der Benotung die Ausübung des Grundrechts auf Meinungsfreiheit gesehen würde, wäre in diesem Fall dem Recht auf informationelle Selbstbestimmung der Betroffenen der Vorrang einzuräumen (siehe auch Entschließung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 17./18. April 2008, abgedruckt im Anhang). Es handelt sich hier um eine Veröffentlichung von sensiblen personenbezogenen Daten, die nicht etwa auf den Kreis einer Schülerzeitung beschränkt bleibt,

sondern weltweit abrufbar ist. Dadurch wird zum einen ein viel größerer Personenkreis erreicht und zum anderen ein ganz anderer Informationscharakter der Bewertung suggeriert, nämlich weg von der reinen subjektiven Bewertung hin zu einem objektiven Ergebnis. Aus Sicht des Datenschutzes überwiegt deshalb das schutzwürdige Interesse der Betroffenen auf informationelle Selbstbestimmung.

➡ Der Rechtsstreit um das Bewertungsportal ist jetzt in der 3. Instanz. Es bleibt zu hoffen, dass der Bundesgerichthof zu einer datenschutzgerechten Beurteilung des Bewertungsportals kommt.

3.4 Soziale Netzwerke – die schöne Welt der virtuellen Gemeinschaften

Unzählige so genannte "social communities" haben das bisher anonyme Internet verändert. Menschen sind soziale Wesen und wollen sich austauschen. In Internetangeboten wie Xing oder StudiVZ können sich Gleichgesinnte treffen. Dank der Profile, die Mitglieder dieser sozialen Netzwerke über sich selbst im Netz veröffentlichen, wissen auch scheinbar alle, mit wem sie es zu tun haben – aber alle anderen wissen es auch.

Die Vorläufer der sozialen Netzwerke sind die Foren und Chaträume im Internet. Dort können alle ihre Meinung kundtun und sich über bestimmte Leitthemen austauschen. Zur Registrierung reicht meist ein Pseudonym (nickname), weitere persönliche Angaben sind nicht erforderlich, so dass die Personen hinter den Pseudonymen meistens verborgen bleiben. In den sozialen Netzwerken ist es nunmehr üblich, das eigene, gesamte Profil zu gestalten – angefangen vom eigenen Foto bis hin zu der Veröffentlichung intimer Details. Hierdurch werden hochsensible persönliche Daten weltweit veröffentlicht und das alles mit persönlicher Einwilligung, denn die Teilnahme und die Profilbildung sind ja freiwillig. Im Zeitalter von Castingshows und Dschungel-Camps wird einer ganzen Generation suggeriert, alle könnten Superstars sein. Wichtig ist nur die richtige, einfallsreiche Präsentation der eigenen Person.

Bei allen Veröffentlichungen sollte jedoch bedacht werden, dass sich nicht nur gutwillige andere Mitglieder der Community für die Profile

interessieren, sondern auch beispielsweise die Werbeindustrie, potentielle Arbeitgeberinnen und Arbeitgeber oder Straftäterinnen und Straftäter. So geben die meisten Personalleitungen zu, sich über Bewerberinnen und Bewerber erst einmal ein Bild im Internet zu machen. Mittlerweile gibt es Suchmaschinen, die sich auf die Personensuche spezialisiert haben und die auch soziale Netzwerke durchforsten können. Peinlich, wenn vor der Personalleitung dann die letzten Fotos feucht-fröhlicher Partys erscheinen oder radikale politische Artikel aus vergangenen Jahren. Es kommt hinzu, dass alles, was einmal ins Netz gestellt wurde, nicht mehr wirklich daraus entfernt werden kann. Fotos und alle anderen Einträge können jederzeit kopiert, archiviert oder in ganz anderem Zusammenhang genutzt werden. Es bleibt festzustellen, dass ins Internet gestellte personenbezogene Daten faktisch Allgemeingut werden.

Nach dem Telemediengesetz sind die Anbietenden der sozialen Netzwerke verpflichtet, eine anonyme oder pseudonyme Nutzung des Dienstes anzubieten. Bei der Nutzung der Dienste sollte diese Art der Teilnahme ins Auge gefasst werden. Da bei diesen Diensten Einnahmen im Prinzip nur über die Werbung erzielt werden können, werden Personenprofile gerne zu Werbezwecken genutzt, denn die Daten über besondere Vorlieben sind bares Geld wert. Daten dürfen jedoch selbst nach dem bisher geltenden Recht nur für Werbezwecke genutzt werden, wenn den Nutzenden auch eine Widerspruchsmöglichkeit eingeräumt wurde.

Bei der Registrierung in einem sozialen Netzwerk sollten Nutzende sich darüber informieren, welche Einstellungen für die Profildaten möglich sind. Ziel sollte es sein, die eigene Privatsphäre möglichst umfassend zu schützen. Dies kann beispielsweise dadurch geschehen, dass die Profildaten nicht von vornherein für alle freigegeben werden, sondern jeweils erst durch eindeutige Erklärungen nur an diejenigen Personen, die die Nutzenden vorher selber bestimmt haben. Dazu gehört auch, dass die Profildaten wieder auf einfache Weise gelöscht werden können (siehe auch Entschließung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 17./18. April 2008, Abdruck im Anhang).

- Es ist noch viel Aufklärungsarbeit zu leisten, um die Nutzerinnen und Nutzer sozialer Netzwerke dafür zu sensibilisieren, mit ihren persönlichen Daten vorsichtig

und sparsam umzugehen. Es sind aber auch die Betreibenden der Portale in die Pflicht zu nehmen, ihre Mitglieder über die Verarbeitung der personenbezogenen Daten und die Wahl der Gestaltungsmöglichkeiten zum Schutz der Privatsphäre umfassend zu informieren.

3.5 SPAM Filter – Notwendigkeit oder Zensur?

Der Anteil unerwünschter oder unverlangt zugesandter Nachrichten besitzt in vielen Fällen einen so hohen Anteil am E-Mail Aufkommen, dass die Verfügbarkeit des Gesamtsystems bedroht ist. Aus Sicht von Firmen und Behörden sind deshalb Maßnahmen zur Abwehr erforderlich, die eine geeignete Filterung vornehmen. Rechtlich sind der Filterung allerdings Grenzen gesetzt.

Firmen und Behörden wickeln heute einen großen Teil ihrer Korrespondenz über E-Mail ab. Um die Funktionsfähigkeit des E-Mail-Zugangs zu erhalten sind geeignete Mechanismen zur Abwehr von SPAM einzusetzen. In der Anti-SPAM-Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind eine Reihe von Verfahren beschrieben, die unterschiedlich stark in die Persönlichkeitsrechte der Beschäftigten eingreifen. Unter den in Betracht kommenden Verfahren sollte das datenschutzfreundlichste gewählt werden. Hierbei sollte der Grundsatz gelten, dass eine Markierung der unerwünschten Meldungen einer Löschung vorzuziehen ist. Eine Unterdrückung von Nachrichten oder Anhängen darf nur erfolgen, wenn die Mail ein Format aufweist, das eine Gefährdung der Datensicherheit erwarten lässt. Insgesamt sollte die SPAM-Filterung so konzeptioniert sein, dass die Empfängerinnen und Empfänger von E-Mails in größtmöglicher Autonomie über den Umgang der an sie gerichteten Nachrichten selbst entscheiden können. Die Art des Verfahrens sollte für die Beschäftigten transparent sein.

Darf der dienstliche E-Mail-Anschluss auch privat genutzt werden, so ist beim E-Mail-Verkehr insgesamt das Fernmeldegeheimnis zu wahren. Dies bedeutet insbesondere, dass eine inhaltliche Filterung der eingehenden Mails über Contentfilter ohne Zustimmung der Nutzenden nicht erfolgen darf.

➡ Bei der Konzeptionierung von SPAM-Filtern ist darauf zu achten, dass die Rechte der Empfängerinnen und Empfänger von E-Mails im Hinblick auf das Fernmeldegeheimnis nicht beschnitten werden.

3.6 Speicherung von IP-Adressen bei Anbietenden von Websites

Bei IP-Adressen handelt es sich um personenbezogene Nutzungsdaten, deren Speicherung nach dem Telemediengesetz (TMG) nur dann zulässig ist, wenn die Erhebung und Verwendung der Daten zur Inanspruchnahme und Abrechnung von Telemediendiensten erforderlich ist.

In den Hinweisen zum Datenschutz wird bei Internetangeboten häufig angegeben, dass die Kommunikationsdaten mit den vollständigen IP-Adressen der Besucherinnen und Besucher eine Zeit lang (mehrere Wochen) gespeichert werden, bevor diese Daten für statistische Zwecke anonymisiert und weiter verarbeitet werden. Diese Praxis ist nach dem TMG nicht zulässig. Hinzuweisen ist in diesem Zusammenhang auf eine Entscheidung des Landgerichts Berlin vom 6. September 2007 (23 S 3/07), das einem Bundesministerium untersagt, über seine Website personenbezogene Daten wie die IP-Adressen über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern.

Abzugrenzen ist die Protokollierung von Kommunikationsdaten bei der Nutzung von Webangeboten von der Protokollierung im Rahmen von Intrusion-Detection-Systemen zu Zwecken der Datensicherheit. Das TMG enthält hierzu keine Regelungen. Protokollierungen zum Schutz interner Systeme und Netze sind auf der Grundlage von § 10 Datenschutzgesetz NRW oder § 9 Bundesdatenschutzgesetz zulässig. Insbesondere wenn das Internet-Angebot nicht ausschließlich der allgemeinen Information, sondern auch der Kommunikation oder der Abwicklung von Transaktionen zwischen Firmen und öffentlichen Stellen dient, sollen beispielsweise Firewallsysteme vor allem den unbefugten Zugriff auf die eigenen Systeme verhindern und damit Vertraulichkeit, Verfügbarkeit und Integrität der gespeicherten Daten sichern. Zu achten ist aber darauf, dass die Daten nur zu Zwecken der Datensicherheit genutzt werden dürfen.

Um eine Anonymisierung der IP-Adresse vorzunehmen, muss sie bereits entsprechend modifiziert auf den Webservern abgelegt werden. Der Sächsische Datenschutzbeauftragte hat Module zur IP-Anonymisierung auf Web-Servern realisieren lassen und stellt diese auf seiner Homepage unter http://www.saechsdsb.de/ipmask zur Verfügung.

➡ Beim Betrieb eines Webangebotes ist darauf zu achten, dass eine Speicherung der ungekürzten IP-Adressen in den Protokolldateien der Webserver über die Zeit der Erbringung der Dienstleistung hinaus nicht erfolgt und eine Anonymisierung der IP-Adressen bereits unmittelbar nach Beendigung der Kommunikation vorgenommen wird.

3.7 Internet – die einfache Möglichkeit der Analyse des Surfverhaltens

Das Telemediengesetz erlaubt keine personenbezogene Auswertung des Nutzungsverhaltens der Besucherinnen und Besucher von Webangeboten. Sollen Nutzungsprofile zur Marktforschung oder zur bedarfsgerechten Gestaltung von Webangeboten genutzt werden, darf dies nur unter Verwendung von Pseudonymen und nach vorheriger Unterrichtung der Betroffenen unter Hinweis auf eine Widerspruchsmöglichkeit erfolgen.

Prominentestes Beispiel für Analysetools ist Google Analytics, ein kostenloses Produkt zur Ermittlung des Nutzungsverhaltens der Besucherinnen und Besucher von Webangeboten. Es wird von zahlreichen Webdienstleistern genutzt, da es leicht umsetzbar ist und vielfältige Analysemöglichkeiten bietet. Technisch beruht es darauf, dass über Cookies und Skripte personenscharfe Informationen einschließlich der vollständigen IP-Adresse der Nutzenden erfasst werden und über die aufgerufenen Websites an Google weitergeleitet und hier gespeichert werden. Auf den Google-Plattformen können dann Analysetools aufgerufen und die gewünschten Auswertungen durchgeführt werden. Ein derartiger Einsatz von Analysetools durch die Webseitenbetreiber ist nach dem Telemediengesetz nicht erlaubt. Er wäre nur bei ausdrücklicher Einwilligung der Nutzenden zulässig. Diese liegt in der Regel aber nicht vor. Vielmehr weisen Betreibende von Websites im Allgemeinen nicht einmal auf den Einsatz dieser Tools hin. Hinzu kommt, dass alle

Datenübermittlungen an Google in die USA erfolgen und es sich somit um Verarbeitungen außerhalb der Reichweite der europäischen Gesetze handelt. Weiter erhält Google Kenntnis über alle Nutzungsdaten von Websites, die Analytics einsetzen. Die Datenschutzaufsichtsbehörden sind im Gespräch mit Google Deutschland, dass die IP-Adressen der Nutzenden möglichst kurzfristig anonymisiert werden.

➡ Verantwortliche für Websites müssen sich bewusst sein, dass personenbezogene Auswertungen des Nutzungsverhaltens der Besucherinnen und Besucher nicht zulässig sind. Damit werden Datenschutzrechte verletzt.

3.8 Internet – die billige Art der Abzocke

Die Anzahl der Internetabzocker steigt stetig. Dabei werden Surferinnen und Surfer mit angeblich reizvollen Angeboten auf Internetseiten gelockt, welche sich später als kostenpflichtige Dienste herausstellen. Auch wenn dies in erster Linie ein Problem des Verbraucher- und Vertragsrechts ist, wenden sich viele Betroffene auch an die LDI NRW.

Die Masche der Internetabzocker ist in nahezu allen Fällen gleich. Mit Angeboten, die kostenlose Dinge versprechen, den Alltag erleichtern oder gar einen finanziellen Vorteil verschaffen sollen, werden die Betroffenen geködert. Webadressen mit Schlagwörtern wie Nachbarschaft, Hausaufgaben, Fabrikverkauf, Rezepte oder Geburtstag beschreiben dabei kurz und knapp, was zu erwarten ist. Nach dem Öffnen der Startseite ist mit der Angabe des Namens und der Adresse sowie der Bestätigung, dass die AGB gelesen wurden, der versprochene Dienst sofort verfügbar. Profitiert wird dabei von der Ungeduld und Unerfahrenheit der Betroffenen, auf die spekuliert wird. Zugegeben – wer liest schon das lästige Anhängsel und scrollt tatsächlich durch den gesamten Text der Geschäftsbedingungen? Mit einem "Klick" liegt einem die Welt zu Füßen. Genau hier aber beginnt das Problem. Plötzlich liegen Mahnschreiben von Inkasso- oder Rechtsanwaltsbüros im Briefkasten. Es wird behauptet, dass durch die Eingabe der persönlichen Daten ein Vertrag zustande gekommen sei, der zur Zahlung eines meist einmaligen Preises oder – noch schlimmer – zu einem Abonnement verpflichte. Die Abzocker spekulieren hier auf die

Angst der Betroffenen. Statistiken zeigen auch, dass fast jede vierte Person die Rechnung bezahlt.

Nach Auffassung der Verbraucherzentrale NRW ist jedoch kein wirksamer Vertrag zustande gekommen. Es fehlt an der Preisklarheit. Die angeblichen Verträge können wegen arglistiger Täuschung angefochten und wegen der unzureichenden Hinweise auch unbefristet widerrufen werden. Mahnschreiben können unbeachtet bleiben. Erst wenn per Postzustellung ein gerichtlicher Mahnbescheid zugestellt werden sollte, muss reagiert werden. Solchen offiziellen Bescheiden ist jedoch immer auch ein Formular beigefügt, mittels dessen der Forderung widersprochen werden kann. Die Erfahrung zeigt jedoch, dass es soweit in der Regel nicht kommt, da die Abzocker sich bewusst sind, einen Zahlungsanspruch nicht durchsetzen zu können.

In den oben beschriebenen Fällen können die Datenschutzbehörden nur behilflich sein, um einen Anspruch auf Löschung der persönlichen Daten oder eine Auskunft über die Herkunft der Daten zu erreichen. Schon dies ist meistens nur schwer möglich, da sich die zudem wechselnden Firmensitze häufig im Ausland befinden und auch an deutsche Adressen wegen falscher Angaben oftmals keine Post zugestellt werden kann.

- Webangebote sind nicht immer umsonst und sind deshalb vollständig, aufmerksam und in Ruhe durchzusehen. Oftmals sind Kostenhinweise an versteckter Stelle untergebracht. AGB und Datenschutzbestimmungen sind deshalb sorgfältig zu prüfen, da sie Kostenhinweise oder Berechtigungen zur Datenweitergabe enthalten können. Mit der Bekanntgabe persönlicher Daten sollte zurückhaltend und sparsam umgegangen werden.

3.9 Internet – leichte Datenerhebung über Kontaktformulare

Webangebote enthalten in der Regel Kontaktmöglichkeiten über bereitgestellte Formulare. Häufig werden hierüber mehr personenbezogene Daten erhoben als für den eigentlichen Zweck erforderlich sind.

Webangebote sind heute ein Muss für Behörden und Unternehmen. Jeder hat sie, jeder macht sie, aber auch jeder erwartet sie. Neben den eigentlichen Inhalten wird zur Kontaktaufnahme immer öfter ein Webformular bereit gehalten. Dort können über so genannte Freifelder Kommentare abgegeben und/oder Fragen gestellt werden. Gleichzeitig wird eine schnelle Beantwortung der Anliegen versprochen. Soweit handelt es sich um eine gute Idee. Häufig sind dabei jedoch neben der Mail-Adresse eine Reihe anderer Pflichtfelder vorhanden wie Name, Anschrift, Telefonnummern oder auch das Geburtsdatum, die für eine Beantwortung der Anliegen nicht unbedingt erforderlich sind. Dies bedeutet, dass eine Absendung nicht möglich ist, auch wenn nur eine dieser Angaben fehlt. Eine derartige Datenerhebung steht im krassen Widerspruch zu den Grundsätzen des Datenschutzes, also zu Datensparsamkeit, Datenvermeidung, anonymer und pseudonymer Nutzung und auch zur Erforderlichkeit einer Datenerhebung. Grundsätzlich sollten nur diejenigen Angaben gemacht werden, die für eine Kontaktaufnahme ausreichend sind. Die Wahl sollte dabei – soweit möglich – den Anfragenden überlassen bleiben. Ist beispielsweise eine Antwort mittels E-Mail gewünscht, so sind Fragen nach Wohnort und Telefonnummer nicht nötig. Wenn eine Antwort mittels Telefon gewollt ist, sind Angaben zu Anschrift und Mail-Adresse nicht erforderlich. Insofern sollten zusätzliche Angaben allenfalls optional erfolgen. Weitere Probleme, die mit dem Nutzen solcher Webformulare auftreten, sind, dass diese oft nicht über eine verschlüsselte Verbindung übertragen werden und somit auf dem Transportwege im Internet wie eine offene Postkarte zu betrachten sind. Auch wird häufig nicht ausreichend über den Umgang und die Nutzung der erhobenen Daten sowie über die Speicherdauer aufgeklärt.

➡ Kontaktformulare in Webangeboten sind so zu gestalten, dass die Grundprinzipien des Datenschutzes, also Erforderlichkeit, Datensparsamkeit, Datenvermeidung, anonyme und pseudonyme Nutzung eingehalten werden.

3.10 Internet – Gewinnspiele und Adresshandel

Undurchsichtige Teilnahmebedingungen und lückenhafte Datenschutzerklärungen dienen Unternehmen, die Gewinnspiele

oder Gewinnspieleintragdienste im Internet anbieten, häufig als Grundlage für den Adresshandel.

"Sie sind der 999.999 Besucher dieser Internetseite und haben gewonnen." Diesen und andere Hinweise auf angeblich bereits sichere Gewinne kennen nahezu alle, die sich im Internet bewegen. Derartige Aufmacher befinden sich direkt in einschlägigen Webangeboten oder werden mittels "Pop-Up" in andere Angebote eingeblendet. Doch bei allen diesen Versprechungen ist Vorsicht geboten. Grundsätzlich gilt, nichts ist umsonst – auch nicht im Internet. In der Regel wird mit der Bekanntgabe des Namens, der Anschrift und der Mail-Adresse bezahlt. Die Geschäftsbedingungen oder Datenschutzerklärungen weisen darauf hin, dass die Teilnehmenden sich mit der Speicherung der Daten für Werbezwecke und der Weitergabe ihrer Daten an Dritte oder Partnerunternehmen einverstanden erklären.

Rechtmäßig ist der Handel oder die Datenübermittlung an Dritte aufgrund der Hinweise in den AGB oder Datenschutzerklärungen nicht. Unabdingbare Voraussetzung für eine Datenübermittlungsbefugnis an Dritte – hierunter sind auch Partner- und Tochterunternehmen zu verstehen – ist eine ausdrückliche Einwilligung der Betroffenen. Diese Einwilligung kann nach § 13 Abs. 2 Telemediengesetz auch elektronisch abgegeben werden. Sie muss allerdings genau aufführen, an welche Unternehmen im Einzelnen die Daten weitergegeben werden. Eine allgemeine Formulierung "Dritte und Partnerunternehmen" ist unzureichend, weil die Teilnehmenden völlig im Unklaren darüber gelassen werden, an wen die Daten übermittelt werden. Gewinnspielveranstalter versuchen allerdings, durch diese Art der Formulierung eine Art Freibrief für ihr Handeln zu erwirken.

Für eine unkontrollierbare Datenweitergabe ungleich gefährlicher sind so genannte Gewinnspieleintragsdienste. Den Interessierten wird dabei zugesagt, an einer bestimmten Anzahl von Gewinnspielen teilzunehmen, wenn sie ihre Daten bei dem Diensteanbieter angeben. Dieser übernimmt dann in ihrem Auftrag die Eintragungen bei den jeweiligen Gewinnspielen. Selbstverständlich wird versprochen, bei jedem Gewinnspiel auch auf die Teilnahmebedingungen und Datenschutzerklärungen zu achten, damit es nicht zu ungewollten Datenweitergaben kommt. Doch wie die stetig steigende Anzahl der diesbezüglichen Beschwerden zeigt, scheinen diese Aussagen meistens nicht zuzutreffen.

➡ Vor einer Teilnahme an Gewinnspielen ist das genaue Lesen der Geschäftsbedingungen und der Datenschutzhinweise unerlässlich. Nur so kann Ärger über ungewollte Weitergabe von Adressdaten vermieden werden. Sollen Einblendungen von Gewinnspielen erst gar nicht auftauchen, sind die Browser so einzustellen, dass Pop-Up-Fenster blockiert werden.

4 Videoüberwachung

4.1 Eine unendliche Geschichte – Videoüberwachung verlängert

Die polizeiliche Videoüberwachung wird vielfach als Allheilmittel zur Kriminalitätsbekämpfung angepriesen. Tatsächlich ist die Effektivität der Videoüberwachung im Hinblick auf die Verhütung von Straftaten jedoch mehr als fraglich.

Der Einsatz von Videokameras durch staatliche Stellen stellt einen schwerwiegenden Eingriff in das grundrechtlich geschützte Recht jedes einzelnen Menschen dar, sich grundsätzlich frei und unbeobachtet auf allen öffentlichen Straßen und Plätzen bewegen zu können. Das Bundesverfassungsgericht bewertet einen solchen Eingriff mit großer Streubreite, bei dem eine Vielzahl von Personen, die den Eingriff nicht durch ihr Verhalten veranlasst haben, betroffen sind, als Grundrechtsbeeinträchtigung von erheblichem Gewicht (siehe hierzu zuletzt BVerfG vom 23. Februar 2007 - 1 BvR 2368/06 - zur Verfassungswidrigkeit der Videoüberwachung eines Kunstwerks auf einem öffentlichen Platz). Der Einsatz polizeilicher Videoüberwachung zur Verhütung von Straftaten ist daher an enge Voraussetzungen geknüpft.

Seit Jahren bestehen erhebliche Bedenken gegen die präventiv-polizeiliche Videoüberwachung. Hierzu trugen insbesondere Studien aus Großbritannien als dem "Mutterland der Videoüberwachung" bei. Knapp formuliert trägt Videoüberwachung danach weder maßgeblich dazu bei, die Straftatenzahl zu senken noch die Aufklärungsrate zu erhöhen. In Nordrhein-Westfalen machten bisher vier Polizeibehörden – die Polizeipräsidien in Düsseldorf, Mönchengladbach und Bielefeld sowie die Kreispolizeibehörde in Coesfeld – von der Möglichkeit einer polizeilichen Videoüberwachung gemäß § 15a Polizeigesetz NRW (PolG NRW) Gebrauch. Neu hinzugekommen ist zum 25. September 2008 eine polizeiliche Videoüberwachung am Elisenbrunnen in Aachen. Die LDI NRW hatte bereits im Bericht 2001 (unter 3.1.4 und 3.1.5), im Bericht 2005 (unter 8.1) und im Bericht 2007 (unter 4.1) darauf hingewiesen, dass das Vorliegen der Voraussetzungen des § 15a PolG NRW als Rechtsgrundlage für die genannten Maßnahmen nicht hinreichend belegt sei.

Am 24. April 2008 wurde im Innenausschuss des Landtags eine Sachverständigenanhörung zur Frage der Verlängerung der Geltung des § 15a PolG NRW durchgeführt. Den Sachverständigen gelang es in diesem Rahmen nicht, einen Nachweis für die Effektivität der Videoüberwachung zu erbringen. Selbst Polizeivertreter mussten einräumen, dass die Videoüberwachung zwar die Einsatzplanung erleichtere und das subjektive Sicherheitsempfinden der Bürgerinnen und Bürger steigere, ein Verhütungseffekt aber tatsächlich nicht beobachtet werden könne. Die LDI NRW äußerte in ihrer Stellungnahme (LT-Stellungnahme 14/1845) sowohl grundsätzliche Bedenken als auch konkrete Kritik. Mit Gesetz vom 10. Juni 2008 (GV.NRW.2008 S. 471 f.) wurde gleichwohl eine Verlängerung der polizeirechtlichen Bestimmung bis zum Jahr 2013 beschlossen, obwohl es unter dem Aspekt des Grundrechtsschutzes wünschenswert gewesen wäre, von einer Verlängerung abzusehen.

➡ Bürgerinnen und Bürger werden sich in Zukunft weiterhin mit polizeilichen Videoüberwachungsmaßnahmen konfrontiert sehen. Aufgabe der LDI NRW wird es sein, die Entwicklung der Standorte auch weiterhin durch Kontrollen intensiv zu begleiten.

4.2 Videoüberwachung in Schulen: Einigkeit mit dem Schulministerium

Endlich hat sich auch das Schulministerium NRW in Sachen Videoüberwachung an und in Schulen klar positioniert.

Das Problem der Videoüberwachung in und an Schulen ist seit Jahren ein Dauerthema (siehe Bericht 2005 unter 4.1 und Bericht 2007 unter 4.3). Inzwischen trägt die Orientierungshilfe der LDI NRW "Ich sehe das, was Du so tust – Videoüberwachung an und in Schulen" maßgeblich dazu bei, die Anforderungen des Datenschutzes und der Datensicherheit auf breiter Ebene bekannt zu machen und vor allem Plänen einer Installation von Kameras, mit denen während des laufenden Schulbetriebs überwacht werden kann, schon im Vorfeld entgegenzuwirken.

In Einzelfällen sind diese Anforderungen den Schulträgern und Schulleitungen indes noch immer nicht bekannt oder sie werden ignoriert.

So gab der Hinweis, in einem Berufskolleg seien bereits beim Neubau eines Gebäudetrakts vor Jahren Videokameras in der Cafeteria, dem Eingangsbereich und zwei Fluren installiert worden, die rund um die Uhr aktiviert seien, Anlass für eine Überprüfung vor Ort, der sich der Datenschutzbeauftragte des Schulministeriums NRW informationshalber anschloss. Die rechtlichen Beurteilungen wichen nicht voneinander ab: Während des laufenden Schulbetriebs ist eine Videoüberwachung sowohl durch die Schulleitung als auch durch den Schulträger in aller Regel unzulässig. Es ist keine Rechtsgrundlage ersichtlich, die den Einsatz von Videokameras zur Überwachung des ordnungsgemäßen Verhaltens der Schülerinnen und Schüler erlauben würde. Außerhalb des Schulbetriebs kann eine Videoüberwachung durch den Schulträger nur in Betracht kommen, wenn die Voraussetzungen des § 29b Datenschutzgesetz NRW erfüllt sind. Die Videokameras in dem Berufskolleg wurden unverzüglich deaktiviert und abgebaut.

➡ Das Schulministerium NRW und die LDI NRW ziehen in Sachen Videoüberwachung in Schulen an einem Strang. Diese grundsätzliche Übereinstimmung dürfte die Einhaltung und Durchsetzung der datenschutzrechtlichen Anforderungen in Zukunft noch fördern.

4.3 Schutz vor unzulässiger Beobachtung durch technische Maßnahmen im Wohnbereich

Videoüberwachung greift auch im Wohnbereich immer stärker um sich. Mit einfachen technischen Maßnahmen lässt sich die Beeinträchtigung der Privatsphäre der Mitmenschen leicht verhindern.

Zwar kann Videoüberwachung auf dem eigenen Grundstück zulässig sein (siehe Bericht 2003 unter 5). Zunehmend werden aber im privaten Wohnbereich Videokameras an den eigenen Hauswänden angebracht, ohne zu berücksichtigen, dass bereits durch die Art der Anbringung und Ausrichtung der Kameras in der Nachbarschaft der Eindruck entstehen kann, sie würde auf dem eigenem Grundstück oder vor der eigenen Wohnungstür überwacht. Gerade wenn in der Nachbarschaft ein gespanntes Verhältnis besteht, trägt die Kamerainstallation schnell zu weiteren Missverständnissen bei, zumal die

betroffenen Personen selbst nicht feststellen können, was die Kamera tatsächlich aufnimmt und was hinter der Kamera abläuft.

Besteht aus der Sicht einer unbefangenen dritten Person aufgrund der Kameraposition der Eindruck der Überwachung, muss auch dann von einem unzulässigen permanenten Überwachungsdruck ausgegangen werden, wenn die tatsächliche Bildwiedergabe auf dem Monitor keine Beeinträchtigung der im Umfeld der Kamera lebenden Personen erkennen lässt. Diese Auffassung ist von der Rechtsprechung in verschiedenen Urteilen bestätigt worden. Selbst bei gerechtfertigter Videobeobachtung auf dem eigenen Grundstück darf deshalb die Kamera nicht so ausgerichtet sein, dass Personen außerhalb des Grundstücks in den Erfassungsbereich der Kamera geraten können oder auch nur den Eindruck haben müssen, ihre Bewegungen würden durch die Kamera erfasst.

Es muss somit alle Sorgfalt darauf verwandt werden, die Kamera so anzubringen und das Kameraobjektiv so auszurichten, dass ausschließlich das gefährdete Objekt erfasst wird. Dies kann durch geringfügige technische Maßnahmen erreicht werden. Schon eine andere als die ursprünglich vorgesehene Position der Kamera kann zu dem gewünschten Ergebnis führen. Des Weiteren ist in Betracht zu ziehen, den Anbringungswinkel der Kamera so steil nach unten auszurichten, dass jeder weitere Erfassungsbereich vermieden wird. Außerdem muss die Kamera bei ihrer Anbringung so fixiert werden, dass ihre Ausrichtung nicht durch einfache Drehbewegungen verändert werden kann. Oftmals wird nämlich nach kurzer Zeit der Korrektur von Seiten der betroffenen Nachbarinnen und Nachbarn vorgetragen, dass die Ausrichtung der Kamera wieder verstellt worden sei. Schließlich kann zusätzlich durch die Anbringung von Seitenblenden rechts oder links des Kameraobjektives erreicht werden, dass eine eindeutige Abschirmung des Erfassungsbereiches erfolgt.

➡ Technische Maßnahmen müssen verhindern, dass die Videoüberwachung auf dem eigenen Grundstück zu weitergehenden Beeinträchtigungen führt.

4.4 Schutz vor unzulässiger Beobachtung durch technische Maßnahmen im Straßenverkehr

Die Beobachtung des Straßenverkehrs zur Verkehrslenkung oder die Beobachtung betrieblicher Einrichtungen zur Betriebsorganisation oder zur Wahrung der Betriebssicherheit schießt oft über das Ziel hinaus.

Die Verkehrsüberwachung sowie Verkehrslenkung in kommunalen Verkehrsleitstellen und die organisatorisch notwendige Beobachtung in Betriebsbereichen von Verkehrsunternehmen kommen häufig nicht ohne Videokameras aus. Oft wird gar nicht geprüft, ob die gewünschten Zwecke auch zu erreichen wären, ohne dass Aufnahmen gemacht werden, auf denen Personen identifizierbar oder Kraftfahrzeugkennzeichen gut lesbar abgebildet werden. Solche Aufnahmen sind jedoch grundsätzlich nicht zu rechtfertigen, da jede personenbezogene Videobeobachtung nur unter engen gesetzlichen Voraussetzungen zulässig ist. Wäre bei der Einrichtung der Videoüberwachung daran gedacht worden, entsprechende technische Maßnahmen einzusetzen, wäre ein Konflikt mit dem Datenschutz zu vermeiden gewesen.

In der Regel reichen Übersichtsbilder für die Verkehrsbeobachtung und Verkehrslenkung aus, denn es kommt nicht darauf an, die am Verkehrsgeschehen beteiligten Personen oder Fahrzeuge zu erkennen und zu identifizieren. Letzteres entspräche auch nicht der Aufgabenstellung einer Verkehrsleitstelle oder technischen Überwachung. Wie kann nun sichergestellt werden, dass tatsächlich nur Übersichtsbilder auf dem digitalen Bildschirm erscheinen? Wenn etwa den beobachtenden Personen die Möglichkeit des Zoomens ohne Einschränkung zur Verfügung gestellt wird, kann eine unzulässige personenscharfe Videobeobachtung nicht ausgeschlossen werden. Daher muss der Bildsensor der digitalen Kamera unveränderbar so eingestellt sein, dass nur Bilder mit einer Auflösung von höchstens 800 x 640 Pixeln und nicht mehr als 72 oder 96 Bildpixeln auf einen Zoll Bildschirmfläche angefertigt werden. Außerdem darf zu diesem Zweck keine Zoomtechnik eingesetzt werden.

Soweit etwa die beobachtende Person bei unvorhersehbaren Ereignissen erkennen und veranlassen will, welche Rettungskräfte gerufen, und ob Fahrzeuge abgeschleppt werden sollen, muss die Nutzung einer Zoomtechnik durch Weisungen verbindlich bestimmt und auf Fälle

unvorhersehbarer Ereignisse beschränkt sein. In solchen Fällen ist außerdem zu dokumentieren, wer die Zoomtechnik zu welchem Zweck wann eingesetzt hat, damit eine datenschutzrechtliche Kontrolle möglich bleibt.

➡ Reichen Übersichtsbilder zur Verkehrsbeobachtung und -lenkung aus, dürfen keine personenscharfen Aufnahmen gemacht werden. Dies ist durch technische und organisatorische Maßnahmen sicherzustellen.

5 Bildung und Wissenschaft

5.1 Innovationen im Schulbereich: Gut gemeint, aber ...

... nicht immer auch gut gemacht. Vor allem der Befund notwendiger Bildungsreformen hat zu einigen rasanten Änderungen im Schulbereich geführt. Nicht immer hält jedoch die Schaffung datenschutzgerechter Rahmenbedingungen mit der Geschwindigkeit der Entwicklung neuer Ideen, Konzepte, Projekte und Strategien Schritt. Drei Beispiele zeigen dies:

Erhebung von Daten zum Migrationshintergrund: Vergleichsstudien belegen, was längst schon befürchtet worden war: Schülerinnen und Schüler mit Migrationshintergrund haben hierzulande oftmals schlecht(er)e Bildungschancen. National, aber auch international werden deshalb zu Recht eine bessere und gezielte Förderung dieser Kinder und Jugendlichen sowie ihre Chancengleichheit angemahnt. Um den Schulen eine Erhebung und Verarbeitung entsprechender Grundlagendaten zu ermöglichen und außerhalb der Schulen anhand von statistischen Daten strukturelle Probleme aufzeigen und nachvollziehen zu können, wurde im Juni 2007 die Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I) novelliert.

Was jedoch bei dem Bestreben, zügig und schnell verlässliche statistische Angaben zu bekommen, offenbar nicht bedacht wurde, war das Erfordernis, sowohl die Schulleitungen und Lehrkräfte als auch die betroffenen Schülerinnen, Schüler und ihre Eltern rechtzeitig und umfassend aufzuklären: Häufig fehlten klare und eindeutige Informationen, durch wen, zu welchem Zweck und auf welcher Rechtsgrundlage die Daten zum Migrationshintergrund erhoben und verarbeitet werden sollten. Auch der unbedingt erforderliche Hinweis auf die Auskunftspflicht der betroffenen Personen wurde häufig vermisst. Viele Probleme und Sorgen vor Ort hätten dem Vernehmen nach vermieden werden können, wenn das Schulministerium NRW als veranlassende Stelle selbst die erforderlichen Informationen erstellt, geeignete Erhebungsbögen konzipiert und den Schulen Hinweise zur Durchführung der Erhebung gegeben hätte.

So aber kam es zu einer Vielzahl von Nachfragen besorgter Personen, die etwa eine Übermittlung personenbezogener Daten an das Schulmi-

nisterium NRW oder an andere Stellen, eine zentrale Verwaltung dieser Personendaten im Land sowie eine Stigmatisierung von Kindern mit Migrationshintergrund befürchteten. Mangels Aufklärung wurden in einigen Schulen unzulässigerweise Daten zur Existenz und Dauer einer Aufenthaltserlaubnis erhoben. Bei dem Erhebungsverfahren selbst wurde nicht immer den Anforderungen des Datenschutzes entsprechend verfahren, indem etwa die Erhebungen während des Unterrichts durchgeführt oder bei Kindern Angaben über ihre Eltern erhoben wurden. Als Folge der Anfrageflut entstand die Information "Datenerhebung zum Migrationshintergrund durch Schulen", die auf der Homepage www.ldi.nrw.de abrufbar ist.

Die verantwortlichen Stellen werden anhand der Praxiserfahrungen zukünftig noch zu überprüfen haben, ob tatsächlich die Erhebung und Verarbeitung aller in der Neufassung der VO-DV I vorgesehenen Angaben zum Migrationshintergrund auch tatsächlich erforderlich sind. Nicht außer Acht gelassen werden darf in diesem Zusammenhang, dass die Daten über den Migrationshintergrund von Kindern einer Schule in anonymisierter Form grundsätzlich nach § 4 Abs. 1 Informationsfreiheitsgesetz NRW zugänglich sind.

Sprachstandsfeststellung: Um rechtzeitig festzustellen, welche Kinder eine zusätzliche Sprachförderung benötigen, wurde 2007 relativ kurzfristig das so genannte Sprachstandsfeststellungsverfahren eingeführt, dem sich alle Kinder zwei Jahre vor der Einschulung verpflichtend zu unterziehen haben. Bei Beginn des Verfahrens stand noch nicht abschließend fest, wie letztlich mit den Daten verfahren werden sollte. Die kurzfristig erstellten Informationen erreichten offenbar nicht stets die Verantwortlichen und Betroffenen vor Ort oder sie wurden nicht immer richtig verstanden.

Vor der Durchführung des Verfahrens 2008 wurden noch verschiedene Vorschriften ergänzt oder neu geschaffen. So wurden durch eine Änderung des § 120 Abs. 1 Satz 1, Abs. 3 Satz 1 Schulgesetz NRW (SchulG NRW) die Kinder, die an der Sprachstandsfeststellung teilzunehmen haben, in den Anwendungsbereich der spezifischen Datenschutzregelungen des SchulG NRW einbezogen. Die Neuregelung in § 14 Abs. 3 Satz 1 Kinderbildungsgesetz NRW erlaubt nunmehr die Übermittlung bestimmter Angaben durch die Erzieherinnen und Erzieher der Kindergärten zur Durchführung der Sprachstandsfeststellung. Auch in der zweiten Runde gab es noch Nachfragen zur Datenverar-

beitung und wiederum Hinweise, dass die vorbereiteten Informationen ihren Zielgruppen nicht immer zugingen und nicht alle Fragen hinreichend klärten. Deshalb findet sich eine eigene Information "Elefant, Bär, Affe & Co. – Wenn beim 'Zoobesuch' der Sprachstand getestet wird (Sprachstandsfeststellung 2008)" auf der Homepage www.ldi.nrw.de. Darin wird der Prozess der Datenverarbeitung im Rahmen des Sprachstandsfeststellungsverfahrens eingehend dargestellt. Damit sind zugleich auch die Grenzen der zulässigen Datenverarbeitung für die Zukunft transparent abgesteckt, sofern das Verfahren keinen Änderungen unterworfen wird.

Landesimpfkampagne: Als letztes Beispiel sei die als gemeinsame Aktion des Schul- und des Gesundheitsministeriums NRW ins Leben gerufene "Landesimpfkampagne" genannt. Ziel war es, den Impfstatus von Schülerinnen und Schülern anhand ihrer Impfausweise von den Gesundheitsämtern überprüfen zu lassen und gegebenenfalls Nach- und Neuimpfungen anzubieten. Als freiwilliges Serviceangebot ist gegen diese Aktion nichts einzuwenden.

Die Betonung muss hier indes auf der Freiwilligkeit des Angebotes liegen, denn es gibt keine Rechtsvorschrift, die eine solche Datenverarbeitung im Rahmen einer allgemeinen Prävention ohne die Einwilligung der Betroffenen erlauben würde. In den gemeinsamen Anschreiben der beiden Ministerien an Schulen und Eltern fanden sich diesbezüglich allerdings nur vage und unzureichende Hinweise.

Die Folge waren wiederum viele Nachfragen zum Datenschutz, die durch eine vorherige hinreichende Information aller beteiligten Stellen und betroffenen Personen hätte vermieden werden können. Das Schulministerium NRW stellte in einem Schreiben an das Gesundheitsministerium NRW ausdrücklich klar, dass die Schulen die Kampagne nicht dadurch unterstützen dürften, dass sie Schülerlisten über die Abgabe und Nichtabgabe von Impfausweisen für die Gesundheitsämter erstellten und diesen übermittelten. Die Angabe "Vorlage des Impfausweises" sei zudem kein Datum, das von den Schulen erhoben und an andere Stellen übermittelt werden dürfe. Die Teilnahme an der Kampagne und den angebotenen Impfungen sei vielmehr freiwillig. Diese Auffassung ist zutreffend, hätte aber auch den Schulen bekannt gegeben werden müssen. Eine andere Wertung könnte allenfalls geboten sein, wenn ein Gesundheitsamt aufgrund einer konkreten Gefahrenlage im Einzelfall ausnahmsweise weitergehende Maßnahmen zur Ge-

fahrenabwehr für unbedingt erforderlich halten und anordnen würde, nicht jedoch bei einer allgemeinen Vorsorgeaktion wie der Landesimpfkampagne.

Das Schulministerium NRW wurde auf die Verunsicherungen vor Ort hingewiesen, und es wurde empfohlen, durch geeignete Maßnahmen darauf hinzuwirken, dass den Anforderungen des Datenschutzes bei der Durchführung der Kampagne Rechnung getragen, insbesondere auch die Freiwilligkeit der Teilnahme hinreichend bekannt gegeben sowie sichergestellt wird. Da die Kampagne zu diesem Zeitpunkt bereits begonnen hatte, erscheint zweifelhaft, dass etwaige Informationen die Verantwortlichen und Betroffenen vor Ort rechtzeitig erreichten.

➡ Datenschutz und Datensicherheit müssen von Anfang an selbstverständliche Bestandteile aller Planungen, Projekte und Innovationen im Schulbereich sein. Dabei sind die rechtlichen Rahmenbedingungen ebenso zu beachten wie die Notwendigkeit, die Handelnden und die Betroffenen rechtzeitig und umfassend über die geplanten Datenverarbeitungen zu informieren.

5.2 Schule und Jugenddelinquenz: Damit aus "Mücken" keine "Elefanten" werden ...

... und "Elefanten" nicht zu "Mücken" schrumpfen, ist in Schulen vor allem eines wichtig: Das richtige Fingerspitzengefühl der Schulleitungen und Lehrkräfte in jedem Einzelfall. Dies gilt vor allem auch für die Entscheidung über die Einschaltung der Polizei und die damit verbundene Übermittlung personenbezogener Daten.

Im Schulgesetz NRW (SchulG NRW) ist klar geregelt, mit welchen erzieherischen Einwirkungen und Ordnungsmaßnahmen die Schule auf Fehlverhalten ihrer Schülerinnen und Schüler reagieren kann. In aller Regel genügen diese Sanktionen, um die geordnete Unterrichts- und Erziehungsarbeit sowie den Schutz von Personen und Sachen in der Schule sicherzustellen. Nur im Ausnahmefall bedarf es der Einschaltung der Polizei. Ein gemeinsamer Runderlass verschiedener

Ministerien resultiert aus der Bemühung, den Schulen zu diesem Themenkomplex Hilfestellungen zu geben.

Sollen personenbezogene Daten von Schülerinnen und Schülern an die Polizei übermittelt werden, ist dies nur nach Maßgabe des § 120 Abs. 5 Satz 2 SchulG NRW zulässig. Weder der angesprochene Erlass noch der in verschiedenen Vorschriften verankerte Appell zur "guten Zusammenarbeit" zwischen Schulen und Polizei kommen als Rechtsgrundlagen für einen solchen Datentransfer in Betracht. Zugegebenermaßen kann die Entscheidung, ob die Polizei zur Gefahrenabwehr oder zwecks Strafverfolgung eingeschaltet werden muss, im Einzelfall schwierig sein. Die Schulen dürfen dabei vor allem ihre eigenen Aufgaben, die Verantwortung für ihre Schülerinnen und Schüler sowie den Grundsatz der Verhältnismäßigkeit nicht aus den Augen verlieren.

Ein Fall, der das notwendige Fingerspitzengefühl in eklatanter Weise vermissen ließ, ereignete sich an einem Gymnasium. Weil eine Lehrkraft bei einem 13jährigen Schüler festgestellt zu haben glaubte, dass er während des Unterrichts wiederholt Blickkontakt zu einem als rechtsradikal bekannten Mitschüler suchte, er sich in einigen Pausen mit ihm unterhielt und einmal während des Geschichtsunterrichts – zu der abstrakten Frage der Abgrenzung zwischen Anhängern, Mitläufern und Kritikern faschistischer Bewegungen – äußerte, Anhänger seien diejenigen, die ihre eigenen Ziele verfolgten und zu jeder Zeit wüssten, wann sie aussteigen könnten, schaltete die Schule den polizeilichen Staatsschutz ein. Pädagogische Einwirkungen wurden ebenso wenig erwogen wie ein Gespräch der Lehrkraft mit dem Kind und/oder seinen Eltern. Am nächsten Tag wurde der Junge in der Schule in Anwesenheit einer Lehrkraft einem 45minütigen sogenannten "Präventionsgespräch" mit zwei Polizeibeamten ausgesetzt. Seine Eltern waren weder über die Datenübermittlung noch über das bevorstehende "Gespräch" informiert worden. Die Polizei kam letztlich zu der Erkenntnis, das Kind sei vollkommen unauffällig und nicht an der rechten Szene interessiert. Gleichwohl hatte die verhörähnliche Situation für den Jungen gravierende Folgen: Eltern und Schule stellen übereinstimmend eine große Verängstigung und nachhaltige Verunsicherung des Kindes seit diesem Termin fest. Das Gesprächsprotokoll wird noch immer personenbezogen bei der Polizei aufbewahrt. Die LDI NRW hat das Verhalten der Schule förmlich beanstandet und wirkt darauf hin, dass die

über das Kind gespeicherten Daten bei der Polizei vollständig gelöscht werden.

Anders war ein Fall zu beurteilen, in dem ein Schüler in einem Schriftstück den Holocaust leugnete. Hier war die Entscheidung der Schulleitung, die Unterlage mit den entsprechenden Angaben zur Person des Schülers an die Polizei weiterzugeben, nicht zu beanstanden, da der hinreichende Verdacht einer nicht unerheblichen Straftat vorlag. Dasselbe gilt für die Entscheidung einer anderen Schulleitung, Anzeige gegen einen ehemaligen Schüler zu erstatten. Der 13jährige Gymnasiast hatte nach seinem Schulverweis in dem für alle Userinnen und Usern zugänglichen Bereich von "SchülerVZ" einem Freund vorgeschlagen, seine ehemalige Schule aufzusuchen und einen Anschlag auf den Schulleiter und/oder die Schule zu verüben. Da der Junge zuvor bereits mehrfach gewalttätig geworden war, bestand die konkrete Gefahr, dass eine neuerliche erhebliche Gewalttat bevorstehen könnte. Deshalb wurde die Polizei informiert, um gegebenenfalls rechtzeitig eingreifen zu können.

➡ Es gehört zu den originären Erziehungsaufgaben der Schule, auf Fehlverhalten ihrer Schülerinnen und Schüler adäquat zu reagieren. In aller Regel genügen hierzu pädagogische Einwirkungen und Sanktionen. Nur in Ausnahmefällen dürfen personenbezogene Daten an die Polizei übermittelt werden. Bei Minderjährigen sind in diesen Fällen unverzüglich die Eltern zu unterrichten.

5.3 Dunkelfeldforschung im Lichte des Datenschutzes

Wer mit besonders sensiblen Daten forscht, muss strengen Anforderungen genügen. Dies gilt insbesondere für wissenschaftliche Projekte zur offenen oder verdeckten Kriminalität von Jugendlichen. Deshalb rückte im letzten Jahr ein Forschungsvorhaben zur Dunkelfeldkriminalität ins Scheinwerferlicht des Interesses.

Geplant war eine bundesweite Befragung von Kindern und Jugendlichen, die auch an nordrhein-westfälischen Schulen durchgeführt werden sollte. Dabei ging es um verschiedene Themenfelder. Im Zentrum der Studie stand allerdings eine Erhebung zur Kriminalität:

Die Schülerinnen und Schüler sollten in den Fragebögen sowohl Angaben zu eigenem kriminellen Verhalten als auch zu strafbaren Handlungen ihrer Eltern und anderer Personen machen, und zwar insbesondere auch zu solchen Taten, die nicht aufgedeckt und verfolgt worden waren.

Unzweifelhaft sind solche Forschungsvorhaben wichtig. Das ursprüngliche Konzept dieses Projekts berücksichtigte nach Auffassung der LDI NRW – die vom Schulministerium NRW sowie von Datenschutzbeauftragten und obersten Schulaufsichtsbehörden anderer Länder geteilt wurde – die Datenschutzbelange der Betroffenen jedoch nicht hinreichend. Vor allem bestand die Gefahr, dass die ausgefüllten Fragebögen den einzelnen Schülerinnen und Schülern und somit gegebenenfalls auch ihren Eltern hätten zugeordnet werden können. Damit hätten aber zum Beispiel im Falle einer polizeilichen Beschlagnahme die vertraulich geäußerten Selbst- und Fremdbezichtigungen zu ungewollten Folgen für die Betroffenen führen können. Gerade vor diesem Hintergrund schien überdies die Information der Teilnehmenden und ihrer Eltern über die Datenverarbeitung im Rahmen des Projekts unzureichend, so dass insgesamt dringender Beratungsbedarf bestand.

Dabei war die datenschutzgerechte Lösung im Grunde einfach: Wenn bei der Konzeption sichergestellt wird, dass die ausgefüllten Fragebögen weder aus sich selbst heraus noch durch Kombination verschiedener Fragen und/oder mit Zusatzwissen auf einzelne Personen rückbeziehbar – also anonymisiert – sind, können in den Bögen auch sehr persönliche Fragen gestellt und äußerst sensible Angaben – auch zu Dritten wie zum Beispiel den eigenen Eltern – erhoben werden. Darüber hinaus muss selbstverständlich die Durchführung vor Ort den Anforderungen des Datenschutzes genügen. Im konkreten Fall war es vor allem wichtig, dass auf den Fragebögen weder eine Schul- noch eine Klassenangabe vermerkt und bei allen Ortsangaben dafür Sorge getragen wurde, dass die Regionen hinreichend groß gewählt wurden, um auch insoweit die Möglichkeit eines Rückbezugs auf einzelne Personen hinreichend sicher auszuschließen.

Trotz dieser praktikablen Lösung, die den wissenschaftlichen Zweck des Vorhabens nicht gefährdete, entpuppte sich die datenschutzrechtliche Beratung des – nicht in Nordrhein-Westfalen ansässigen – Forschungsteams als außergewöhnlich schwierig, zumal mit der Durch-

führung des Projekts bereits begonnen worden war. Erfreulich gestaltete sich dabei indes die Kooperation mit dem Schulministerium NRW.

Abschließend sei an die Verantwortung der Schulleitungen bezüglich der Durchführung von Forschungsvorhaben an ihren Schulen erinnert. Nach § 120 Abs. 4 Satz 2 Schulgesetz NRW (SchulG NRW) entscheidet nicht etwa die Schulaufsicht über diese Durchführung, sondern die jeweilige Schulleitung. Ein einschlägiger Erlass sollte dabei als Hilfe herangezogen werden. Selbstverständlich haben die Schulaufsichtsbehörden eine Beratungspflicht, sofern sie mit den Projekten befasst werden (siehe auch § 120 Abs. 4 Satz 3 SchulG NRW).

➧ Vor Durchführung eines Forschungsvorhabens muss sichergestellt sein, dass die Konzeption den Anforderungen des Datenschutzes in jeder Hinsicht genügt. Schulleitungen haben in eigener Verantwortung zu prüfen und dafür Sorge zu tragen, dass bei der Durchführung von wissenschaftlichen Projekten an ihren Schulen Datenschutzverstöße ausgeschlossen sind.

5.4 Fundraising: Von goldenen Kälbern ...

... und solchen, die es noch werden sollen. In Zeiten knapper finanzieller Mittel suchen auch Hochschulen verstärkt nach Möglichkeiten, Spenden- und Sponsorengelder zu akquirieren. Bei diesem Fundraising ("Kapitalbeschaffen") dürfen allerdings die Datenschutzbelange der potentiellen Spenderinnen und Spender nicht außer Acht gelassen werden.

Bislang wurde der LDI NRW noch kein Fundraising-Konzept zur Prüfung vorgelegt. Hinweise aus verschiedenen Hochschulen lassen jedoch befürchten, dass der verständliche Wunsch zur Mittelbeschaffung unverständlicherweise Überlegungen zum Datenschutz unberücksichtigt lässt. Drei fiktive, aber dem Vernehmen nach nicht unwahrscheinliche Beispiele verdeutlichen das Problem:

Bei einer wissenschaftlichen Veranstaltung überreicht Herr Dr. X seiner Kollegin Frau Prof. Y seine Visitenkarte. Er beabsichtigt damit, eine Kontaktpflege zum Zweck des wissenschaftlichen Austauschs zu ermöglichen. Frau Prof. Y, gegebenenfalls auch ihre Mitarbeiterinnen und Mitarbeiter, eventuell noch die Kolleginnen und Kollegen des Fachbe-

reichs, sollen die Möglichkeit haben, ihn zu Fragen der Wissenschaft und Forschung zu kontaktieren. Dagegen verfolgt Dr. X mit der Übergabe seiner Visitenkarte nicht den Zweck, dass seine Daten an die Fundraising-Stelle weitergegeben und in eine Datenbank eingestellt werden, um fortan regelmäßig mit Spendenaufrufen behelligt zu werden. Wenig erfreut dürfte er auch sein, wenn die Informationen, die er unbedacht am Rande eines Gesprächs mit der Kollegin geäußert hat (letzter Urlaub in der Karibik, kürzlich Anschaffung eines neuen Luxusautos) mit in die Datenbank eingegeben werden, um Angaben zu seinem möglichen "Wert" als Spender festzuhalten und zu sammeln. Eine Rechtsvorschrift, die eine solche Datenverarbeitung erlauben würde, ist nicht ersichtlich. Seine konkludent erteilte Einwilligung erlaubt nur die Kontaktpflege.

Frau Z meldet sich zu dem – aus Fundraising-Sicht möglicherweise lukrativ klingenden – Symposium "Die Erbinnen und Erben von heute sind die Anlegerinnen und Anleger von morgen" der Wirtschaftsfakultät einer Universität an. Die Daten, die sie in dem Anmeldeformular angibt, dürfen grundsätzlich nur zum Zweck der Abwicklung des Anmeldeverfahrens sowie der Teilnahme und Abrechnung verarbeitet werden. Schon die Aufnahme in eine Teilnehmendenliste, die an alle Anwesenden ausgehändigt werden soll, bedarf der Einwilligung. Erst recht müssen die Teilnehmenden einwilligen, wenn die Daten darüber hinaus zu Fundraising-Zwecken an die entsprechende Stelle der Hochschule oder eine Fundraising-Stiftung weitergegeben, dort zu diesem Zweck gespeichert und genutzt werden sollen.

Spendet der Mäzen M der Hochschule einen Geldbetrag zur Förderung von Forschung und Wissenschaft, darf und muss die Hochschule die in diesem Zusammenhang erforderlichen Daten zum Zweck der ordentlichen Haushaltsführung und der Rechnungslegung verarbeiten. Zugriff auf diese Daten dürfen grundsätzlich nur die mit der Verbuchung und Abrechnung betrauten Beschäftigten nehmen. Zulässig wäre es möglicherweise ferner, dass die Abrechungsstelle selbst dem Mäzen nach angemessener Zeit ein vorgefertigtes Schreiben mit einer erneuten Bitte um eine Spende übersendet. Ob es darüber hinaus auch zulässig sein könnte, dass die Fundraising-Stelle der Hochschule und/oder die Fundraising-Stiftung Zugriff auf seine Daten nimmt, scheint dagegen jedenfalls dann fraglich, wenn nicht unmittelbar an diese Stellen gespendet wurde.

- Zu Zwecken des Fundraising dürfen Hochschulen nicht alle Daten nutzen, die in ihrer Sphäre erhoben und verarbeitet werden oder derer sie habhaft werden können. Auch hier gilt der Gesetzesvorbehalt bei der Einschränkung des Rechts auf informationelle Selbstbestimmung. Im Übrigen sind die Grundsätze der Zweckbindung und Datenvermeidung strikt zu beachten.

6 Handel und Wirtschaft

6.1 Mehr Datenschutz wagen! – Teil 1: Bundestag berät Gesetzentwurf zu Auskunfteien und Scoring

Umfragen belegen es seit Jahren: Die Bürgerinnen und Bürger haben wenig Vertrauen in die datenschutzgerechte Verwendung ihrer Daten durch Unternehmen und sehen darin eine große Gefahrenquelle für ihre Privatsphäre. Dennoch fristete der Schutz vor den Gefährdungen des kommerziellen Datensammelns in der politischen Sphäre lange ein Schattendasein. Nun befinden sich gleich zwei Gesetzentwürfe im Orbit des Raumschiffs Berlin, um den Datenschutz in der Privatwirtschaft zu stärken. Beide sind jedoch bedroht, durch massive Angriffe der jeweiligen Wirtschaftslobby noch weiter vom ursprünglichen Kurs abzukommen oder gar ganz abzustürzen.

Mit dem ersten Gesetzesvorhaben sollen die Anforderungen an Auskunfteien und Scoring-Verfahren im Bundesdatenschutzgesetz (BDSG) konkretisiert werden. Nachdem der Bundestag bereits 2005 über alle Fraktionsgrenzen hinweg Handlungsbedarf zum Datenschutz bei Auskunfteien festgestellt hatte, legte das Bundesinnenministerium Mitte 2007 einen ersten Entwurf vor. Ein Jahr und etwa ein halbes Dutzend Entwurfsfassungen später beschloss das Kabinett einen Gesetzentwurf, den der Bundestag bis Ende 2008 weder beraten noch verabschiedet hat.

Welche Regelungen sind zu Auskunfteien geplant?

- Es soll eine neue Norm (§ 28a BDSG) zu Datenübermittlungen an Auskunfteien geben, die erstmals detaillierte Anforderungen an die Einmeldung von Negativdaten enthält. Auch sollen Positivdaten zu Bankverträgen künftig nicht mehr aufgrund einer – mangels Freiwilligkeit zweifelhaften – Einwilligung wie etwa der SCHUFA-Klausel, sondern aufgrund einer gesetzlichen Regelung erfolgen. Zudem sollen die von Banken an Auskunfteien wie die SCHUFA übermittelten "Konditionenanfragen" von Kreditsuchenden nur noch dann zulässig sein, wenn die Information von den Auskunfteien nicht mehr für Auskünfte oder Score-Berechnungen verwendet werden (siehe zur Problematik den Beitrag unter 6.3). Die Regelungen vollziehen im We-

sentlichen die Auslegungen der Datenschutzbehörden zum bisherigen Recht nach und sind in der von der Bundesregierung vorgelegten Fassung trotz kleinerer Mängel grundsätzlich positiv zu bewerten.

- Eine wirtschaftsfreundliche Definition des zur Abfrage von Auskunfteidaten berechtigenden Interesses in § 29 BDSG ist nach heftiger Kritik hoffentlich endgültig aus dem Entwurf verbannt. Die ersten Entwürfe hatten vorgesehen, dass künftig jedes wirtschaftliche Interesse zum Abruf von Auskunfteidaten berechtigt hätte. Damit wäre letztlich allen Unternehmen und jeder Person mit einem wie auch immer begründeten wirtschaftlichen Interesse die Tür zu Auskunfteidaten weit geöffnet worden. Nach bisheriger Auslegung dürfen Unternehmen nur Bonitätsinformationen abfragen, wenn sie in einer laufenden oder konkret bevorstehenden Vertragsbeziehung mit der betroffenen Person ein finanzielles Ausfallrisiko tragen. Eine entsprechende gesetzgeberische Klarstellung wäre wünschenswert.
- Positiv zu bewerten ist eine geplante Ergänzung des § 34 BDSG dahingehend, dass künftig jede Person einmal je Kalenderjahr eine unentgeltliche Auskunft über die zu ihr gespeicherten Daten verlangen kann.

Welche Regelungen sind zum Scoring geplant?

- Eingefügt werden soll ein neuer § 28b BDSG, der in sehr allgemeiner Form regelt, welche personenbezogenen Daten für die Berechnung von Score-Werten genutzt werden dürfen. Inhaltlich ist insbesondere Folgendes zu kritisieren: Künftig soll die "Nutzung von Anschriftendaten" der betroffenen Personen für die Berechnung der Score-Werte zulässig sein, soweit die Betroffenen vorab darüber unterrichtet wurden. Hinter der harmlos wirkenden Formulierung "Nutzung der Anschriftendaten" verbirgt sich die berüchtigte Wohnumfeldbewertung einer Person. Im Rahmen eines Score-Verfahrens zur Bonitätsbewertung bedeutet dies, dass die betroffene Person in "statistische Sippenhaft" genommen wird mit den sonstigen Personen in dem entsprechenden Stadtteil und deren durchschnittlichem Ausfallrisiko. So kann sich ein Wohnumfeld, das angeblich vorwiegend durch Personen mit "niedrigem sozialen Status"

geprägt ist, negativ auf den Score-Wert aller dort lebenden Person auswirken – unabhängig von den tatsächlichen Eigentums- und Vermögensverhältnissen im Einzelfall. Dies kann zur Folge haben, dass etwa eine Person allein aus diesem Grund höhere Zinsen zahlen muss. Gesamtgesellschaftlich kann die Nutzung der Wohnumfeldbewertung für das Scoring zur sozialen Ausgrenzung von Stadtteilen – "Ghettoisierung"– beitragen (mehr zu der Problematik wie auch zum Scoring allgemein im Bericht 2005 unter 5.7). Der Bundestag sollte daher im weiteren Gesetzgebungsverfahren die "Nutzung der Anschriftendaten" wie auch die Nutzung anderer möglicherweise diskriminierender Merkmale – etwa die Herkunft und das Geschlecht einer Person – für Zwecke des Scoring untersagen.

- Grundsätzlich positiv zu bewerten ist eine Ergänzung des § 34 BDSG mit Regelungen, die das Auskunftsrecht zu Score-Werten verbessern sollen (zu der entscheidenden Bedeutung der Transparenz für das Scoring und den rechtlichen und technischen Möglichkeiten, diese zu verbessern, siehe Bericht 2007 unter 7.1). Allerdings gab es im Rahmen des bisherigen Gesetzgebungsverfahrens gerade zur Frage der Transparenz eine bedauerliche Aufweichung der Anforderungen. In den ursprünglichen Entwürfen waren detaillierte Regelungen enthalten, die etwa eine Auskunftspflicht zu der Gewichtung der für den konkreten Score-Wert wesentlichen Datenarten vorsahen. Nach massiver Kritik der Auskunfteien und Banken schwächten die beteiligten Ministerien die Formulierungen nach und nach ab. So wurden aus einer späteren Fassung des Gesetzentwurfs auch die von den Aufsichtsbehörden einmütig formulierten Anforderungen an die Transparenz, die sogar in den USA bereits für Auskunfteien gesetzlich festgeschrieben sind (siehe Bericht 2007 unter 7.1), wieder entfernt und stattdessen eine allgemein gehaltene und damit unterschiedlich auslegbare Formulierung aufgenommen. Hoffnungsvoll stimmt in diesem Zusammenhang allein, dass die Banken in einem Gutachten zu den Folgekosten der geplanten Gesetzesänderung die entsprechende Regelung zur Transparenz datenschutzfreundlich im Sinne der Bürgerinnen und Bürger auslegten.

Welche sonstigen Verbesserungen sind geplant? Positiv hervorzuheben ist, dass ein neuer Bußgeldtatbestand für nicht erteilte Auskünfte an Betroffene geschaffen werden soll. Damit würde endlich die Gesetzeslücke geschlossen, nach der zwar die Unternehmen und sonstigen Stellen zur Auskunftserteilung verpflichtet sind, diese Pflicht aber ungestraft verletzt werden kann.

Was fehlt in dem Entwurf? Neben den bereits erwähnten Unzulänglichkeiten des Entwurfs insbesondere im Bereich des Scoring fällt vor allem das Fehlen einer Regelung zu einer Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme auf. Der Deutsche Bundestag hatte 2005 einstimmig die Bundesregierung aufgefordert, die Beschränkung der Profilbildung und die Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme durch gesetzliche Regelungen zu prüfen. Ebenfalls 2005 hatten die Datenschutzbehörden das Bundesinnenministerium gebeten, den § 29 BDSG klarstellend dahingehend zu präzisieren, dass Vermieterinnen und Vermietern nur Daten aus branchenspezifischen Auskunftssystemen übermittelt werden dürfen. Sowohl die Forderung des Bundestages als auch der Wunsch der Datenschutzbehörden finden sich im Entwurf nicht wieder.

➡ Der Bundestag sollte dem Druck der Auskunfteien und Banken nach weiteren Aufweichungen der Regelungen standhalten und den Gesetzentwurf noch in dieser Legislaturperiode beschließen. Besser würden die Bürgerinnen und Bürger jedoch vor unfairen, undurchschaubaren Scoring-Verfahren und den stetig wachsenden Datensammlungen der Auskunfteien geschützt, wenn der Bundestag mehr Datenschutz wagt als die Bundesregierung und die oben dargestellten Mängel beseitigt.

6.2 Mehr Datenschutz wagen! – Teil 2: Gesetzentwurf zum Schutz vor unerwünschtem und illegalem Datenhandel

2008 war das Jahr der Datenschutzskandale. In einer nicht abreißenden Serie von "Pannen" gelangten mehrere Millionen sensibler Kundendaten in falsche Hände. Als daraus gesetzge-

berische Konsequenzen gezogen werden sollten, wehrten sich die am Datenhandel verdienenden Unternehmen massiv gegen den Verlust ihrer Privilegien. Erst nachdem auch im Dezember 2008 ein Datendiebstahl den nächsten jagte, legte die Bundesregierung einen Gesetzentwurf vor. Doch welche der vielen Verbesserungsvorschläge berücksichtigt der Entwurf – und welche nicht?

Die zweite Gesetzesnovelle zum Bundesdatenschutzgesetz (BDSG) ist Ausfluss des so genannten Datenschutzgipfels des Bundes und der Länder Anfang September 2008 in Berlin. Dort wurde beraten, wie künftig der Missbrauch von Kundendaten soweit wie möglich verhindert werden kann. Je eine Arbeitsgruppe auf Bundes- wie auf Länderebene entwickelten daraufhin zügig Vorschläge für erforderliche Gesetzesänderungen. Der Bericht der Länderarbeitsgruppe basierte auf den praktischen Erfahrungen der mit der Kontrolle von Unternehmen befassten Datenschutzbehörden. Schnell wurde jedoch deutlich, dass einige Bundesministerien keinen Wert auf die Vorschläge der Länder legten. So blieben die weitergehenden und teilweise auch effektiveren Vorschläge der Länderarbeitsgruppe im Gesetzentwurf der Bundesregierung unberücksichtigt. Stattdessen konnte die Lobby des Adresshandels, der Werbewirtschaft und der davon abhängigen Unternehmen einige Ausnahme- und Übergangsregeln durchsetzen. Abzuwarten bleibt, ob der Bundestag nun die Forderungen der Datenschutzbehörden aufnimmt oder den Unternehmen noch weiter entgegenkommt.

Der Gesetzentwurf enthält folgende wesentliche Änderungen:

- **Einschränkung des so genannten Listenprivilegs:** Bislang dürfen Unternehmen bestimmte Daten auch ohne Einwilligung der Betroffenen für Werbezwecke anderer Stellen verkaufen oder nutzen. Zu diesen unter das so genannte Listenprivileg fallenden Daten gehören der Name, der Beruf, die Anschrift, das Geburtsjahr sowie eine Angabe über die Zugehörigkeit der Betroffenen zu einer Personengruppe. Der Gesetzentwurf sieht vor, dass künftig ein Verkauf oder eine Nutzung dieser Daten für Webezwecke Dritter grundsätzlich nur mit Einwilligung der Betroffenen möglich ist. Allerdings gibt es einige Ausnahmen, so dass das Listenprivileg – anders als auf dem Datenschutzgipfel angekündigt – nicht vollständig gestrichen wird.

Auch ohne Einwilligung sollen künftig Daten gehandelt werden dürfen, wenn dies für die Spendenwerbung steuerbegünstigter Organisationen erfolgt. Die Erfahrungen der Datenschutzbehörden zeigen allerdings, dass Spendenorganisationen nicht unbedingt sorgfältiger und datenschutzgerechter mit personenbezogenen Daten umgehen. Eine weitere Ausnahme soll für die Werbung gegenüber freiberuflich oder gewerblich Tätigen unter deren Geschäftsadresse gemacht werden. Auch hierfür soll die Einwilligung nicht erforderlich sein.

Ohne Einwilligung zulässig sein soll auch die Nutzung von Kundendaten, um sie für Werbezwecke Dritter eigenen Werbe- oder Geschäftsschreiben beizulegen. Und schließlich sollen Unternehmen ihre eigenen Kundinnen und Kunden weiterhin ohne deren Einwilligung bewerben und für diese Werbung zusätzliche Daten speichern dürfen.

- **Anforderungen an die Einwilligung für Werbezwecke:** Positiv zu bewerten ist, dass eine zusammen mit anderen Erklärungen erteilte Einwilligung für Werbezwecke anders als bisher nur wirksam sein soll, wenn sie durch ein aktives, ausschließlich auf die Einwilligung bezogenes Tun, etwa durch Ankreuzen oder eine gesonderte Unterschrift, erteilt wird. Auch darf der Abschluss eines Vertrages nicht von der Einwilligung abhängig gemacht werden, wenn der Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht oder nur in unzumutbarer Weise möglich ist.
- **Übergangsfrist für die neuen Regelungen zur Werbung:** Aufgrund des massiven Drucks der Wirtschaft soll ihr eine sehr großzügige Übergangsregelung gewährt werden. Danach dürfen Daten, die vor dem 1. Juli 2009 erhoben wurden, bis Juli 2012 nach den bislang geltenden Regelungen verwendet und verkauft werden. Die Bürgerinnen und Bürger müssen also noch mehr als drei Jahre warten, bis sie tatsächlich selbst darüber entscheiden können, wer mit ihren Daten handelt.
- **Informationspflicht bei schwerwiegenden Datenschutzpannen:** Stellt ein Unternehmen fest, dass Dritte unrechtmäßig Kenntnis von den bei dem Unternehmen gespeicherten, im Gesetzentwurf abschließend aufgezählten besonders sensiblen

Daten erhalten haben und dadurch den Betroffenen schwerwiegende Beeinträchtigungen drohen, ist das Unternehmen regelmäßig verpflichtet, die Betroffenen sowie die zuständige Datenschutzbehörde darüber zu informieren. Sollte die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern, kann sie durch eine näher geregelte Information der Öffentlichkeit in Tageszeitungen ersetzt werden.

Der Gesetzentwurf nennt folgende Kategorien von Daten, deren unrechtmäßige Kenntnis durch Dritte die Informationspflicht auslöst: Daten, die nach § 3 Abs. 9 BDSG einem besonderen Schutz unterliegen (etwa Daten zur Gesundheit, zum Sexualleben oder zu politischen oder religiösen Überzeugungen), Daten, die einem Berufsgeheimnis unterliegen, Bank- und Kreditkartendaten sowie Daten, die sich auf strafbare Handlungen beziehen.

- **Stärkung der Stellung der betrieblichen Datenschutzbeauftragten:** Der Kündigungsschutz und die Möglichkeiten, der betrieblichen Datenschutzbeauftragten sich fort- und weiterzubilden, sollen gestärkt werden.
- **Erweiterung des Bußgeldrahmens:** In Angleichung an den Bußgeldrahmen des Telekommunikationsrechts sollen der Bußgeldrahmen für Verfahrensverstöße von 25.000 Euro auf 50.000 Euro und der Bußgeldrahmen für Verstöße gegen materielle Vorschriften von 250.000 Euro auf 300.000 Euro angehoben werden. Im Übrigen soll das Bußgeld den wirtschaftlichen Vorteil übersteigen, den die Täterin oder der Täter aus der Ordnungswidrigkeit gezogen hat. Dabei darf im Einzelfall auch der Bußgeldrahmen überschritten werden.

Was fehlt in dem Gesetzentwurf?

- **Schaffung wirksamer Eingriffsbefugnisse für die Datenschutzbehörden:** Die zentrale und einvernehmliche Forderung der Länder und der Datenschutzbehörden lautete: Die Aufsichtsbehörden für den Datenschutz müssen die Möglichkeit erhalten, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Bislang können die Datenschutzbehörden den illegalen

Handel mit personenbezogenen Daten nur nachträglich durch die Verhängung eines Bußgeldes ahnden. Sie können also erst eingreifen, wenn das "Kind bereits in den Brunnen gefallen ist", also wenn die Daten nachweislich rechtswidrig an eine konkret zu ermittelnde Person übermittelt wurden und in einem Bußgeldverfahren ein individueller Schuldvorwurf feststellbar ist. Eine effektive Gefahrenabwehr bedarf anderer Instrumente. Folgerichtig haben die Ordnungsbehörden außerhalb des Datenschutzes das Recht, bei Gesetzesverstößen präventiv mit hoheitlichen Eingriffsbefugnissen tätig zu werden. Sie können eingreifen, wenn "das Kind auf dem Brunnenrand steht" und müssen nicht erst den Sturz und die Klärung des Schuldvorwurfs abwarten. Dieses ureigene Recht einer Aufsichtsbehörde, Anordnungen zu treffen, haben die Datenschutzbehörden bislang nur bei festgestellten technischen und organisatorischen Mängeln, nicht aber bei den oftmals schwerwiegenderen materiell-rechtlichen Datenschutzverstößen wie etwa dem illegalem Datenhandel. Die Schaffung einer wirksamen Eingriffsbefugnis wäre kostenneutral und würde rechtstreue Unternehmen nicht belasten. Vor allem aber bekäme der von Bürgerinnen und Bürgern, aber auch von betrieblichen Datenschutzbeauftragten oftmals beklagte "Papiertiger Datenschutzbehörde" Zähne. Das könnte einen entscheidenden Beitrag dazu leisten, dem Datenschutz in den Unternehmen Respekt zu verschaffen. Trotz dieser zahlreichen Vorteile wurde die zentrale Forderung der Länder nicht in den Gesetzentwurf aufgenommen. Dabei verlangt bereits die EG-Datenschutzrichtlinie aus dem Jahr 1995, dass die Datenschutzbehörden "wirksame Einwirkungsbefugnisse" erhalten sollen und nennt als Beispiel etwa die Möglichkeit, "das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen". Es bleibt das Rätsel des in anderen Bereichen auf starke Eingriffsrechte drängenden Bundesinnenministers, weshalb er den Datenschutzbehörden dieses Recht verweigern will.

- **Kennzeichnungspflicht über die Herkunft der Daten:** Eine der wesentlichen Forderungen des Datenschutzgipfels war eine Kennzeichnungspflicht über die Herkunft von Daten. Die Werbepost versendenden Unternehmen sollen mitteilen, woher sie die Daten der angeschriebenen Person haben. Nur so können

die Bürgerinnen und Bürger erkennen, ob es sich um einen Fall von illegalem Datenhandel handelt. Dennoch fehlt die Kennzeichnungspflicht in dem Gesetzentwurf. Die wenig überzeugende Begründung lautet: Künftig dürften die Daten ja ohnehin nur noch mit Einwilligung der Betroffenen gehandelt werden. Völlig unberücksichtigt bleiben dabei die zahlreichen vorgesehenen Ausnahmen und die Übergangszeit von drei Jahren. Und selbst wer eine Einwilligung zum Datenhandel erteilt hat und Jahre später unerwünschte Werbung erhält, möchte häufig – ohne zeitaufwändige Recherchen anstellen zu müssen – erfahren, woher die für die Werbung genutzten Daten stammen.

- **Schließung bedeutsamer Sanktionslücken im Bußgeldkatalog:** Der Gesetzentwurf enthält zwar zwei neue Bußgeldtatbestände, aber die entscheidende Lücke wurde trotz eines entsprechenden Vorschlags der Länderarbeitsgruppe nicht geschlossen: Werden in einem Unternehmen aufgrund fehlender Schutzvorkehrungen – etwa vor unberechtigtem Zugriff oder unbefugtem Zugang zu den Datenverarbeitungssystemen – sensible Daten entwendet, kann das Fehlverhalten des Unternehmens nicht geahndet werden. Es gibt zwar im BDSG eine Rechtspflicht, die entsprechenden technischen und organischen Maßnahmen zu ergreifen, aber keinen Bußgeldtatbestand, um ein Unterlassen zu sanktionieren. Vielen Datenschutzskandalen und –pannen lagen derartige mangelhafte Schutzvorkehrungen zur Datensicherheit zugrunde: So entwendeten vermutlich Beschäftigte eines großen Telekommunikationsunternehmens mangels interner Zugriffskontrollen 17 Millionen sensibler Kundendaten. Aufgrund eines Datenlecks im Internet bei demselben Unternehmen bestand für unbefugte Externe die Möglichkeit, 30 Millionen Daten von Handynutzerinnen und -nutzern abzurufen. Vergleichbare Datenlecks gab es 2008 bei einem Rechenzentrum, das für eine Bank in Berlin sensible Kreditkartendaten bearbeitete, und bei der Bewerberdatenbank eines großen Unternehmens. Zehntausende Daten landeten auf einem frei zugänglichen, aber für die deutschen Datenschutzbehörden nicht kontrollierbaren Webserver in China. Ein Datenleck bei einem Verlag führte dazu, dass Bankverbindungsdaten tausender Anzeigenkunden über das Internet weltweit abrufbar waren und Unbe-

fugte zudem delikate Chiffre-Inserate den konkreten Inserenten zuordnen konnten. Anders als beim – teilweise sich anschließenden – illegalen Datenhandel helfen hier präventive Eingriffsbefugnisse nur selten weiter. Denn derartige Datenschutzpannen werden in der Regel erst bekannt, wenn "das Kind in den Brunnen gefallen ist" und das Unternehmen unmittelbar danach das Datenleck schließt. Mangels Bußgeldtatbestand bleibt das Fehlverhalten des Unternehmens ungeahndet. Selbst wenn ein Unternehmen vorsätzlich, aus Kostengründen Akten mit sensiblen personenbezogenen Daten in öffentlich zugänglichen Papiercontainern entsorgt, fehlt nach der Sicherstellung der Akten bislang jede Möglichkeit, gegen das Unternehmen ein Bußgeldverfahren einzuleiten. Die geforderte Sanktionsmöglichkeit könnte helfen, den technisch-organisatorischen Maßnahmen zum Datenschutz einen größeren Stellenwert in der Unternehmenskultur zu verschaffen.

➡ Die Verabschiedung des Gesetzentwurfs wäre ein Fortschritt gegenüber der jetzigen Rechtslage, aber keine hinreichende Reaktion auf die mit den Skandalen aufgedeckten strukturellen Mängel des Datenschutzes in der Privatwirtschaft. Vor allem können nur Datenschutzbehörden mit wirksamen Eingriffs- und Sanktionsmöglichkeiten sowie ausreichendem Personal die zur Vertrauensbildung in der Bevölkerung notwendigen Kontrollen durchführen. Ohne Eingriffsmöglichkeiten und Personal drohen die Behörden Papiertiger wider Willen und die neuen Regelungen geduldiges Papier zu bleiben. Fragt sich nur, wem das nützt?

6.3 Alles über Auskunfteien – Datenschutzfragen rund um das Geschäft mit Bonitätsdaten

Die Tätigkeit von Auskunfteien und Warndateien gewinnt leider sowohl für Bürgerinnen und Bürger als auch für Unternehmen zunehmend an Bedeutung. Viele Unternehmen, die gegenüber ihren Kundinnen und Kunden in Vorleistung treten, befürchten Zahlungsausfälle. Um sich davor zu schützen, bedienen sie sich der Bonitätsinformationen, die Auskunfteien oder Warndienste

anbieten. Die häufigsten Fragen dazu sollen im Folgenden beantwortet werden.

Was machen Auskunfteien? Auskunfteien sind private Unternehmen, die Bonitätsinformationen sammeln und gegen Entgelt an anfragende Stellen schriftlich, telefonisch oder online weitergeben. Verbraucherauskunfteien wie die SCHUFA, arvato infoscore oder die CEG speichern Bonitätsinformationen zu Privatpersonen. Handels- und Wirtschaftsauskunfteien wie die Vereine Creditreform oder Bürgel arbeiten mit Informationen über die wirtschaftliche Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit von Unternehmen, gewerblich tätigen Personen und zunehmend auch Privatpersonen. Darüber hinaus bieten branchenspezifische Warndienste wie Mieterwarndateien ihre Dienste an (siehe hierzu Bericht 2007 unter 7.6).

Auf welcher Rechtsgrundlage arbeiten Auskunfteien? Da es kein spezielles Gesetz für die Datenverarbeitung durch Auskunfteien und Warndateien gibt, richtet sich die Zulässigkeit des Datenaustausches insbesondere nach dem Bundesdatenschutzgesetz (BDSG) und dort vor allem nach dessen §§ 28 und 29. Da diese Normen bislang sehr allgemein gehalten sind – eventuell wird der Gesetzgeber daran künftig etwas ändern – bedarf es hier regelmäßig der Abwägung zwischen den finanziellen Sicherungsinteressen der Unternehmen einerseits und der informationellen Selbstbestimmung und den wirtschaftlichen Interessen der betroffenen Personen andererseits. Daraus haben sich in der Praxis der Aufsichtsbehörden die folgenden Regeln für den Datenaustausch der beteiligten Akteure ergeben.

Welche Daten dürfen Auskunfteien erheben und verwenden?

- **Identifikationsdaten** (Name, Anschrift, Geburtsdatum, Voranschriften), um Namens- und Personenverwechslungen zu vermeiden.
- **Negativdaten**, also Informationen zu negativen Zahlungserfahrungen. Mit Blick auf die Zulässigkeit wird zwischen harten und weichen Negativdaten unterschieden. Harte Negativdaten sind Informationen zu titulierten Forderungen aus Vollstreckungsbescheiden oder Urteilen, Angaben aus öffentlichen Schuldnerverzeichnissen wie eidesstattliche Versicherungen oder Angaben zu Verbraucherinsolvenzverfahren. Weiche Negativdaten umfassen im Gegensatz dazu Informationen zu

nicht titulierten, unstrittigen Forderungen, etwa Angaben zu Inkassoverfahren oder offenen Salden.

Grundsätzlich dürfen nur solche Negativdaten zum Zahlungsverhalten erhoben und verwendet werden, die eindeutig Rückschlüsse auf Zahlungsunfähigkeit oder -unwilligkeit zulassen. Bei harten Negativdaten ist dies grundsätzlich gegeben, weil sie aus rechtsstaatlichen Verfahren mit Mitwirkungsrechten der Betroffenen stammen. Anders ist das bei weichen Negativdaten. Hier bedarf es zusätzlicher Voraussetzungen, damit nur gesicherte Informationen über das Zahlungsverhalten in die Auskunft einfließen: Die entsprechenden Forderungen müssen erfolglos gemahnt und unbestritten sein. Zudem müssen die Betroffenen rechtzeitig vorab über die beabsichtigte Einmeldung bei der Auskunftei informiert werden, um etwaige Einreden oder Gegendarstellungen vortragen zu können.

- **Positivdaten:** Das sind Daten, die keine negativen Zahlungserfahrungen beschreiben, aber bonitätsrelevant sind, weil sie etwas über die Zahlungsfähigkeit oder -willigkeit aussagen. Häufig handelt es sich um Angaben zum vertragsgemäßen Verhalten der Betroffenen, also Informationen über die Beantragung, Erfüllung und Beendigung einer Geschäftsbeziehung, etwa laufende oder beglichene Kredite, Girokonten oder Kreditkartenverträge. Die Einmeldung dieser Informationen bei einer Auskunftei ist nur mit Einwilligung der Betroffenen nach § 4a BDSG zulässig. Für Bankverträge plant die Bundesregierung indes die Aufnahme einer speziellen Regelung im BDSG, so dass die Erhebung dieser Positivdaten künftig auf gesetzlicher Grundlage, also ohne Einwilligung, erfolgen könnte.

- **Score-Daten:** Das sind statistisch begründete Prognosewerte über das künftige Risiko eines Zahlungsausfalls. Beim Scoring wird die zu bewertende Person mithilfe der bei der Auskunftei gespeicherten Daten automatisiert einer statistisch gebildeten Vergleichsgruppe zugeordnet. Das für die gefundene Vergleichsgruppe in der Vergangenheit festgestellte Ausfallrisiko ergibt dann die Prognose für einen möglicherweise in der Zukunft eintretenden Zahlungsausfall der zu bewertenden Person. Die Prognose wird in einem Zahlenwert – etwa einer Prozentzahl – zusammengefasst, dem so genannten Score-Wert.

Auskunfteien wie die SCHUFA ermitteln jeweils Score-Werte zu unterschiedlichen Vertragstypen und Branchen. Informationen zu den rechtlichen Anforderungen und praktischen Problemen im Zusammenhang mit der Beauskunftung von Score-Daten enthalten die Berichte 2003 unter 8.4.2, 2005 unter 5.7 und 2007 unter 7.1.

An wen dürfen Auskunfteien Daten übermitteln? Nach § 29 Abs. 2 BDSG ist entscheidend, ob die abfragenden Unternehmen im konkreten Fall ein berechtigtes Interesse an den Bonitätsdaten glaubhaft darlegen und gleichzeitig kein schutzwürdiges Interesse der Betroffenen am Ausschluss der Übermittlung besteht. Das berechtigte Interesse liegt nur vor bei bestehenden oder unmittelbar bevorstehenden Vertragsbeziehungen, die für das Unternehmen ein finanzielles Ausfallrisiko mit sich bringen. Sonstige wirtschaftliche Gründe oder Neugier berechtigen nicht zur Abfrage von Bonitätsauskünften. So haben etwa Versicherungen kein finanzielles Ausfallrisiko und damit auch keine Berechtigung bei Vertragsschluss Auskunfteidaten zu erheben, wenn sie bei ausstehender Zahlung der Prämie von der Leistungspflicht befreit sind oder im Leistungsfall mit der ausstehenden Prämie aufrechnen können (mehr zum Thema Versicherungen und Auskunfteien im Bericht 2007 unter 7.4).

Um entsprechende Kontrollen der Abfrageberechtigung zu ermöglichen, sind die abfragende Stelle und das vorgebrachte berechtigte Interesse zu dokumentieren.

Schutzwürdige Interessen der Betroffenen am Ausschluss der Übermittlung der Daten bestehen, wenn die entsprechenden Daten keine gesicherten Auskünfte über die Zahlungsfähigkeit- oder -willigkeit der jeweiligen Person zulassen. Das führt insbesondere zu den oben dargestellten Anforderungen an die Erhebung und Verwendung weicher Negativdaten. Zudem kann für Abfragen bestimmter Branchen, etwa der Wohnungswirtschaft, nur die Übermittlung eines eingeschränkten Katalogs von Datenkategorien zulässig sein (siehe Bericht 2007 unter 7.6).

Welche Informationspflichten haben die Auskunfteien und die abfragenden Unternehmen? Das abfragende Unternehmen hat die betroffene Person gemäß § 4 Abs. 3 BDSG vorab – bei der Erhebung der für die Abfrage erforderlichen Identifikationsdaten – darüber zu

unterrichten, dass es ihre Daten auch zum Zweck der Auskunfteiabfrage verwenden will. Soweit die Auskunftei Daten ohne Kenntnis der Person speichert, hat sie diese gemäß § 33 BDSG von der erstmaligen Übermittlung und der Art der übermittelten Daten zu unterrichten – es sei denn die Person hat auf andere Weise Kenntnis von der Übermittlung erlangt, etwa durch eine SCHUFA-Klausel.

Welche Auskunftsansprüche haben die Betroffenen? Nach § 34 BDSG hat jede Person das Recht zu erfahren, welche Daten eine Auskunftei über sie gespeichert hat. Grundsätzlich müssen die Auskunfteien dabei auch mitteilen, woher die Daten stammen und an wen sie weitergegeben wurden. Da Auskunfteien wie die SCHUFA die an Unternehmen übermittelten Score-Werte nicht speichern, geht der Auskunftsanspruch hierzu bislang ins Leere (stattdessen werden gegen Entgelt tagesaktuelle Score-Werte angeboten). Der Gesetzgeber plant indes eine Änderung, um künftig auch zu den Score-Werten eine effektive Auskunftsgewährung sicherzustellen.

Um missbräuchliche "Selbst"-Auskünfte durch Unberechtigte zu verhindern, dürfen Auskunfteien zur Identitätsprüfung bei schriftlichen Anträgen auf Auskunftsgewährung eine Kopie des Ausweises anfordern (mehr dazu im Bericht 2003 unter 8.1).

Dürfen die Auskunfteien für die Erteilung der Selbstauskunft ein Entgelt verlangen? Ja, anders als sonstige Stellen dürfen Auskunfteien ein Entgelt verlangen, wenn die Person die Daten gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Dies ist bei schriftlichen Auskünften regelmäßig der Fall. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Die Entgeltpflicht besteht nicht, wenn besondere Gründe die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden oder sich dies nachträglich durch die Auskunft ergibt. Darüber hinaus muss die Auskunftei die Möglichkeit einräumen, die Daten unentgeltlich vor Ort einzusehen. Im Übrigen beabsichtigt der Gesetzgeber eine Änderung des BDSG dahingehend, dass jede Person künftig einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen kann.

Was tun, wenn die Auskunftei unzutreffende Daten speichert? Falls die Selbstauskunft ergibt, dass unrichtige oder bestrittene Daten gespeichert sind, können die Betroffenen ihre Rechte auf Löschung,

Sperrung oder Berichtigung geltend machen. Unrichtige Daten sind zu berichtigen oder zu löschen. Wird die Richtigkeit der Daten bestritten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten gemäß § 35 Abs. 4 BDSG zu sperren (mehr dazu im Bericht 2003 unter 8.4.3).

Gibt es allgemeine Löschungsfristen? Die Löschung der Daten richtet sich bei Auskunfteien insbesondere nach § 35 Abs. 2 Nr. 4 BDSG und § 915a der Zivilprozessordnung (ZPO). Nach der Regelung im BDSG hat die Auskunftei am Ende des vierten Kalenderjahres beginnend mit der erstmaligen Speicherung der Daten zu prüfen, ob eine weitere Speicherung erforderlich ist. Ist die ausstehende Forderung inzwischen erledigt und kein weiterer Negativeintrag erfolgt, sind die Daten zu löschen. Abweichend davon löscht die SCHUFA Negativdaten drei Jahre nach ihrer Erledigung. Dies gilt auch für die Löschung von Informationen zu Privatinsolvenzen. Die Erteilung der Restschuldbefreiung gilt als der Zeitpunkt, an dem die Frist zu laufen beginnt.

Daten aus dem Schuldnerverzeichnis müssen Auskunfteien gemäß § 915a ZPO bereits drei Jahre nach Ende des Jahres der Eintragung im Schuldnerverzeichnis löschen. Sofern eine Eintragung im Schuldnerverzeichnis vorzeitig gelöscht wird, sind auch die Auskunfteien zur vorzeitigen Löschung dieser Daten verpflichtet.

Wer hilft bei datenschutzrechtlichen Problemen mit Auskunfteien? Bei Berichtigungs-, Sperrungs- oder Löschungsansprüchen oder sonstigen datenschutzrechtlichen Fragen können sich die Betroffenen an die betrieblichen Datenschutzbeauftragten der jeweiligen Auskunftei wenden. Die SCHUFA hat darüber hinaus eine Vertrauensperson eingesetzt, die unternehmensintern als Schiedsstelle dient.

Selbstverständlich besteht auch die Möglichkeit, sich direkt an die datenschutzrechtlichen Aufsichtsbehörden zu wenden. Insoweit ist die Aufsichtsbehörde des jeweiligen Bundeslandes zuständig, in dem die Auskunftei ihren Sitz hat, also etwa das Regierungspräsidium Darmstadt für die SCHUFA, das Innenministerium Baden-Württemberg für die arvato infoscore und die LDI NRW für die CEG.

➡ Zwischen den finanziellen Sicherungsinteressen der Unternehmen einerseits und der informationellen Selbstbestimmung sowie den wirtschaftlichen Interessen der Betroffenen andererseits besteht ein unver-

meidbares Spannungsfeld, in dem Auskunfteien und Warndienste mit eigenen Geschäftsideen und Interessen agieren. Die Datenschutzbehörden werden – hoffentlich mit Unterstützung des Gesetzgebers – weiterhin auf datenschutzgerechte Verfahren und Konfliktlösungen hinwirken.

6.4 Ich weiß, wie Du wohnst

Sie wurden schon in verschiedensten Ecken in Deutschland gesichtet – die schwarzen Autos der Firma Google mit einer Kamera auf dem Dach. Sie fahren die Straßen deutscher Städte ab und fertigen dabei 360°-Aufnahmen von Häusern und Grundstücken an. Google will die Aufnahmen mit der Funktion Google Maps verknüpfen. Sucht jemand eine Adresse, soll künftig nicht nur die Lage des Hauses in einer Landkarte oder in einem Luftbild dargestellt werden, sondern zusätzlich soll ein Bild der Gebäudefassade frei im Internet verfügbar sein.

Die Datenschutzaufsichtsbehörden verfolgen die Aktivitäten von Google und die Bildaufnahmen für die Funktion "Street View" sehr aufmerksam. Problematisch ist zum einen, dass zufällig anwesende Personen mit fotografiert werden. Google hat jedoch angekündigt, Gesichter von Passanten und Autokennzeichen unkenntlich zu machen, bevor die Bilder veröffentlicht werden.

Ein weiteres Problem besteht darin, dass Bilder von Häuserfassaden unter Umständen einzelnen Personen zugeordnet werden können. Dies kann beispielsweise der Fall sein, wenn Hausnummern mit fotografiert werden oder wenn anhand von Geokoordinaten oder mit Hilfe anderer Quellen den Häuserfassaden Adressen zugeordnet werden können. Sind wiederum die Adressen von Bewohnerinnen und Bewohnern oder Hauseigentümerinnen und -eigentümern bekannt, können auch die Aufnahmen der Häuserfassaden personenbezogene Daten sein. Es ist daher verständlich, dass zahlreiche Bürgerinnen und Bürger Bedenken haben, wenn Google Straßenaufnahmen anfertigt, da diese im Internet veröffentlicht werden sollen und somit weltweit einsehbar wären.

Der Düsseldorfer Kreis – das Gremium der obersten Datenschutzaufsichtsbehörden des Bundes und der Länder im nicht-öffentlichen Bereich – hat in seiner Sitzung am 13./14. November 2008 einen Be-

schluss "Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet" gefasst (Abdruck im Anhang). Der Düsseldorfer Kreis vertritt die Ansicht, dass Gesichter, Kraftfahrzeugkennzeichen und Hausnummern unkenntlich gemacht werden müssen. Zudem muss es den betroffenen Eigentümerinnen und Eigentümern sowie den Mietparteien eines Hauses möglich sein, der Veröffentlichung ihrer Gebäudefassade im Internet zu widersprechen. Um eine frühzeitige Möglichkeit zum Widerspruch zu eröffnen, soll die beabsichtigte Datenerhebung vor Ort mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig bekannt gegeben werden.

Für Widersprüche im Zusammenhang mit dem Projekt Google Street View sollten sich die Betroffenen direkt an die Google Germany GmbH in Hamburg wenden. Zuständige Aufsichtsbehörde für Datenerhebungen und –verwendungen der Google Germany GmbH ist der Hamburgische Datenschutzbeauftragte.

➡ Die datenschutzrechtliche Bewertung des Düsseldorfer Kreises von digitalen Straßenansichten bezieht sich selbstverständlich nicht nur auf Google Street View, sondern auch auf ähnliche Projekte anderer Unternehmen.

6.5 Ungewollter Kredit

Immer mehr Banken bieten Kredite über das Internet an – "sofort, einfach und günstig". Aber woher weiß die Bank, wer bei ihr online einen Kredit nachfragt und entsprechende Angaben in die Antragsformulare eingibt? Wird die Identität der Online–Kundschaft nicht überprüft, besteht die Gefahr, dass sich jemand unter falschem Namen für einen Kredit interessiert und so Informationen über die Bonität einer anderen Person erhält.

"Wir bedauern Ihnen mitteilen zu müssen, dass wir Ihrem Antrag auf einen Ratenkredit in Höhe von 14.000 Euro nicht entsprechen können." Eine Berliner Bürgerin staunte nicht schlecht, als sie diese Zeilen einer Bank aus Nordrhein-Westfalen in ihrem Briefkasten fand. Dabei hatte sie nie einen Kredit angefragt.

Unter dem Namen der Berlinerin hatte eine andere Person online einen Kreditantrag gestellt. Dazu benötigte diese nicht viel mehr als die An-

gaben zu Name, Adresse und Geburtsdatum. Die Bank versuchte dann eine SCHUFA-Auskunft zu erlangen. Da allerdings das Geburtsdatum nicht stimmte, konnte die SCHUFA in diesem Fall keinen Datensatz zuordnen. Dies war wohl einer der Gründe, warum die Bank dem Kreditantrag nicht entsprach.

Das Ergebnis seiner Prüfung teilte das Kreditinstitut der Berlinerin auf dem Postwege mit. Dadurch erfuhr sie überhaupt nur, dass jemand unter ihrem Namen einen Kreditantrag gestellt hatte. Auch im Falle einer Kreditzusage wechselt die Bank vom Medium Internet oder E-Mail zur Briefpost. Schicken die Kundinnen oder Kunden den Kreditvertrag unterschrieben an die Bank zurück, müssen sie sich in einer Postfiliale mittels Post-Ident-Verfahren legitimieren. Dabei überprüft die Post die Identität der Betroffenen anhand eines amtlichen Ausweises und einer Unterschrift, bevor die Unterlagen mit einem entsprechenden Vermerk an die Bank geschickt werden.

Dieser Fall zeigt, dass bei Online-Krediten die Gefahr des Missbrauchs besteht. Eine Überprüfung der Identität ist in jedem Fall erforderlich. Es muss sichergestellt sein, dass die Bank erst nach einer Identitätsprüfung Angaben macht, die Rückschlüsse auf die Bonität einer Person zulassen.

Bei Online-Kreditanträgen stellt sich zudem die Frage, ob eine wirksame Einwilligung zur Einholung einer SCHUFA-Auskunft und zur Befreiung vom Bankgeheimnis vorliegt. Denn diese Einwilligungen müssen grundsätzlich schriftlich erteilt werden. Eine online abgegebene Erklärung genügt grundsätzlich nicht. Nach dem Bundesdatenschutzgesetz kann jedoch auf die Schriftform verzichtet werden, soweit wegen besonderer Umstände eine andere Form angemessen ist. Hier kann bei Kreditanträgen eine Ausnahme von der Schriftform gemacht werden – allerdings nur, wenn die Tatsache der Anfrage bei der SCHUFA weder in die Score-Berechnung einfließt noch von der SCHUFA an andere Unternehmen übermittelt wird (siehe hierzu unter 6.3).

➡ Allzu schnell und einfach können auch online keine Kreditverträge abgeschlossen werden. Die Banken müssen sicherstellen, dass Angaben zur Bonität einer Person nicht in falsche Hände geraten.

6.6 Kundendaten im Teleshop – Umsetzung datenschutzrechtlicher Unterrichtungspflichten

Teleshops bieten in speziellen Einkaufssendungen im Fernsehen Waren zum Kauf an. Interessierte können die dort angebotenen Waren telefonisch unter einer eingeblendeten Rufnummer oder über die Internetseite des Teleshops bestellen. Bei dieser besonderen Form des Einkaufs werden Daten erhoben, deren weitere Verwendung für die Kundinnen und Kunden frühzeitig transparent sein muss.

Ein Unternehmen aus Nordrhein-Westfalen betreibt einen Teleshop und erhebt bei der Bestellung von Waren zahlreiche personenbezogene Daten. Das Unternehmen ist daher verpflichtet, seine Kundinnen und Kunden bereits zum Zeitpunkt der Erhebung der Daten über die bevorstehende Datenverarbeitung und ihre Zwecke zu unterrichten.

Regelmäßig erfolgt eine Information zum Datenschutz, insbesondere über die Verwendung der Adressdaten für Zwecke der Werbung und der Markt- und Meinungsforschung, in den Allgemeinen Geschäftsbedingungen des jeweiligen Teleshops. Diese erhalten die Kundinnen und Kunden im Normalfall mit der Rechnung. Sie haben in der Regel auch die Möglichkeit, diese Klauseln auf der Internetseite des Teleshops oder auf einer entsprechenden Videotextseite zur Einkaufssendung einzusehen. Hiermit kommt der Teleshop seiner datenschutzrechtlichen Unterrichtungspflicht im Grunde nach.

Die Besonderheit beim Einkauf im Teleshop besteht jedoch darin, dass die Kundinnen und Kunden, die eine telefonische Bestellung und damit ihre persönlichen Daten während einer Einkaufssendung abgeben, gerade keinen rechtzeitigen Hinweis auf die Fundstellen zu den Allgemeinen Geschäftsbedingungen und den Datenschutzklauseln erhalten. Damit haben sie keine Möglichkeit, die von dem Unternehmen erteilte datenschutzrechtliche Unterrichtung rechtzeitig zur Kenntnis zu nehmen. In diesen Fällen erhalten die Betroffenen die Informationen erst mit der Rechnung, also lange nach Erhebung ihrer Daten.

Um die gesetzlich geforderte Transparenz zum Zeitpunkt der Datenerhebung zu schaffen, blendet der Teleshop aus Nordrhein-Westfalen nun in seiner Einkaufssendung regelmäßig Hinweise auf die Allgemeinen Geschäftsbedingungen und Datenschutzklauseln im Videotext so-

wie auf der Internetseite ein. Damit ist eine frühzeitige, datenschutzgerechte Unterrichtung der Kundinnen und Kunden gewährleistet.

➡ Mit einem deutlichen Hinweis in der Einkaufssendung auf die Fundstellen der Datenschutzerklärung kommt ein Teleshop den gesetzlichen Unterrichtungspflichten gegenüber seinen Kundinnen und Kunden nach.

6.7 Verbrauchsorientierte Energieausweise

Vermieten Sie Wohnungen und wollen Sie einen verbrauchsorientierten Energieausweis erstellen lassen? Benötigen Sie hierzu die Angaben Ihrer Mieterinnen und Mieter über deren Verbrauch von Strom und Gas in den letzten drei Jahren? Folgende Möglichkeiten gibt es, diese Angaben, bei denen es sich um personenbezogene Daten handelt, zu erlangen.

Zunächst können Sie natürlich darum bitten, dass Ihnen Ihre Mieterinnen und Mieter die Angaben anhand ihrer Unterlagen zur Verfügung stellen. Des Weiteren können Sie sie um eine Einwilligung bitten, die das Versorgungsunternehmen ermächtigt, Ihnen gegenüber entsprechende Angaben zu machen.

Ohne eine solche Einwilligung darf das Versorgungsunternehmen nur anonymisierte Daten übermitteln. Die Datenschutzaufsichtsbehörden in Deutschland sind einhellig der Auffassung, dass Verbrauchswerte dann keine personenbezogene Daten sind, wenn sie für mindestens drei Mietparteien eines Gebäudes als anonymisierte aggregierte Durchschnittswerte übermittelt werden.

Können Sie auf diesen Wegen die erforderlichen Angaben über den Energieverbrauch nicht erlangen, verbleibt nur die Möglichkeit, einen bedarfsorientierten Energieausweis zu erstellen.

Ausführliche Hinweise finden sich im Internet unter www.ldi.nrw.de.

➡ Wenn mindestens drei Mietparteien betroffen sind, gibt es eine pragmatische Lösung, indem ein Durchschnittswert gebildet werden kann. Im Übrigen wäre es wünschenswert gewesen, wenn der Gesetz- und Verordnungsgeber bei Einführung des Energieausweises

eine Rechtsgrundlage für die Übermittlung von Verbrauchsdaten geschaffen hätte.

6.8 Smart Metering – Energie sparen durch Datensammeln?

So genannte intelligente Stromzähler (smart meters) sind aus der Ferne auslesbar und können umfangreiche und aktuelle Daten über den Energieverbrauch liefern. Die modernen Zähler sollen künftig vor allem die Transparenz des Stromverbrauchs erhöhen und so das energiesparende Verhalten der Verbraucherinnen und Verbraucher fördern. Doch wie sieht es mit dem Datenschutz aus?

Mit der im September 2008 in Kraft getretenen Novellierung des Energiewirtschaftsgesetzes soll ab 2010 das energiesparende Verhalten der Verbraucherinnen und Verbraucher unterstützt werden. Vorgesehen sind unter anderem technische Innovationen beim Zähl- und Messwesen (intelligente Stromzähler), die verbindliche Einführung von "lastvariablen" oder tageszeitabhängigen Tarifen sowie die Verpflichtung, auf Wunsch der Verbraucherinnen und Verbraucher auch monatliche Abrechnungen des Energieverbrauchs zu ermöglichen.

Um den flächendeckenden Einsatz der neuen Zählertechnik zu erproben, hat ein nordrhein-westfälisches Unternehmen in Mülheim an der Ruhr ein flächendeckendes Pilotprojekt gestartet. Damit das Unternehmen nicht nur technisch, sondern auch datenschutzrechtlich auf der sicheren Seite ist, bat es vorab um eine Bewertung des vorgesehenen Verfahrens.

In dem Mülheimer Pilotprojekt ändern sich mit dem schrittweise erfolgenden Austausch der alten Stromzähler durch die so genannten intelligenten Stromzähler weder die Datenwege noch die Kategorien der übermittelten Kundendaten. Der einzige Unterschied zum aktuellen Status quo besteht darin, dass die Zählerstände nicht mehr standardmäßig einmal im Jahr abgelesen, sondern monatlich übermittelt und im erforderlichen Umfang weiterverarbeitet werden. Da keine tägliche, stündliche oder gar viertelstündliche Erhebung erfolgt, werden keine Verbrauchsprofile gebildet, die ein schutzwürdiges Interesse der Kundinnen und Kunden an dem Ausschluss der geplanten Datenver-

wendungen begründen würden. Daher ist eine flächendeckende Erprobung im gesamten Stadtgebiet unabhängig von der Zustimmung der einzelnen Verbraucherinnen und Verbraucher möglich.

In einem weiteren Pilotprojekt in einer anderen nordrhein-westfälischen Stadt, an dem die Kundinnen und Kunden freiwillig teilnehmen können, sollen die Zählerstände viertelstündlich erhoben werden. Da detaillierte Verbrauchsprofile entstehen, ist dies nur mit schriftlicher Einwilligung der teilnehmenden Personen möglich. Damit die jederzeit widerrufbaren Einwilligungen wirksam sind, müssen insbesondere die geplanten Erhebungen, Verarbeitungen und Nutzungen der Daten sowie die damit verbunden Zwecke für die Teilnehmenden durch entsprechende Informationen transparent sein.

Aus datenschutztechnischer Sicht ist beim Einsatz der fernauslesbaren Zähler darauf zu achten, dass die Übertragung der Daten durch Verschlüsselung hinreichend geschützt ist. Außerdem sind die Datenbanken der verantwortlichen Stellen so zu organisieren, dass die zahlreichen am Stromnetz, an der Stromversorgung und am Messbetrieb beteiligten Unternehmen keinen freien Zugriff auf die Zählerstände der Kundinnen und Kunden haben, sondern diese nur im erforderlichen Umfang erhalten.

➡ Die Erprobung der neuen Generation von Stromzählern ist mit dem Datenschutzrecht vereinbar, soweit die dargestellten Vorgaben beachtet werden. Um die Akzeptanz bei den Verbraucherinnen und Verbrauchern zu erhöhen, sollte – unabhängig vom Erfordernis einer Einwilligung oder Unterrichtung der Betroffenen – nicht nur Transparenz über den Stromverbrauch, sondern auch über die beabsichtigten Datenverarbeitungen und ihre Zwecke geschaffen werden.

7 Polizei

7.1 DNA-Analyse-Datei: In der Masse steckt die Klasse?

Der Datenbestand der DNA-Analyse-Datei ist weiter stark angeschwollen: Drei Jahre nach der Neuregelung waren darin bundesweit bereits im Dezember 2008 fast 750.000 DNA-Identifizierungsmuster gespeichert. Die Rechtsänderung von November 2005 und der mit ihr einhergehende starke Anstieg der Einträge waren Anlass für Kontrollen bei verschiedenen Polizeibehörden des Landes.

Die Änderung der Strafprozessordnung, mit der die Voraussetzungen für die Speicherung in der DNA-Analyse-Datei aufgeweicht und die Einwilligungslösung eingeführt wurde, ist von den Datenschutzbeauftragten des Bundes und der Länder sehr kritisch betrachtet worden (siehe im Bericht 2007 unter 10.1 sowie die Entschließung vom 15. Februar 2005 in dessen Anhang). Seit die Einholung einer richterlichen Anordnung nicht mehr zwingend vorgeschrieben ist, ist die Entnahme und Untersuchung von DNA-Proben Verdächtiger auf Grundlage ihrer Einwilligung nun leider der Regelfall geworden. Zwar besteht theoretisch Einigkeit darüber, dass das Vorliegen der gesetzlichen Speichervoraussetzungen von den Ermittlungsbehörden geprüft und bejaht worden sein muss, bevor die Betroffenen um ihre Einwilligung in die DNA-Analyse gebeten werden. Praktisch aber sind die einzelnen Polizeibeamtinnen und –beamten vor Ort mit der Anwendung dieser konturlos gewordenen Norm allein gelassen, deren Regelungsgehalt erst recht für die betroffenen Personen selbst kaum zu durchschauen ist.

Kontrollen bei vier Polizeibehörden (zwei Polizeipräsidien in Großstädten und zwei Kreispolizeibehörden in ländlich geprägten Gebieten) haben daher erwartungsgemäß gezeigt, dass ein erheblicher Anteil der von den DNA-Analysen betroffenen Personen zu Unrecht in der Datei gespeichert ist. Abgesehen von einigen im Graubereich der unklaren gesetzgeberischen Vorgaben liegenden Zweifelsfällen waren 10% der 126 geprüften Einspeicherungen im Ergebnis wieder aus der DNA-Datei herauszunehmen. In einer Behörde mussten gar 20% der überprüften Datensätze gelöscht werden.

Die Gründe hierfür liegen zum Teil in der unklaren gesetzlichen Regelung, die das einigermaßen bestimmbare Merkmal der erheblichen Straftat durch eine Wertentscheidung im Einzelfall ersetzt hat. Um diese Wertentscheidung zu treffen, muss der Unrechtsgehalt von Straftaten anhand aller maßgeblichen Umstände abgewogen und bestimmt werden. Hierzu gehört neben der Rechtsgutsverletzung und der mit ihr zum Ausdruck gekommenen rechtsfeindlichen Gesinnung auch der Grad der Störung des Rechtsfriedens und der Beeinträchtigung des Gefühls der Rechtssicherheit der Allgemeinheit. Ferner setzt die Speicherung die Prognose voraus, dass die verdächtige Person auch zukünftig Straftaten mit erheblichem Unrechtsgehalt begehen wird. Hierbei müssen ebenfalls alle Umstände einschließlich Art und Ausführung der Tat, Persönlichkeit und Lebenssituation der Beschuldigten und "sonstige Erkenntnisse" festgestellt und bewertet werden.

Für diese schwierige rechtliche Prüfung wurden weder landesweite inhaltliche Vorgaben entwickelt noch eine allgemeine Pflicht zur Dokumentation der Entscheidungsfindung vorgesehen. Angesichts dessen ist es kaum verwunderlich, dass die Überprüfung von 126 aufgrund von Einwilligungen vorgenommenen Speicherungen in vier verschiedenen Polizeibehörden ergeben hat, dass die Dokumentationspraxis von Behörde zu Behörde so unterschiedlich ist, wie die bei der Entscheidung angewandten Maßstäbe und Kriterien. Die fehlende Dokumentation der Prüfung bedeutet nicht nur einen höheren Aufwand bei der nachträglichen Kontrolle, sondern auch, dass das Gedächtnis der damals zuständigen Sachbearbeiterinnen oder Sachbearbeiter die einzige Informationsquelle für das Vorliegen der gesetzlichen Voraussetzungen zum Zeitpunkt der Einholung der Einwilligung ist. Ein Umstand, der mit zunehmender zeitlicher Distanz zu den Einspeicherungen, deren Dauer ja nicht von vorneherein befristet ist, immer problematischer wird.

Die vorherrschende Rechtsunsicherheit und die teils wenig aussagekräftige Aktenlage führten dazu, dass im Verlauf des Kontrollprojekts in einigen Fällen lieber gelöscht wurde, als eine tragfähige Begründung für die Speicherung nachzuliefern.

Insgesamt kann dies kein dauerhafter Zustand sein. Hier muss vom Innenministerium NRW gegengesteuert werden, indem die Dokumentation der Prüfvoraussetzungen angeordnet und im übrigen versucht wird, landesweit gültige Bewertungsmaßstäbe vorzugeben, so dass die Zahl ungerechtfertigter Speicherungen reduziert und sowohl

für die Betroffenen als auch für die Polizei mehr Rechtssicherheit geschaffen wird.

- Die Anwendung der Einwilligungslösung bei der Einspeicherung von Verdächtigen in die DNA-Analyse-Datei setzt das Prüfniveau erheblich herab und führt zu unrechtmäßigen Speicherungen in nicht geringer Zahl. Hier muss durch organisatorische Maßnahmen wie die Einführung einer Dokumentationspflicht und weitere Anwendungshilfen massiv gegengesteuert werden.

7.2 Die Polizei als Reiseveranstalter – sichere Anreise nach Heiligendamm

Der Ortsverband einer Partei, der Mitfahrgelegenheiten nach Heiligendamm zu den Veranstaltungen anlässlich des G 8-Gipfels organisierte, staunte nicht schlecht, als er in diesem Zusammenhang Anrufe der Polizei erhielt.

Die polizeiliche Kontaktaufnahme erfolgte zu dem Zweck, die Anzahl der Interessierten sowie deren Namen, Telefonnummern, Alter und verwendete Fahrzeuge in Erfahrung zu bringen. Die Polizeibehörde begründete die Vorgehensweise damit, dass die Polizei aufgrund des sich aus dem Brokdorf-Beschluss des Bundesverfassungsgerichts vom 14. Mai 1985 (1 BvR 233/81) ergebenden polizeilichen Auftrags zur Deeskalation und Kooperation sowie zur Differenzierung zwischen friedlichen und gewaltorientierten Versammlungsteilnehmerinnen und -teilnehmern gehalten sei, nicht nur den Schutz der Versammlung, sondern auch schon die reibungslose Anreise der friedlichen Teilnehmerinnen und Teilnehmer an den Versammlungsort zu gewährleisten. Rechtsgrundlage für die Datenerhebung sei das polizeiliche Befragungsrecht gewesen. Der Verweis auf den Brokdorf-Beschluss des Bundesverfassungsgerichts ist in diesem Zusammenhang allerdings fast ein Witz. Der Beschluss bezieht sich in seinen Ausführungen (Leitsatz 3) auf das Verhältnis zwischen den Veranstalterinnen und Veranstaltern von Großdemonstrationen und den für die Gewährleistung eines friedlichen Veranstaltungsverlaufs zuständigen staatlichen Sicherheitsbehörden. Von einer staatlichen Verpflichtung zur Gewährleistung einer "friedlichen Anreise" von einzelnen Teilnehmerinnen und Teilnehmern der Großveranstaltung ist jedoch an

keiner Stelle die Rede. Im Ergebnis stellte sich letztlich heraus, dass es in dem konkreten Fall nicht zu Datenerhebungen und -speicherungen gekommen war. Dies allerdings nur, weil die Abreise von Standorten außerhalb des örtlichen Zuständigkeitsbereiches der betreffenden Polizeidienststelle erfolgte.

Wegen der grundsätzlichen Bedeutung der Angelegenheit wurde jedoch das Innenministerium NRW auf Folgendes hingewiesen: Das polizeiliche Befragungsrecht gibt kein pauschales Recht zur Datenerhebung. Eine Erhebung personenbezogener Daten zu unbestimmten oder noch nicht bestimmten Zwecken ist unzulässig. Eine Datenerhebung über nicht gefahren- oder tatbezogene Merkmale ist nur zulässig, soweit dies für Identifizierungszwecke oder zum Schutz der betroffenen Personen erforderlich ist. Die Vorschrift ermächtigt aber gerade nicht zu einer Datenerhebung auf Vorrat, die darauf gerichtet ist, pauschal personenbezogene Daten für den Fall zu erheben, zu speichern und auszuwerten, dass es sich vielleicht herausstellen könnte, dass die betreffenden Personen Verbindungen in das Milieu gewaltbereiter Demonstrantinnen und Demonstranten haben könnten.

➡ Die Polizei darf – auch bei anstehenden Großdemonstrationen – Daten über teilnehmende Personen nicht ohne Anlass und im Voraus erheben.

7.3 rsCase: Datenschutz in allen Fällen

In besonders umfangreichen und komplexen Strafverfahren ist die von den Ermittlungsbehörden zu verarbeitende Flut von Hinweisen und Informationen oft kaum zu bewältigen. Bei der Lösung dieses Problems soll der nordrhein-westfälischen Polizei nun das neue Programm rsCase helfen, das in unterschiedlichen Versionen auch bereits von den Polizeibehörden einiger anderer Länder eingesetzt wird.

In Großverfahren beinhaltet die Ermittlungsakte der Polizei meist unzählige Ordner mit chronologisch abgehefteten Berichten, Vermerken, Protokollen und weiteren Unterlagen. Diese bergen eine für die einzelnen Sachbearbeiterinnen und Sachbearbeiter praktisch nicht mehr überschaubare Informationsfülle. Das neue Programm rsCase soll dazu dienen**,** die polizeilichen Erkenntnisse zu strukturieren und so mitein-

ander zu verknüpfen, dass Bezüge zwischen handelnden Personen aufgezeigt und Handlungsmuster sichtbar werden. Mit dem Programm sollen grundsätzlich alle in dem betreffenden Ermittlungsverfahren erhobenen Daten und Informationen verarbeitet werden, auch etwa solche, die durch Telekommunikationsüberwachung oder andere verdeckte Ermittlungsmaßnahmen gewonnen wurden.

Abgesehen von einzelnen kleineren Mängeln, die im Austausch mit dem Innenministerium NRW bereits weitgehend behobenen wurden, ist das Verfahren nach den der LDI NRW vorliegenden Unterlagen datenschutzrechtlich grundsätzlich nicht bedenklich. Es muss allerdings gewährleistet werden, dass auch im Rahmen der Anwendung dieser Software die strafprozessualen Anforderungen an die Speicherung und Nutzung der erhobenen Daten erfüllt werden. Insbesondere müssen die gesetzlichen Kennzeichnungspflichten für Daten, die aufgrund besonders intensiver Grundrechtseingriffe gewonnen wurden, auch bei elektronischer Speicherung eingehalten werden. Die Kennzeichnung ist auch dann aufrechtzuerhalten, wenn die Informationen aus den besonderen Ermittlungsmaßnahmen mit Informationen aus anderen Quellen vermischt werden. Denn durch die Kennzeichnung soll sichergestellt werden, dass die jeweiligen Verwendungsbeschränkungen für diese Daten eingehalten werden.

Da eine automatisierte Kennzeichnung offenbar derzeit technisch nicht umgesetzt werden kann, vom Gesetzgeber aber auch nicht gefordert ist, wurde dem Innenministerium NRW vorgeschlagen, durch eine Dienstanweisung für die händische Kennzeichnung der Daten zu sorgen.

➧ Nicht nur die Staatsanwaltschaft, auch die Polizei muss, wenn sie als Ermittlungsbehörde Daten verarbeitet, die Vorgaben der Strafprozessordnung einhalten. Hierzu gehört auch die Pflicht, die durch bestimmte, besonders grundrechtsintensive Ermittlungsmaßnahmen erhobenen Daten entsprechend zu kennzeichnen.

7.4 "Russenmafia" überall?

Wie einfach es ist, aufgrund der aktuellen oder früheren Staatsangehörigkeit ins polizeiliche Fadenkreuz zu geraten, ließ sich anhand eines polizeilichen Auswertungsprojektes zur Erforschung der "Russischen Kriminalität und ihrer Strukturen" feststellen.

Eine Meldebehörde sah sich mit dem polizeilichen Wunsch nach den Meldedaten aller Einwohnerinnen und Einwohner konfrontiert, auf die das Kriterium "früherer Wohnsitz Sowjetunion" zutraf. Gemeldet werden sollten in diesem Zusammenhang auch Personen, die mittlerweile über die deutsche Staatsangehörigkeit verfügten sowie solche, die von Amts wegen als "nach unbekannt abgemeldet" erfasst waren. Die polizeiliche Datenanforderung sollte der Analyse von Strukturen der Organisierten Kriminalität (OK) von Personen mit russischer Staatsangehörigkeit beziehungsweise russischem Migrationshintergrund dienen. Für diese Form des "Rasterns" gibt es jedoch keine Rechtsgrundlage: Die Polizei darf im Einzelfall öffentliche Stellen um die Übermittlung von personenbezogenen Daten ersuchen, soweit die Voraussetzungen für eine polizeiliche Datenerhebung vorliegen. Die Polizeibehörde verwies hier insofern auf ihr polizeiliches Befragungsrecht. Ein Vergleich der relevanten Vorschriften mit der Bestimmung zur präventiv-polizeilichen Rasterfahndung zeigt jedoch, dass diese Regelungen eine derart umfangreiche Datenerhebung nicht tragen können. Die präventive Rasterfahndung, die einen der geplanten Vorgehensweise vergleichbaren schweren Eingriff in das Persönlichkeitsrecht der betroffenen Personen darstellt und ähnliche Ziele verfolgt, ist an enge gesetzliche Voraussetzungen gebunden, insbesondere an einen Richtervorbehalt. Diese Kriterien wurden hier jedoch gerade nicht erfüllt. Im konkreten Fall sollten auch unbescholtene Bürgerinnen und Bürger allein wegen ihrer ethnischen Herkunft in einer Datensammlung, die dem Zweck der Analyse russischer OK-Strukturen dienen sollte, erfasst werden. Damit ist ein immenses Risiko verbunden, eventuell in den Fokus von Ermittlungsmaßnahmen zu geraten und im Alltag einer Stigmatisierungsgefahr ausgesetzt zu sein.

➡ Das Projekt wurde auf Betreiben der LDI NRW gestoppt und bereits erhobene Daten wurden gelöscht.

8 Justiz

8.1 Die Anstalt weiß, was Du nicht weißt: Über Dich

Gefangene sind gläsern. Umfangreiches Wissen über ihre sozialen Beziehungen, ihre finanziellen Verhältnisse, ihren beruflichen Werdegang, ihre Gesundheit und ihr Vorleben ist in fremder Hand: Die Datenerhebungsbefugnis der Haftanstalt erstreckt sich grundsätzlich über alle Lebensbereiche. Damit nicht genug legt das neue Jugendstrafvollzugsgesetz den Grundstein für eine Zentraldatei aller Häftlinge, auf die landesweit zugegriffen werden kann, deren Inhalt aber gesetzlich nicht definiert ist.

Das Bundesverfassungsgericht hat in seinem Urteil vom 31. Mai 2006 daran erinnert, dass Grundrechtseingriffe gegenüber Gefangenen, die über den Freiheitsentzug als solchen hinausgehen, einer eigenen gesetzlichen Grundlage bedürfen, die die Eingriffsvoraussetzungen in verfassungsgemäßer Weise festlegt. Das Gericht hatte dem Gesetzgeber eine letzte Frist bis zum 31. Dezember 2007 eingeräumt, um die bisher fehlende gesetzliche Regelung für den Jugendstrafvollzug zu treffen.

Durch die Föderalismusreform ist die entsprechende Gesetzgebungskompetenz im September 2006 vom Bund auf die Länder übergegangen und die Landesgesetzgeber mussten ans Werk gehen. Das nordrhein-westfälische Jugendstrafvollzugsgesetz trat pünktlich zum 1. Januar 2008 in Kraft. Hieran wurde die LDI NRW aber nicht frühzeitig, wie im Datenschutzgesetz NRW vorgesehen, sondern erst zeitgleich mit der Anhörung der Interessenverbände beteiligt. Deswegen konnten die zahlreichen datenschutzrechtlichen Probleme, die ein so umfassendes neues Regelungswerk aufwirft, nicht schon im Entwurfsstadium mit dem Justizministerium NRW beraten werden. Datenschutzrechtliche Forderungen und Verbesserungsvorschläge der LDI NRW haben im Ergebnis daher nur in wenigen Detailfragen Eingang in das Gesetz gefunden.

Es bleiben wichtige Kritikpunkte, von denen hier exemplarisch nur drei genannt werden sollen:

Für das Auskunftsrecht der Betroffenen über Daten zur eigenen Person wird zwar auf die Vorschriften des nordrhein-westfälischen Daten-

schutzgesetzes verwiesen, dieses enthält jedoch Ausnahmeregelungen, die – je nach Interpretation durch die Anstalt – den grundsätzlichen Auskunftsanspruch leicht vereiteln können. Zudem wurde für das Recht auf Akteneinsicht die Regelung aus dem Strafvollzugsgesetz für Erwachsene übernommen, obwohl im Gesetzgebungsverfahren darauf hingewiesen wurde, dass diese zu eng ist und in der gängigen Auslegung der Justizvollzugsbehörden praktisch leerläuft. Wesentliche Voraussetzung für die vom Bundesverfassungsgericht geforderte Verbesserung des gerichtlichen Rechtsschutzes wäre ferner, wie von der LDI NRW gefordert, die Auskunftsanträge auf Verlangen schriftlich zu bescheiden. Nur mündliche Auskünfte sind nämlich kaum auf Vollständigkeit und Richtigkeit überprüfbar, weshalb sie dem Schutzbedürfnis der Jugendlichen nicht Rechnung tragen.

Des weiteren wurde die ärztliche Schweigepflicht, die grundsätzlich auch das Patientengeheimnis von Gefangenen schützt, gegenüber der Haftanstalt so stark ausgehöhlt, dass eine Störung des Vertrauensverhältnisses zwischen den Inhaftierten und ihren medizinischen Betreuerinnen und Betreuern befürchtet werden muss. Dies kann auch folgenschwere Auswirkungen auf die Bereitschaft der Gefangenen zur medizinischen Behandlung haben.

Schließlich sieht das Gesetz eine landesweite Zentraldatei vor, in der ohne gesetzliche Beschränkung die im Vollzug erhobenen Daten der Häftlinge zentral gespeichert werden können. Alle im Justizvollzug Beschäftigten und auch das Justizministerium NRW als Aufsichtsbehörde können dann auf die Daten zugreifen. Die Verfassungsmäßigkeit dieser Regelung ist schon wegen ihrer Unbestimmtheit sehr zweifelhaft. Weder Inhalt noch Zweck der Datei wurden im Gesetz festgelegt.

➡ Das Jugendstrafvollzugsgesetz NRW leidet an zahlreichen datenschutzrechtlichen Mängeln, die reparaturbedürftig sind. Einstweilen muss in der Praxis soweit möglich eine datenschutzkonforme Auslegung und Umsetzung erfolgen.

8.2 Besucherscannen verboten

Das Scannen der Personalausweise von Besucherinnen und Besuchern in Haftanstalten zum Zweck der Speicherung ihrer

Daten ist rechtswidrig. Das Justizministerium NRW lässt sich davon aber nur widerwillig überzeugen.

Bereits im Jahr 2002 hat die LDI NRW das Justizministerium NRW darauf hingewiesen, dass die Praxis, bei der Besuchskontrolle in einer Justizvollzugsanstalt die Daten aus der maschinenlesbaren Zone der Personalausweise zu erheben und zu speichern, rechtwidrig ist. Es fehlt nämlich eine gesetzliche Grundlage, die erlauben würde, die Maschinenlesbarkeit der Personalausweise zur Datenspeicherung zu nutzen (siehe hierzu ausführlich im Bericht 2003 unter 17.3). Da das Justizministerium NRW dieser Auffassung jedoch nicht gefolgt ist, musste der Rechtsanwalt des Beschwerdeführers gerichtliche Hilfe in Anspruch nehmen. Das zuständige Verwaltungsgericht hat nun im Sommer 2008 die von der LDI NRW vertretene Position gestützt. Das Justizministerium NRW versuchte sich hiergegen nochmals zu wehren, indem es einen Antrag auf Zulassung der Berufung stellte. Dieser ist nunmehr vom Oberverwaltungsgericht des Landes Nordrhein-Westfalen unanfechtbar abgelehnt worden.

➡ Das Justizministerium NRW muss nun endlich die bisherige rechtswidrige Praxis stoppen und die unerlaubt erhobenen Daten unverzüglich löschen.

8.3 Gerichtshilfe, Bewährungshilfe, Führungsaufsicht: Zusammenwachsen darf nur, was zusammen gehört

Per Organisationserlass hat das Justizministerium NRW die drei ambulanten sozialen Dienste der Justiz zum 1. Juni 2008 in einer Behörde zusammengefasst. Aber jedes Instrument in diesem Trio muss nach eigenen gesetzlichen Regeln spielen.

Aus den unterschiedlich gesetzlich geregelten Diensten Gerichtshilfe, Bewährungshilfe und Führungsaufsicht, die bisher auch weitgehend unabhängig von einander agierten, sind nach dem Erlass drei Fachbereiche einer am jeweiligen Landgericht angesiedelten, einheitlichen Dienststelle geworden. Dabei sind nach den gesetzlichen Regelungen den Diensten jeweils unterschiedliche Funktionen zugewiesen: Bei der Gerichtshilfe steht die Recherche im Ermittlungsverfahren im Vordergrund, bei der Führungsaufsicht die Kontrolle und bei der Bewährungshilfe die Unterstützung der zu betreuenden Person.

Die aus Kreisen der Bewährungshilfe monierte Verwischung von Zuständigkeiten, die sich in der Verwendung des neuen Begriffs Fachkraft, der Schaffung einer einheitlichen Dienststellenleitung mit Aufsichtsbefugnissen und den fachbereichsübergreifenden Vertretungsregelungen niederschlägt, hat auch eine datenschutzrechtliche Dimension: Die Struktur des neuen ambulanten sozialen Dienstes hat zu gewährleisten, dass gesetzliche Aufgabenzuweisungen, die immer auch Zuständigkeiten für bestimmte Datenverarbeitungen bedeuten, nicht unterlaufen werden. Es dürfen durch organisatorische Vereinheitlichung und funktionsunabhängige Vertretungsregelungen keine gesetzlich nicht erlaubten Datenzugriffe ermöglicht werden. Ebenso wenig kann es eine Datenübermittlung zu Aufsichtszwecken neben der gesetzlich vorgesehenen Aufsicht geben. Die LDI NRW wurde weder an der Erstellung noch an der Umsetzung des Erlasses beteiligt.

➡ Es wird zu kontrollieren sein, ob in den neuen Dienststellen ein datenschutzrechtlich konfliktfreies Zusammenspiel gewährleistet ist. Insbesondere Vertretungs- und Aufsichtsregelungen der neuen Dienststellen müssen auf den Prüfstand.

8.4 IT-Vernetzung mit Fallstricken

Bereits vor der Zusammenlegung der ambulanten sozialen Dienste (siehe hierzu 8.3) hat das Justizministerium NRW ein Programm entwickelt, das Gerichtshilfe, Bewährungshilfe, Führungsaufsicht und darüber hinaus den Sozialdienst in den Justizvollzugsanstalten elektronisch miteinander vernetzen soll. So entsteht eine landesweite Zentraldatei, in der umfangreiche Datensätze aller von den genannten Diensten betreuten Personen gespeichert sind.

Unter dem Namen SoPart (Sozial-Partner) wurde eine landesweite Datenbank geschaffen, in der alle Mitarbeiterinnen und Mitarbeiter der genannten sozialen Dienste das ihnen anvertraute Klientel erfassen und die Vorgangsbearbeitung elektronisch durchführen sollen. Dabei sind zwei Stufen der Datenverarbeitung zu unterscheiden: Auf einer ersten Stufe finden sich im Wesentlichen nur die der Identifizierung dienenden Stammdaten der Betroffenen und die Kontaktdaten der für sie zuständigen Bearbeiterinnen oder Bearbeiter. Auf einer zweiten

Ebene, der Ebene der Fachdaten, findet die eigentliche Fallbearbeitung statt. Dementsprechend werden dort alle von und über die Betroffenen erhobenen Informationen verarbeitet und der Schriftverkehr sowie Vermerke gespeichert.

Auf der Ebene der Stammdaten galt es zunächst, nicht zur Identifizierung der Betroffenen erforderliche Daten und Freitextfelder aus dem Stammdatensatz entfernen zu lassen. Diese Anforderung soll nach Auskunft des Justizministeriums NRW bis zum Ende des Jahres 2008 umgesetzt sein.

Das Hauptaugenmerk bei der Prüfung der Stammdatenverarbeitung lag zunächst auf dem Problem, dass der Zugriff auf die Stammdaten allen Nutzerinnen und Nutzern des Programms offen stehen sollte. Eine Zugriffsmöglichkeit aller rund 1.700 in den verschiedenen sozialen Diensten Beschäftigten auf die Stammdaten von vielen Tausend Beschuldigten, Verurteilten oder auch Inhaftierten war nicht zu rechtfertigen. Die jetzt vorgesehene Lösung besteht darin, dass die Beschäftigten nur noch mittels einer von ihnen auszufüllenden Suchmaske Zugang zu den Stammdaten erlangen können. Es erscheint dann lediglich eine Trefferliste, die mit den eingegebenen Daten abgeglichen werden kann, um bei der Erfassung einer Betreuungsperson das Anlegen einer Dublette zu vermeiden.

Durch diese Lösung ist die Zahl der für die Beschäftigten zugänglichen Stammdatensätze ganz erheblich reduziert worden. Da bei der Verwendung der Suchmaske unwiderruflich ein neu zu bearbeitender Vorgang gestartet wird, ist ferner die missbräuchliche Verwendung zu nicht dienstlichen Zwecken weitgehend ausgeschlossen. Dennoch wird noch weiter nach einer Lösung gesucht, die den Zugriff auf Daten von Personen, für die keine fachliche Zuständigkeit besteht, vermeidet und dabei dem Ziel, das Anlegen von Dubletten zu verhindern, so weit wie möglich gerecht werden kann.

Viel einschneidender für die Betroffenen sind jedoch die durch die Verwendung von SoPart neu gegebenen Möglichkeiten des Zugriffs auf die sie betreffenden Fachdaten. Hierzu können auch in größerem Umfang besonders sensible Daten gehören, wie zum Beispiel Gesundheitsdaten, Daten die unter das Sozial- oder Steuergeheimnis fallen oder auch Informationen, die die Betroffenen der für sie zuständigen Bewährungshelferin oder dem für sie zuständigen Bewährungshelfer

im Hinblick auf deren grundsätzlich bestehende Verschwiegenheitspflicht anvertraut haben. Während die vom Gericht persönlich bestellten Bewährungshelferinnen und Bewährungshelfer bisher weitgehend selbst bestimmten, wem sie die ihnen anvertrauten Daten im Vertretungsfall zugänglich machten, bestehen nach dem Zugriffskonzept von SoPart grundsätzliche Zugriffsmöglichkeiten aller mit der Sachbearbeitung betrauten Beschäftigten einer Dienststelle. Innerhalb einer Dienststelle des neu geschaffenen ambulanten sozialen Dienstes wird hier nicht einmal nach Fachbereichen differenziert. Für den Vertretungsfall, auch im Rahmen der Notvertretung des Bereitschaftsdienstes, muss nach Auffassung des Justizministeriums NRW der Zugriff der diensthabenden Beschäftigten auf die Fachdaten offen stehen.

Damit wird faktisch allen Fachkräften einer Dienststelle – unabhängig von der eigenen Zuständigkeit – freier Zugang zu den bei der Fallbearbeitung gespeicherten Fachdaten im jeweiligen Landgerichtsbezirk verschafft. Die Anweisung, dass die in "SoPart gespeicherten Daten nur bei vorhandenem dienstlichem Bezug eingesehen werden" dürfen, ist, abgesehen von der inkorrekten, da viel zu weichen Formulierung des Erforderlichkeitsgrundsatzes, nur die Wiedergabe einer rechtlichen Selbstverständlichkeit, aber kein echtes Korrektiv der faktisch unbegrenzten Zugriffsmöglichkeiten. Der Zugang zu den innerhalb persönlicher Zuständigkeitsbereiche gespeicherten Daten darf nur der tatsächlich für die Fallbearbeitung zuständigen Fachkraft offen stehen und muss durch geeignete Barrieren, etwa die Verwendung von Passwörtern, geschützt werden. Sofern ausnahmsweise ein Zugriff im Fall einer Notvertretung erforderlich wird, kann dieser zwar technisch – zum Beispiel durch die Zurücksetzung des Passworts über die Systemadministration – ermöglicht werden, muss dann aber für die Vertretenen sichtbar werden, etwa durch einen automatisch generierten Hinweis. Zudem ist die Protokollierung aller Zugriffe auf vertrauliche Fachdaten eine Mindestanforderung zum Schutz gegen missbräuchliche Einsichtnahme. Die Verfahrenspflegestelle hat inzwischen zugesagt, zu prüfen, ob künftig Protokollberichte erstellt werden, um zumindest eine nachträgliche Kontrolle der Zugriffsberechtigung zu ermöglichen.

➡ Das Zugriffsberechtigungskonzept von SoPart ist unter anderem im Hinblick auf zu weitgehende Vertretungsrechte nicht datenschutzgerecht und bedarf noch weiterer Überarbeitung.

9 Kommunales

9.1 Zugang zu Geodaten – der Blick über den Landkartenrand

Mit der Umsetzung der so genannten INSPIRE-Richtlinie zur Nutzung von Geodaten wird eine Vielzahl teilweise auch personenbeziehbarer Informationen öffentlich verfügbar gemacht.

Die Einführung einer einheitlichen Geodateninfrastruktur und die Bereitstellung der bei öffentlichen Stellen vorhandenen Daten eröffnen ein großes Potenzial an volkswirtschaftlichem Nutzen und ermöglichen viele eGovernment- und eCommerce-Anwendungen. Die INSPIRE-Richtlinie zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft vom 14. März 2007 (2007/2/EG) regelt die Bereitstellung von amtlich vorhandenen Geodaten nach einheitlichen Standards für kommerzielle und private Nutzungen durch elektronischen Abruf über das Internet. Sie ist bis zum 15. Mai 2009 in nationales Recht umzusetzen. Die Landesregierung NRW hat daher im Dezember 2008 den Entwurf eines Geodatenzugangsgesetzes in den Landtag eingebracht. Auf Bundesebene ist ein entsprechendes Gesetz bereits verabschiedet worden.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben (zum Beispiel Luftbilder mit Geokoordinaten) aufgrund der neuen Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- und Standortdaten zu personenbezogenen Daten. Diesem Umstand müssen die neu zu schaffenden gesetzlichen Regelungen Rechnung tragen. Hierzu bedarf es angemessener Datenschutzregelungen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher mehrfach, zuletzt am 6./7. November 2008 (Entschließung im Anhang) die Gesetzgeber von Bund und Ländern aufgefordert, in den anstehenden Gesetzgebungsverfahren einen angemessenen Ausgleich zwischen den berechtigten Interessen der Nutzerinnen und Nutzer einerseits und den schutzwürdigen Belangen Betroffener andererseits zu schaffen. Der Umstand, dass Geodaten in einigen Fällen sehr leicht zu erheben und zu erlangen sind, macht sie nicht automatisch zu einer allgemein zugänglichen Quelle. Das Grundrecht auf informationelle Selbstbestimmung ist auch für Geodaten zu beachten. Nach der INSPIRE-Richtlinie selbst soll die Zugangsmöglichkeit eingeschränkt wer-

den, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann. Die Interessen der Nutzerinnen und Nutzer können nur dann Vorrang haben, wenn sie schwerer zu gewichten sind, als die schutzwürdigen Belange der Betroffenen. Diesem Anliegen wird die für NRW geplante Regelung bisher jedoch nicht gerecht. Für die vorzunehmende Interessenabwägung wird auf eine Regelung des Umweltinformationsgesetzes NRW verwiesen, welche den Betroffenen nur dann eine Möglichkeit einräumt, gegen die Veröffentlichung personenbezogener Daten vorzugehen, wenn sie eine "erhebliche Beeinträchtigung" ihrer Interessen nachweisen können. Diese Schwelle zur Abwehr von Eingriffen in das Recht auf informationelle Selbstbestimmung ist zu hoch. Ferner entstünde ein Wertungswiderspruch zu den Regelungen des Vermessungs- und Katastergesetzes NRW, das für die Herausgabe von Eigentümerangaben ein "berechtigtes Interesse" voraussetzt.

➡ Der Zugang zu Geodaten für die Allgemeinheit sollte nicht erst dort seine Grenzen haben, wo Einzelne "erheblich" beeinträchtigt werden. Auch die Beweislast hierfür darf nicht bei den Betroffenen liegen. Zumindest sollten ihnen Widerspruchsmöglichkeiten eingeräumt werden. Daneben sollten die Verfahren transparent und datenschutzfreundlich gestaltet und umfassende Vorab-Datenschutzprüfungen durchgeführt werden.

9.2 Der neue elektronische Personalausweis – Pflicht oder faktischer Zwang?

Ab dem 1. November 2010 soll der elektronische Personalausweis verpflichtend eingeführt werden. Nach wie vor bestehen hier datenschutzrechtliche Bedenken wegen der Speicherung biometrischer Merkmale. Zudem soll der neue Personalausweis zur elektronischen Authentifizierung genutzt werden können. Auch dies ist problematisch.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich bereits bei der Einführung des elektronischen Reisepasses mehrfach gegen die Speicherung digitalisierter biometrischer Merkmale ausgesprochen (siehe Bericht 2007 unter 11.1). Anders als

bei einer erkennungsdienstlichen Behandlung durch die Polizei haben jedenfalls Fingerabdrücke in den Ausweispapieren für die gesamte Bevölkerung nichts zu suchen. Nur aufgrund öffentlichen Drucks konnte gerade noch erreicht werden, dass die Aufnahme von Fingerabdrücken in den Personalausweis zumindest dem Gesetz nach nur freiwillig erfolgen soll. Dennoch steht zu befürchten, dass – jedenfalls auf Dauer – der soziale Druck gegenüber jeder und jedem Einzelnen dazu führt, dass von einer wirklich freiwilligen Entscheidung nicht gesprochen werden kann und alle Deutschen quasi erkennungsdienstlich erfasst werden. Die Speicherung der Fingerabdrücke ist allerdings nur im Personalausweis selbst erlaubt.

Ein digitalisiertes Passbild wird aber in jedem Falle erstellt, in der Ausstellungsbehörde gespeichert und in den Ausweis aufgenommen. Ob die Fälschungssicherheit damit wirklich gestärkt wird, muss bezweifelt werden, zumal die Daten über einen kontaktlosen Chip ausgelesen werden können. Funkgesteuerte Chips können grundsätzlich leichter manipuliert und ausgelesen werden.

Auch die Möglichkeit, sich auf freiwilliger Basis im Rechtsverkehr gegenüber Dritten identifizieren zu können (elektronische Authentifizierung), ist kritisch zu sehen. Zwar kann eine Authentifizierungsfunktion und deren freiwillige Nutzung zur Abwicklung von Online-Transaktionen nützlich sein. Allerdings besteht keine Notwendigkeit, eine solche Funktion mit der des Personalausweises zu verbinden. Es stellt sich bereits die Frage, ob der Staat diese Möglichkeit erschließen muss. Jedenfalls sollten getrennte Speichermedien für die verschiedenen Verwendungszwecke eingesetzt werden. Dezentrale Lösungen sind datenschutzrechtlich immer weniger fehler- und missbrauchsanfällig. Zudem besteht hier für die Betroffenen die Gefahr, bei einem Verlust des Ausweises auch die "elektronische Identität" zu verlieren.

➧ Die Einführung der neuen elektronischen Personalausweise bleibt auch ohne eine Pflicht zur Speicherung der Fingerabdrücke problematisch.

9.3 Melderegister – offen für alle

Im Juni 2008 wurden Bevölkerung und Behörden von der Meldung überrascht, die kommunalen Melderegister von 15 deut-

schen Städten seien wegen einer Software-Panne über einen geraumen Zeitraum im Internet frei zugänglich gewesen. Offene Register auch in Nordrhein-Westfalen?

Recherchen eines TV-Magazins hatten ergeben, dass es über Monate hinweg möglich war, etwa Adressen, Passbilder und Religionszugehörigkeit von insgesamt circa 500.000 Bürgerinnen und Bürgern herauszufinden. Der Zugangscode entsprach einem auf der Internetseite der Herstellerfirma der Software hinterlegten Code für die Präsentation der Anwendung einer Internet-Gewerberegisterauskunft. Besucherinnen und Besucher der Internetseite konnten durch einfache Mausbewegungen über den entsprechenden Link die Zugangsdaten für die Melderegister sehen. Diese Anwendungsmöglichkeit bestand jedoch nur bei denjenigen Kommunen, die Online-Melderegisterauskünfte anbieten, und die bei der Inbetriebnahme des Programms die herstellerseitig eingestellte Codierung nicht verändert hatten. Dies war tatsächlich bei 13 der 425 Anwenderkommunen der Fall.

Das Innenministerium NRW hat nach einer Empfehlung der LDI NRW die Kommunen noch am Tage der Ausstrahlung des TV-Beitrags auf die Sicherheitslücke hingewiesen. Nach dem späteren Bericht der Landesregierung an den Innenausschuss des Landtags (Vorlage 14/1963) wurde ein unberechtigter Zugriff bei Meldebehörden in Nordrhein-Westfalen nicht festgestellt. Bei einem Kontrollbesuch in einer betroffenen Kommune bestätigte sich dies zwar, aber es musste auch festgestellt werden, dass die nach dem Datenschutzgesetz NRW vorzuhaltenden Prüfunterlagen zum Verfahrensverzeichnis und zum Sicherheitskonzept unvollständig waren. Die Kommune hat zugesagt, die Unterlagen auch für die anderen von ihr betriebenen Verfahren zu erstellen oder zu vervollständigen und das vorgeschriebene Sicherheitskonzept zu erarbeiten.

➡ Technik kann nur bei entsprechender Sorgfalt der sie bedienenden Menschen gut funktionieren. Interne wie externe Kontrollen bleiben ein wichtiges Instrument des Datenschutzes.

9.4 Einfache Melderegisterauskunft und Adresshandel

Der Handel mit Adressen ist im Berichtszeitraum mehrfach in die Kritik geraten. Eine Quelle für dieses Wirtschaftsfeld stellt auch die gesetzlich vorgesehene so genannte einfache Melderegisterauskunft dar.

Das nordrhein-westfälische Melderecht ermöglicht, wie die Regelungen anderer Bundesländer auch, auf Antrag Auskunft etwa über aktuelle Vor- und Familiennamen, Doktorgrad und Anschrift einzelner Einwohnerinnen und Einwohner zu erhalten. Einfache Melderegisterauskünfte werden von den Meldebehörden auf Antrag im Einzelfall erteilt. Hierzu genügt es, zu der gesuchten Person eindeutige Angaben machen zu können. Die Nennung von Namen, Anschrift oder des Geburtsdatums bei der Antragstellung sind ausreichend. Bei der Entscheidung über die Anträge haben die Behörden einen Ermessensspielraum. In der bisherigen Praxis ist den Anträgen jedoch in der Regel entsprochen worden. Denn entgegenstehende schutzwürdige Interessen der Betroffenen müssen ein gewisses Gewicht aufweisen, um eine Auskunfterteilung zu verhindern.

In der Praxis werden einfache Melderegisterauskünfte jedoch vielfach auch genutzt, um offene Forderungen zu realisieren. Versandhandelsunternehmen und andere Firmen vergeben hierzu häufig extern Aufträge an weitere gewerbliche Unternehmen. Diese erforschen zunächst die Anschriften säumiger Kundinnen oder Kunden. Dazu werden einfache Melderegisterauskünfte eingeholt und die Anschriften an die Auftraggeber weitergegeben. Ein solches Vorgehen ist grundsätzlich nicht zu beanstanden. Wenn jedoch die Daten nicht nur für den benötigten Zweck verwendet, sondern zusätzlich in einer eigenen Datenbank bei den externen Unternehmen gespeichert werden, um sie auch an weitere Stellen weiterzugeben, ist der Schutz der Meldedaten nicht mehr gewährleistet. Dies wird insbesondere dann besonders deutlich, wenn zwischenzeitlich eine Auskunftssperre eingetragen worden ist.

Im Sommer 2008 hat das Innenministerium NRW die Meldebehörden darauf hingewiesen, dass die Ermessensentscheidung der Meldebehörden eine Prüfung in jedem einzelnen Fall erfordert. Denn das Melderegister ist kein öffentliches Register, das für alle beliebig verfügbar ist. Für eine Speicherung der Melderegisterdaten durch gewerbsmäßige Adresshändler in eigenen Dateien oder die Weitergabe an andere Auf-

traggeber dürfen einfache Melderegisterauskünfte nicht erteilt werden. Gewerbsmäßige Adresshändler sollen daher erklären, dass die übermittelten Daten nur an einen Auftraggeber weitergegeben und nicht länger als 30 Tage sowohl bei der anfragenden Firma als auch bei deren Auftraggeber gespeichert werden. Einzelne gewerbliche Adressenhändler haben daraufhin kurzfristig entsprechende Erklärungen gegenüber dem Innenministerium NRW abgegeben.

➡ Einfache Melderegisterauskünfte dürfen zum Zwecke der gewerblichen Nutzung nur nach strengen Maßstäben erteilt werden. Dies haben die Meldebehörden zu gewährleisten.

9.5 Bund plant zentrales Melderegister

Mit der Föderalismusreform wurde der Bund zuständig für das Meldewesen. Der Referentenentwurf eines Bundesmeldegesetzes, das an die Stelle der bisherigen Landesmeldegesetze treten soll, begegnet erheblichen Bedenken. Gegenstand der Kritik ist insbesondere die Einführung eines Bundesmelderegisters.

Dadurch würden die Daten der 82 Millionen Einwohnerinnen und Einwohner der Bundesrepublik zusätzlich zu den bestehenden kommunalen Melderegistern zentral erfasst. Diese Datenvorhaltung ist nicht erforderlich, weil der Bund seine Bedürfnisse durch eine Vernetzung der kommunalen Register decken kann. Die Datenschutzbeauftragten des Bundes und der Länder haben sich zu diesen Planungen bereits mehrfach kritisch geäußert.

Nach den Vorstellungen der Bundesregierung sollen in diesem Bundesmelderegister von jeder in Deutschland gemeldeten Person mindestens 27 persönliche Daten gespeichert werden. Darunter Geschlecht, die Religionszugehörigkeit, der Familienstand sowie die lebenslange Steueridentifikationsnummer. Auch Pass- und Ausweisdaten sollen gespeichert werden, wenn auch nicht die biometrischen Merkmale. Unter Umständen könnte der Datensatz jeder Person auf über 60 Einträge anwachsen. Neben der "elektronischen Bürgeradresse", einer Art Online-Postfach bei den geplanten Bürgerportalen des Bundes, sowie Tag der Eheschließung und Ort sollen auch die gesetzlichen

Vertretungen samt Doktorgrad, Anschrift, Geburtstag, Geschlecht und Todestag im Bundesmelderegister erfasst werden. Fast alle diese Daten sollen auch von Ehegatten, Lebenspartnerinnen und –partnern und von minderjährigen Kindern gespeichert werden. Weitere Informationen sollen für bestimmte Zwecke erfasst werden: Darf die Person wählen oder gewählt werden? Ist sie bereits für den Wehrdienst erfasst worden? Wurde eine Waffenerlaubnis erteilt; wenn ja, wann? Wurde eine sprengstoffrechtliche Erlaubnis erteilt; wenn ja, wann?

So entsteht eine "Superdatensammelbehörde", die für die zentralen Zwecke des Meldewesens nicht erforderlich ist. Vielmehr besteht die Gefahr, dass auf Dauer zusätzlich zu den bestehenden Melderegistern hier immer mehr Daten zusammengezogen, vernetzt und gebündelt werden. Dadurch werden immer neue Begehrlichkeiten geweckt und die Missbrauchsgefahr erhöht. Für zentrale Zwecke reichen wenige Grunddaten, etwa Name, Geburtsdatum, Geburtsort, früherer Wohnsitz, Tag des Zuzugs und Geschlecht aus.

Der Referentenentwurf sieht zudem die Zugriffsmöglichkeit für Geheimdienste und Verfassungsschutz vor. Bundesnachrichtendienst und Militärischer Abschirmdienst sollen auf alle beim Bundesmeldereister und den Meldebehörden gespeicherten Daten zugreifen dürfen. Das gleiche Recht hätten auch Polizei, Staatsanwaltschaften, Justizvollzugsbehörden, Zollfahndung und zur Strafverfolgung auch Finanzbehörden. Auch andere öffentliche Behörden könnten auf sämtliche Daten der Meldebehörden zugreifen. Zwei Bedingungen müssen dafür erfüllt sein: Ohne die Meldedaten könnte die Stelle ihre rechtmäßige Aufgabe nicht wahrnehmen. Außerdem müssen die Daten bei den Betroffenen entweder nur mit unverhältnismäßigem Aufwand erhoben werden können oder aber der Zweck, für den die Daten gebraucht werden, muss der Datenerhebung bei den Betroffenen entgegenstehen. Diese Zugriffsmöglichkeiten gehen zu weit. Alle im Register erfassten Personen würden für den Staat quasi zu gläsernen Menschen.

Eine Reihe weiterer Punkte des Referentenentwurfes sind bedenklich, von denen hier nur einige genannt werden können:

- Die Datenverarbeitung bei den Meldeämtern sowie alle Übermittlungstatbestände werden nicht ausreichend protokolliert und ausgewertet. Die Protokollierung und die Möglichkeit einer Protokollauswertung stellen jedoch eine wichtige Basis für die

Ausübung des Rechts auf informationelle Selbstbestimmung sowie für die Kontrollen durch die zuständigen Datenschutzbehörden dar.

- Die Möglichkeit eines automatisierten Abrufverfahrens von Meldedaten durch öffentliche Stellen über das Internet ist bedenklich. Diese Möglichkeit soll eröffnet sein, wenn über die Identität der Stelle "kein Zweifel besteht" und die Daten verschlüsselt übermittelt werden. Dies reicht zur Wahrung der schutzwürdigen Interessen der Betroffenen aber nicht aus. Angesichts der Missbrauchsmöglichkeiten des Internet sollten bei elektronischen Abrufverfahren über das Internet auch für öffentliche Stellen zumindest Verfahren der fortgeschrittenen elektronischen Signatur vorgesehen werden.

- Die geplante Internet-Selbstauskunft, mit der alle bei den Meldebehörden vorhandenen Daten zur eigenen Person erfragt werden können, unterliegt einer hohen Missbrauchsgefahr, da ein sicheres elektronisches Verfahren zur Identitätsfeststellung noch nicht existiert. Ob und inwieweit die geplante freiwillige Funktion zur Authentifizierung per Chip auf dem elektronischen Personalausweis hier die erforderliche Lösung bringt, kann erst beurteilt werden, wenn die diesem zugrunde liegenden Sicherheitskonzepte vorliegen.

- Nicht hinzunehmen ist auch, dass das Kontrollrecht der Datenschutzbeauftragten entgegen der landesrechtlichen Regelung im Datenschutzgesetz NRW beschränkt werden soll. Dazu darf es nicht kommen.

- Melderegisterauskünfte, die Firmen im Auftrag Dritter einholen, sollten unterbunden werden, wenn die Daten nicht nur für den ursprünglichen Zweck genutzt werden, sondern auch für andere Zwecke weiterverwendet werden. In Schleswig-Holstein und in Nordrhein-Westfalen haben die jeweiligen Innenministerien entsprechende Erlasse herausgegeben, die solche Datenübermittlungen untersagen beziehungsweise aufgrund derer die Daten nur unter Hinweis auf die Zweckbindung und die Löschfristen übermittelt werden dürfen. Die Kommunen werden dadurch bei der Prüfung, ob schutzwürdige Belange verletzt werden, stärker in die Pflicht genommen (siehe Bei-

trag zu Melderegisterauskunft und Adresshandel unter 9.4). Ohne eine entsprechende gesetzliche Regelung sollte ein Bundesmeldegesetz nicht erlassen werden.

➡ Ein zentrales bundesweites Melderegister ist abzulehnen. Eine Reform des Melderechts sollte genutzt werden, dem originären Zweck des Meldewesens zu entsprechen und die zu speichernden Daten einer kritischen Prüfung unter den Gesichtspunkten der Erforderlichkeit und der Zweckbindung zu unterziehen. Es muss insbesondere sichergestellt werden, dass jede Behörde nur die Daten erhält, die sie zur Durchführung ihrer gesetzlichen Aufgaben benötigt.

10 Soziales

10.1 Verfassungsrechtliche Bedenken am ELENA-Verfahrensgesetz

Rund 40 Millionen Beschäftigte sollen nach Vorstellung des Bundesgesetzgebers zukünftig die monatliche Übermittlung ihrer Einkommensdaten an eine Zentrale Speicherstelle zu dulden haben, obwohl feststeht, dass der überwiegende Teil der vorrätig gehaltenen Daten niemals gebraucht werden wird.

Ziel des Gesetzes ist es, die zur Beantragung insbesondere des Arbeitslosengeldes erforderlichen Entgeltbescheinigungen in elektronischer Form zentral vorrätig zu halten. Ein großer Anteil der Betroffenen wird die von ELENA erfassten Sozialleistungen (Arbeitslosen-, Eltern- und Wohngeld) jedoch niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass die große Mehrzahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Stellung eines Antrags wird zudem nur noch mittels einer zuvor erworbenen und angemeldeten qualifizierten Signatur möglich sein.

Die in der Begründung des nun eingebrachten Gesetzentwurfs insgesamt einseitig dargestellten Hoffnungen auf langfristige Effizienzsteigerungen der Arbeitsverwaltung und die Verbreitung der qualifizierten Signaturkarte dürfen nicht über eine im Ergebnis unverhältnismäßige Duldungspflicht für rund 40 Millionen Menschen erzwungen werden. Trotz entsprechender Hinweise, zuletzt in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008 (Abdruck im Anhang), hat sich der Gesetzgeber mit den verfassungsrechtlichen Bedenken an der Verhältnismäßigkeit einer derartigen zentralen Datensammlung nicht ausreichend auseinandergesetzt.

Zentraldateien wecken zudem meistens neue Begehrlichkeiten. Sie bringen stets Überwachungs-, Zweckänderungs- und Missbrauchsrisiken mit sich. Bereits aus diesem Grunde hätte eine sorgfältige Risiko/Nutzen-Abwägung durchgeführt werden müssen.

Hinzu kommt, dass sich mit der in Aussicht genommenen Einbeziehung weiterer Sozialleistungsverfahren zunehmend das Problem eines die Zweckbindung gefährdenden Ordnungsmerkmals stellt.

➧ Solange die verfassungsrechtlichen Fragen nicht befriedigend geklärt sind, ist der Gesetzentwurf der Bundesregierung über das Verfahren des elektronischen Entgeltnachweises abzulehnen.

10.2 Kindeswohl und Datenschutz

Tragische Fälle von Kindesvernachlässigungen haben nicht nur auf allen öffentlichen Ebenen, sondern auch bei Ärztinnen und Ärzten zu Bemühungen geführt, Kindeswohlgefährdungen frühzeitig zu erkennen und deren Realisierung zu vermeiden. Vier Vorhaben, die diesem Ziel dienen sollen, werden beispielhaft dargestellt und auf ihre Datenschutzkonformität hin überprüft. Dabei sollte jedoch nicht außer Acht gelassen werden, dass gerade die in den Medien dargestellten tragischen Fälle den Jugendämtern bereits bekannt waren.

"Riskid – Risikokinder Informationsdatei": Bei dem Projekt handelt es sich um eine Online–Datenbank. In diese Datei tragen Duisburger Kinderärztinnen und Kinderärzte seit Juli 2007 Angaben zu Kindern nach Risikokategorien ein. Die "Riskid – Risikokinder Informationsdatei" dient als begleitender Wächter neben Jugendamt, Gesundheitsamt und Polizei.

Neben gesicherten Fällen körperlicher Misshandlung, Mangelversorgung und Vernachlässigung werden auch Verdachtsfälle unterschiedlichen Grades bis hin zu Fällen, in denen die Kinder bislang unauffällig, jedoch aufgrund des familiären Umfeldes gefährdet seien (Risikofälle/Geschwisterfälle), eingestellt. Zugriff auf die eingestellten Daten haben alle an dem Projekt teilnehmenden Ärztinnen und Ärzte. Die nach dem ICD-10-Schlüssel abgerechneten Diagnosen reichen dementsprechend von "battered child" über "tätlichen Angriff" und "sexuellen Missbrauch" bis hin zu "auf das familiäre Umfeld beschränkte Störung des Sozialverhaltens".

Der Gesetzgeber ist zu der Entscheidung berufen, ob das klassische und durch die ärztliche Schweigepflicht geschützte Arzt-Patienten-Ver-

hältnis zum Wohle eines Austausches innerhalb der Ärzteschaft neu auszurichten ist. Bis zu einer derartigen gesetzgeberischen Entscheidung setzen sich die teilnehmenden Ärztinnen und Ärzte dem Risiko einer Strafverfolgung (§ 203 Strafgesetzbuch) sowie berufsrechtlicher Konsequenzen (§ 9 Berufsordnung der Ärztekammer Nordrhein) aus, da eine Befugnis für die in der Nutzung von "Riskid" liegende Durchbrechung der ärztlichen Schweigepflicht nach der gegenwärtigen Rechtslage nicht gegeben ist. Demgegenüber haben die Ärztinnen und Ärzte schon jetzt die Befugnis bei Vorliegen konkreter Anhaltspunkte für eine erhebliche und gegenwärtige Kindeswohlgefährdung das Jugendamt oder die Polizei einzuschalten. Je nach den Umständen des Einzelfalles kommt (zunächst) auch das Einwirken auf die Eltern in Betracht. Diese Entscheidung hat die Ärztin oder der Arzt in eigener Verantwortung zu treffen; ein Austausch mit anderen Ärztinnen und Ärzten zur diagnostischen Entscheidungsfindung ist dabei möglich, hat jedoch aufgrund der ärztlichen Schweigepflicht ohne Personenbezug zu erfolgen.

➡ Zum Wohle aller Betroffenen, also auch der teilnehmenden Ärztinnen und Ärzte, kann ein derartiges Interventionssystem, welches weder auf Notstandsfälle zugeschnitten noch begrenzt ist, nur auf Grundlage eines Gesetzes betrieben werden.

"Begrüßungsbesuche": Die Durchführung so genannter "Begrüßungsbesuche" durch Beschäftigte des Jugendamtes in Familien mit neuem Nachwuchs ist bei Vorliegen wirksamer Einwilligungserklärungen dem Grunde nach möglich und die Entscheidung hierüber letztlich keine Frage des Datenschutzes. Lediglich die damit einhergehende Datenerhebung und weitere Datenverarbeitung unterliegt der Kontrolle der LDI NRW. Die reine Begrüßung neu hinzugezogener und neugeborener Bürgerinnen und Bürger kann durchaus zu den bürgermeisterlichen Aufgaben gezählt werden.

Davon streng zu unterscheiden ist die Wahrnehmung öffentlicher Aufgaben nach dem Sozialgesetzbuch Achtes Buch (SGB VIII), für die das Jugendamt zuständig und verantwortlich ist. Eine für die Betroffenen intransparente Verknüpfung dieser unterschiedlichen Aufgabenstellungen und Verantwortlichkeiten bei Durchführung von Begrüßungsbesuchen wäre unzulässig. So sind die Beratung und die Unterstützung der

Eltern zur Verwirklichung des Rechtes eines jeden jungen Menschen auf Förderung seiner Entwicklung und auf Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit Aufgabe der Jugendhilfe (§ 1 Abs. 3 SGB VIII). Danach hat die Jugendhilfe auch dazu beizutragen, positive Lebensbedingungen für junge Menschen und ihre Familien sowie eine kinder- und familienfreundliche Umwelt zu erhalten oder zu schaffen. Leistungen zur Förderung der Erziehung in der Familie sind insbesondere Angebote der Beratung in allgemeinen Fragen der Erziehung und Entwicklung junger Menschen (§ 16 Abs. 2 Nr. 2 SGB VIII).

Die in § 8a SGB VIII getroffene Regelung, wonach das Jugendamt zur Erfüllung seines Wächteramtes und Schutzauftrages bei Kindeswohlgefährdungen Tatsachen erst dann ermitteln darf, wenn gewichtige Anhaltspunkte vorliegen, steht der Durchführung von Begrüßungsbesuchen nicht grundsätzlich entgegen. Allerdings läge eine Umgehung des § 8a SGB VIII dann vor, wenn Begrüßungsbesuche gezielt dazu genutzt würden, Tatsachen im Hinblick auf mögliche Kindeswohlgefährdungen allein deswegen zu ermitteln, weil ein Kind das Licht der Welt erblickt hat. Die Vermeidung von Kindeswohlgefährdungen kann – insbesondere mit Blick auf die zukünftige Entwicklung des Kindes – eine gewünschte mittelbare Folge der Besuche und Beratungen sein. Eine gezielte Sachverhaltsermittlung bei Durchführung der Hausbesuche ohne Vorliegen gewichtiger Anhaltspunkte für eine Gefährdung des Wohls des Kindes verstieße hingegen gegen die grundgesetzlich geschützten Rechte auf informationelle Selbstbestimmung, die Vorrangigkeit der elterlichen Erziehungsverantwortung und die Unverletzlichkeit der Wohnung. Sollten jedoch bei Gelegenheit eines Hausbesuches gewichtige Anhaltspunkte für eine Gefährdung des Wohls des Kindes bekannt werden, darf und hat das Jugendamt selbstverständlich die erforderlichen Maßnahmen zu ergreifen.

Beratungsleistungen und Informationen dürfen bei Durchführung der Begrüßungsbesuche angeboten werden. Darüber hinaus darf dieses Angebot von Hilfen auch aufgrund einer ersten Einschätzung der jeweils vorgefundenen Familiensituation bedarfsgerecht erfolgen, wenn diese Form der beabsichtigten Datenerhebung vor Betreten der Wohnung – insbesondere in einem Anschreiben – transparent gemacht worden ist. Die Beschäftigten des Jugendamtes dürfen die Wohnung der neuen Eltern daher nur mit deren wirksamer Zustimmung betre-

ten. Eine gesetzliche Verpflichtung, Beschäftigten des Jugendamtes zur Durchführung eines Begrüßungsbesuches Einlass zu gewähren, besteht nicht.

Die Zulässigkeit der Begrüßungsbesuche steht und fällt damit in jedem Einzelfall mit dem Vorliegen einer wirksamen Einwilligungserklärung der Betroffenen. Entscheidend ist hierbei, dass die Einwilligung rechtlich wirksam ist. Dazu sind die Betroffenen über die Freiwilligkeit der Besuche genauso aufzuklären wie über die Identität der verantwortlichen Stelle und über die verfolgten Zwecke. Soweit mehrere Zwecke verfolgt werden, ist über alle Zwecke aufzuklären.

Eine Auswertung zu statistischen Zwecken ist nur dann zulässig, wenn ein Personenbezug nicht mehr hergestellt werden kann, die Daten also anonymisiert erhoben und verarbeitet werden. Dies setzt voraus, dass die zu erhebenden Daten ihrer Art nach ein Identifizierungsrisiko möglichst ausschließen. Bedenklich wären insbesondere die Erhebung von Geburtsdaten und die Zulassung von Freitextfeldern auf Vordrucken.

Die zur Auswertung erforderlichen Daten sind bereits bei ihrer Erhebung auf einem ausschließlich für die statistische Auswertung vorgesehenen Vordruck einzutragen, der einen Bezug zu der konkret besuchten Familie nicht herstellen lässt. Eine personenbezogene Datenspeicherung ist nach Durchführung des Begrüßungsbesuches nicht mehr zulässig. Die vom Einwohnermeldeamt erhobenen personenbezogenen Daten sind nach Durchführung oder Ablehnung des Begrüßungsbesuches zu vernichten und dürfen demnach auch nicht in andere Verfahren einfließen. Eine Ausnahme ist die Einleitung erforderlicher Maßnahmen nach § 8a SGB VIII, wenn bei Durchführung eines Begrüßungsbesuches gewichtige Anhaltspunkte für eine Gefährdung des Kindeswohls bekannt werden.

Meldungen des Einwohnermeldeamtes an das Jugendamt können jeweils auf § 18 Melderechtsrahmengesetz und § 31 Meldegesetz NRW in Verbindung mit § 67a Abs. 2 Nr. 2 SGB X gestützt werden und begegnen im Ergebnis keinen durchgreifenden datenschutzrechtlichen Bedenken.

➡ Bei Einhaltung der hier dargelegten Grundsätze kann einer Sorge vor "schwarzen Listen" vorgebeugt und die Bereitschaft zur Zulassung der Begrüßungsbesuche in

der eigenen Wohnung auch in größeren Kommunen zum Wohle der Kinder erhöht werden.

"Verordnung zur Datenmeldung der Teilnahme an Kinderfrüherkennungsuntersuchungen": In Nordrhein-Westfalen sind Früherkennungsuntersuchungen freiwillig. Um die Teilnahme an ihnen dennoch sicherzustellen, ist ein aufwändiges und vor allem "pflichtiges Einladungswesen" eingerichtet worden, welches Auswirkungen sowohl auf die Berufsausübung der Ärztinnen und Ärzte (Meldepflicht) als auch auf die betroffenen Eltern hat (Recht auf informationelle Selbstbestimmung, Elternrecht, Recht auf Unverletzlichkeit der Wohnung). Das Verfahren bezweckt im Wesentlichen eine Einladung durch eine zentrale Stelle an Eltern, nicht zeitig wahrgenommene Untersuchungstermine nachzuholen. Bleibt diese Erinnerung erfolglos, ergeht eine Mitteilung an das Jugendamt.

Dabei setzt ein Tätigwerden des Jugendamtes die Kenntnis gewichtiger Anhaltspunkte für die Gefährdung des Kindeswohls voraus (§ 8a SGB VIII). Allein in der ausbleibenden Inanspruchnahme einer nach wie vor freiwilligen Vorsorgeuntersuchung kann nicht ohne weiteres ein gewichtiger Anhaltspunkt für eine Kindeswohlgefährdung gesehen werden. Der Verordnung ist zudem nicht zu entnehmen, welchen konkreten Nutzen die vorgesehenen Meldungen für die Vermeidung von Kindeswohlgefährdungen haben können. Soll etwa jede Meldung zur Durchführung eines Hausbesuches führen? Dabei ist auch zu berücksichtigen, dass der Landesgesetzgeber den Umgang mit den Meldungen durch die Jugendämter mangels Regelungskompetenz gar nicht vorschreiben kann.

Hinzu kommt, dass Nordrhein-Westfalen das "pflichtige Einladungswesen" zu Früherkennungsuntersuchungen nicht in einem formellen Kinderschutzgesetz, sondern in einer Verordnung regelt. Ermächtigungsgrundlage hierfür sei § 32a Heilberufsgesetz NRW in Verbindung mit § 31 Meldegesetz NRW.

Im Heilberufsgesetz selbst ist der Zweck, die regelmäßige Teilnahme von Kindern an den Früherkennungsuntersuchungen zur Vermeidung von Kindeswohlgefährdungen zu überprüfen und gegebenenfalls notwendige Maßnahmen einzuleiten, jedoch nicht genannt. Die Meldepflicht für Kinderärztinnen und Kinderärzte an eine zentrale Stelle und

die Durchführung eines Datenabgleich stehen isoliert und zweckfrei im Heilberufsgesetz. Auch hinsichtlich der übrigen in das Verfahren einzubeziehenden Stellen fehlt die Bestimmung der Aufgaben und Befugnisse. Die Durchführung des Datenabgleichs wird in § 32a S. 2 Heilberufsgesetz lediglich vorausgesetzt. Die Aufgabe wird erst und nur in der Verordnung geregelt.

Nach Art. 70 der Landesverfassung muss jedoch ein Gesetz Inhalt, Zweck und Ausmaß der erteilten Ermächtigung bestimmen. Diese insoweit mit Art. 80 des Grundgesetzes übereinstimmende Regelung folgt aus dem Rechtsstaatsprinzip. Datenerhebungen, Datenverarbeitungen und Datenübermittlungen auf Grundlage der Verordnung über die Teilnahme an Früherkennungsuntersuchungen für Kinder sind damit insgesamt unzulässig.

➡ Wenn ein Meldeverfahren gewollt ist, so ist es auf eine gesetzliche Grundlage zu stellen. Spätestens bis zum 31. Dezember 2011 ist eine Evaluation durchzuführen, die nicht nur zu klären hat, ob die Teilnahmequote an Früherkennungsuntersuchungen gesteigert werden konnte, sondern auch, wie oft Meldungen an Jugendämter erfolgten und welche Maßnahmen dadurch konkret veranlasst worden sind.

"Zukunft für Kinder in Düsseldorf": Als eines der effektivsten und gleichzeitig rechtskonformen Projekte erscheint nach dem gegenwärtigen Erkenntnisstand das schon seit längerer Zeit praktizierte "Düsseldorfer Modell", welches Risikolagen noch vor der Geburt des Kindes durch Hebammen sowie Frauenärztinnen und Frauenärzte erkennen und eine begleitende Unterstützung der Mütter durch eine gemeinsam vom Gesundheits- und Jugendamt ausgestattete Stelle anbieten kann. Diese Zusammenarbeit zwischen Gesundheitsamt, Jugendamt und weiteren Stellen (Kliniken, Ärztinnen und Ärzte, Hebammen, Soziale Dienste) zum Wohle der betroffenen Kinder wird stets auf die Einwilligung der Personensorgeberechtigten gestützt.

➡ Durch die Einbeziehung der Eltern und die Berücksichtigung ihres Willens kann das Projekt "Zukunft für Kinder in Düsseldorf" alle Kinder und Familien erreichen, bei denen die Förderung des Kindeswohls

wünschenswert erscheint und setzt damit bereits im Vorfeld von Kindeswohlgefährdungen an.

10.3 Datenschutz im Bereich der Jugendhilfe

Was beim Schutz personenbezogener Daten junger Menschen und ihrer Familien im Jugendamt zu beachten ist, erläutert eine Zusammenstellung für die Sachbearbeitung und für alle, die mit dem Jugendamt zu tun haben.

Die aus Anfragen gewonnenen Erfahrungen zum Umgang mit personenbezogenen Daten in Angelegenheiten der Jugendhilfe wurden zusammengefasst und den Jugendämtern in Form ausführlicher Hinweise zur Verfügung gestellt.

➡ Das Dokument kann unter www.ldi.nrw.de heruntergeladen werden.

11 Gesundheit

11.1 (Zunächst weiterhin keine) elektronische Gesundheitskarte

Voraussichtlich im Jahr 2009 soll die elektronische Gesundheitskarte flächendeckend an die gesetzlich Versicherten ausgegeben werden. Die datenschutzrechtlichen Bedenken bleiben bestehen.

Wir erinnern uns: Seit einigen Monaten wird die elektronische Gesundheitskarte mit dem elektronischen Rezept im Testbetrieb eingesetzt. Die Zahl der eingelösten Rezepte ist bisher verschwindend gering, die Bedenken bleiben bestehen: Die Rezepte sind für die Versicherten als auf der Karte gespeicherte Daten nicht ohne weiteres einzusehen und zu nutzen. Zudem kann, wie im Bericht 2007 (unter 13.1) ausgeführt, das elektronische Rezept nicht in allen Situationen Verwendung finden, so etwa bei einem ärztlichen Hausbesuch. In diesen Fällen soll auf das herkömmliche Papierrezept zurückgegriffen werden.

Nachdem bisher nur einige Hundert Karten getestet wurden, soll in einer "zweiten Testphase" die Karte flächendeckend in der Online-Anwendung überprüft werden; das heißt, die Rezepte können dann auch auf zentralen Servern gespeichert werden. Aufgrund weiterer technischer Probleme steht der Beginn der zweiten Testphase jedoch noch nicht fest.

Während in den Testphasen die Anwendung aufgrund einer Einwilligungserklärung der Teilnehmenden möglich ist, stellt sich weiter die Frage nach der Zulässigkeit des Konzepts der elektronischen Gesundheitskarte im Regelbetrieb insgesamt. Die geplante Speicherung von sensiblen Daten aus den Rezepten auf zentralen Servern birgt die Gefahr des Entstehens einer Datensammlung, deren Ausmaß derzeit nur schwer abzuschätzen ist. Dies gilt zumal, da darüber hinaus nach der gesetzlichen Regelung auch andere sensible Gesundheitsdaten – seien es Notfalldaten, Daten aus der Krankheitsgeschichte oder auch eine Organspendeerklärung – auf der Karte gespeichert werden können. Es ist daher durchaus zweifelhaft, ob das Recht auf informationelle Selbstbestimmung der Versicherten dahingehend gewahrt ist, dass die Betroffenen tatsächlich abschätzen können, was mit ihren Daten im Einzelnen geschieht.

Hinzu kommen die bereits im Bericht 2007 aufgezeigten Erschwernisse durch den Einsatz von Patiententerminal und PIN, die sich etwa bei älteren Menschen vielfach als letztlich unüberwindbare Barrieren entpuppen dürften. Das Recht auf informationelle Selbstbestimmung der Betroffenen ist jedoch nur dann gewährleistet, wenn es auch ausgeübt werden kann. Eine barrierefreie Alternative wäre der Aufdruck von Barcodes auf den Rezepten. In diesem Fall erhielten die Versicherten nach wie vor ein Papierrezept; dessen Inhalt könnte durch Auslesen des aufgedruckten Barcodes für die Apotheken zu Abrechnungszwecken elektronisch sichtbar gemacht werden. Damit wäre das Ziel des elektronischen Rezeptes, wie es derzeit vorgesehen ist, erreicht, die Vorteile eines Papierrezeptes blieben aber erhalten. Insbesondere hätten die Versicherten ihre Rezepte ohne weiteres zur Hand, und eine Speicherung auf einem zentralen Server wäre nicht erforderlich.

- Eine hinreichend datenschutzkonforme Ausgestaltung des Verfahrens ist nicht in Sicht. Die Umsetzung der Zusage des Ministeriums für Arbeit, Gesundheit und Soziales NRW, Barcode-Rezepte in die Testung einzubeziehen, steht bisher noch aus.

11.2 Vertraulicher Umgang mit Patientendaten

Die Gewährleistung des Datenschutzes in der Arzt-Patienten-Beziehung spielt in Anfragen und Beschwerden eine immer größere Rolle. Von besonderer Bedeutung ist hierbei der vertrauliche Umgang mit medizinischen Daten.

Schwerpunkte der Beschwerden über Defizite beim Umgang mit medizinischen Daten sind häufig Unachtsamkeiten im Alltag:

Problematisch und wahrscheinlich nur schwer zu verhindern ist das Mithören der bei der Anmeldung notwendigen Daten wie beispielsweise Name und Kassenzugehörigkeit. Zu vermeiden ist aber die Abfrage weiterer Daten insbesondere zur Krankheit in Gegenwart weiterer Personen. Auch patientenbezogene Gespräche zwischen dem Praxispersonal dürfen nicht geführt werden, wenn Dritte sie verfolgen können. Bereits einfache Maßnahmen wie das selbstverständliche Schließen der Türen von Behandlungszimmern, die räumliche Trennung der Warteplätze vom Anmeldebereich oder Empfangstresen, die

Einrichtung von Diskretionszonen sowie die Sensibilisierung des Praxispersonals können bereits die Vertraulichkeit von Gesprächen wirksam verbessern.

Auch die Aufstellung der Monitore im Empfangsbereich ist immer wieder Gegenstand von Beschwerden. Durch falsche Positionierung kann die Kenntnisnahme von Patientendaten ermöglicht werden. Hier ist zu berücksichtigen, dass aufgrund der technischen Entwicklung bei den Flachbildschirmen eine Einsichtnahme in die Inhalte in weiten Sichtwinkeln möglich ist. Es ist deshalb darauf zu achten, dass neben einer günstigen Aufstellung zusätzliche Maßnahmen wie das Anbringen von Sichtschutzfolien oder die schnelle Aktivierung von Bildschirmschonern getroffen werden.

Patientenunterlagen müssen – auch bei Zwischenlagerung – so aufbewahrt werden, dass Dritte nicht die Möglichkeit des Zugriffs oder der Einsichtnahme haben können. Der Organisationsablauf ist deshalb so zu gestalten, dass während des gesamten Behandlungsprozesses eine Einsichtnahme durch Dritte wirksam verhindert wird.

Sehr grobe Verstöße gegen die Wahrung des Patientengeheimnisses sind die immer wieder gemeldeten Funde von Patientenunterlagen. Sie sind ein Zeichen mangelnder Sensibilität und schlechter Organisation. Datenschutzgerechte Vernichtungen von Patientenunterlagen sind mit leistungsfähigen Schreddern und seriösen Fachfirmen leicht möglich.

Ein ebenfalls immer wieder auftauchendes Problem sind Fehlleitungen beim Faxen von Patientenunterlagen. Um hier ein höheres Maß an Sicherheit zu erreichen, sollten die Hinweise auf der Homepage www.ldi.nrw.de beachtet werden.

➡ Zur Gewährleistung der Vertraulichkeit im Umgang mit Patientenunterlagen bedarf es häufig nur der Aufmerksamkeit und kleiner technischer oder organisatorischer Änderungen.

11.3 Der umorganisierte Konzern – ein bizarres Gebilde?

Es gibt zahlreiche Gründe für einen Konzern, seine Organisation zu verändern. Datenschutzrelevanz besitzen solche Änderungen, wenn dabei die Verarbeitung personenbezogener Da-

ten mit umgestellt wird. Das Finden von Datenschutz adäquaten Lösungen wird schwierig, wenn dabei besondere Datenarten, wie etwa medizinische Daten, betroffen sind.

- Wenn beispielsweise im Bereich von Versicherungen umorganisiert werden soll, so ist zu beachten, dass die von den Versicherten bei Vertragsabschluss abgegebenen Einwilligungs- und Schweigepflichtentbindungserklärungen nicht eine beliebige Verlagerung der Datenverarbeitung auf andere Stellen oder Gesellschaften mit abdecken würde. Ebenso scheidet aus, die betroffenen Versicherten lediglich über die geplanten Veränderungen zu informieren und ihnen ein Widerspruchsrecht einzuräumen. Es gibt keine Erlaubnisnorm, die es einem Konzern (oder einer Gesellschaft) gestatten würde, dass Fehlen eines Widerspruchs als wirksame Einwilligungs- und Schweigepflichtentbindungserklärung und damit als Rechtsgrundlage in die Umgestaltung der Datenverarbeitung zu werten. Dies gilt vor allem dann, wenn im Konzern medizinische Daten von Versicherten verarbeitet werden. Die von Versicherten bei Abschluss des Vertrages insoweit formularmäßig gegebene Einwilligungs- und Schweigepflichtentbindungserklärung in die Verarbeitung ihrer medizinischen Daten ist an die konkret benannte Gesellschaft innerhalb des Konzerns gebunden. Durch Umorganisation ist es daher nicht möglich, die Verarbeitung der medizinischen Daten auf eine andere Gesellschaft des Konzerns oder auf eine neu gestaltete rechtlich selbständige dritte Stelle zu übertragen.

- Zu bizarren Ergebnissen kann eine besondere Form der Umorganisation führen, wenn die Gesellschaft eines Konzerns personell völlig entkernt wird. Die Gesellschaft selbst ist nicht mehr in der Lage, die Daten ihrer Kunden zu verarbeiten. Auch die externe Verarbeitung durch Dritte (oder als Datenverarbeitung im Auftrag) könnte weder durch Weisungen begleitet, noch durch Kontrollen überprüft werden. Übrig bleibt lediglich eine leere Hülle, die praktisch nur noch von den Vorstandsvorsitzenden repräsentiert wird. Die Verarbeitung der Daten der Kundinnen und Kunden wird aufgeteilt auf dritte Stellen und dort fortgeführt. Die Betroffenen erfahren hierüber in der Regel nichts, da die bisherigen Briefbögen und sonstigen Vordru-

cke von den dritten Stellen unverändert genutzt werden. Diese treten immer im Namen der "leeren" Gesellschaft auf. Als Datenverarbeitung im Auftrag kann eine solche Verlagerung in der Regel nicht bezeichnet werden, da es tatsächlich keine Auftraggeberin mehr gibt. Eine Funktionsverlagerung scheidet in der Regel wegen der fehlenden Einwilligungs- und Schweigepflichtentbindungserklärung aus.

- Für einen Konzern wird dieses Datenschutzproblem noch besonders verschärft, wenn alle Gesellschaften in dieser Weise umstrukturiert werden und die dritten Stellen die übertragenen Teilbereiche für alle Gesellschaften gemeinsam wahrnehmen. Bei dieser Konstruktion wird faktisch die "verantwortliche Stelle" eingespart, die der zentrale Anknüpfungspunkt für die Gewährleistung des Datenschutzes nach dem Bundesdatenschutzgesetz ist. Ohne Personal in ausreichender Zahl ist eine "verantwortliche Stelle" nicht handlungsfähig.

  ➧ Der Grundsatz der Transparenz der Datenverarbeitung verlangt bei einer Umorganisation eines Konzerns in jedem Fall eine ausreichende Unterrichtung der betroffenen Kundinnen und Kunden über solche Veränderungen, damit diese entscheiden können, ob sie im Konzern und seinen Gesellschaften bleiben.

12 Beschäftigtendatenschutz

12.1 Übermäßige Beschäftigtenkontrolle in Unternehmen – nur Einzelfälle?

Über Bespitzelungen von Beschäftigten und Kamerawildwuchs in Unternehmen wurde bundesweit in den Medien berichtet.

In einem großen Lebensmittel-Discountunternehmen wurden Beschäftigte von Filialen systematisch durch Detekteien und andere Sicherheitsunternehmen überwacht. In deren Einsatzberichten fanden sich unter anderem Informationen über finanzielle Schwierigkeiten und Erziehungsprobleme der Beschäftigten sowie über ihr Verhalten bei der Arbeit und im Umgang miteinander. Die Aufträge hatten den Sicherheitsunternehmen, deren originäre Aufgabe sein sollte, Ladendiebstähle und deren Ursachen zu ermitteln, die rechtlich selbstständigen Vertriebsgesellschaften des Unternehmens erteilt. Die Aufklärung des Sachverhalts erforderte umfangreiche Ermittlungen der Datenschutzaufsichtsbehörden der Länder.

In Nordrhein-Westfalen waren acht Vertriebsgesellschaften des Unternehmens betroffen. Nach Abschluss der Ermittlungen wurden Bußgelder in Höhe von insgesamt 298.000 Euro verhängt. Die Vertriebsgesellschaften hatten in fünfzehn Fällen Berichte eines Sicherheitsunternehmens über Bespitzelungen von Beschäftigten rechtswidrig entgegengenommen und aufbewahrt beziehungsweise auch genutzt. Bei drei Vertriebsgesellschaften war nach Auswertung neun weiterer sogenannter Observationsberichte über heimliche Beobachtungen von Beschäftigten durch Kameraeinsatz festzustellen, dass die Verhaltensweisen der Betroffenen mehrere Tage lang mittels versteckt montierter Videokameras und damit rechtswidrig aufgezeichnet worden waren.

Insbesondere war eine Rechtfertigung der mit der Videoüberwachung verbundenen Eingriffe in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung der betroffenen Beschäftigten nicht ersichtlich. Sie hätte sich allenfalls aus überwiegenden schutzwürdigen Belangen des Arbeitgebers ergeben können. Das Bundesarbeitsgericht hat mit Urteil vom 27. März 2003 (2 AZR 51/02) die grundsätzliche Zulässigkeit einer Videoüberwachung zwar bestätigt, jedoch neben einem konkreten Tatverdacht den Nachweis einer "notwehrähnlichen

Lage" verlangt. Danach ist es erforderlich, dass der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzige verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.

Diese Voraussetzungen konnten in den überprüften Fällen nicht festgestellt werden. Es war nicht ersichtlich, dass konkrete, auf Tatsachen gestützte Diebstahls- oder Unterschlagungverdachtsmomente gegen einzelne oder mehrere Beschäftigte vorgelegen haben, bei denen als einziges Mittel zur Täterüberführung eine verdeckte Videoüberwachung in Frage gekommen wäre. Die vorliegenden Observationsberichtete sind daher unter Verletzung datenschutzrechtlicher Vorschriften und somit rechtswidrig erstellt worden. Sie hätten also ebenfalls nicht entgegengenommen, aufbewahrt oder genutzt werden dürfen. Die Vertriebsgesellschaften haben es sich selbst zuzuschreiben, dass vor Erteilung der Überwachungsaufträge offenbar keine datenschutzrechtlichen Überprüfungen erfolgt und weder Inhalte noch Grenzen der Tätigkeit des Sicherheitsunternehmens festgelegt worden sind.

Zu sanktionieren war auch, dass die Vertriebsgesellschaften ihrer Pflicht nicht nachgekommen waren, eigene betriebliche Datenschutzbeauftragte zu bestellen. Die Vertriebsgesellschaften unterliegen dieser Verpflichtung nach § 4f Bundesdatenschutzgesetz, weil automatisierte Verarbeitungen personenbezogener Daten sowohl bei den Datenverarbeitungsvorgängen in den Unternehmen selbst als auch in den insoweit mit zu berücksichtigenden nachgeordneten, rechtlich unselbstständigen Filialen anfallen. So wurde auch die Chance vertan, durch rechtzeitige Bestellung betrieblicher Datenschutzbeauftragter die sich aufdrängenden datenschutzrechtlichen Probleme betriebsintern zu lösen. Die Nichtbestellung betrieblicher Datenschutzbeauftragter wurde mit einem Bußgeld von je 10.000 Euro geahndet. Das Unternehmen hat nun ein Datenschutzgesamtkonzept erarbeitet, das von den Datenschutzaufsichtsbehörden derzeit geprüft wird.

Im Fall eines der größten Unternehmen der Fleisch verarbeitenden Industrie wurden in weiten Bereichen des Unternehmens an einem Standort unzulässige Videoüberwachungen von Beschäftigten an ihren Arbeitsplätzen festgestellt. Während die Videoüberwachung in den Sozial- und Umkleidebereichen damit begründet wurde, Diebstählen und

Vandalismus vorzubeugen, sollte sie in den Produktions- und Lagerbereichen zusätzlich gewährleisten, dass die hygiene- und lebensmittelrechtlichen Anforderungen sichergestellt werden. Die Firmenverantwortlichen waren sich jedoch über die Voraussetzungen und Grenzen der Videoüberwachung (siehe Bericht 2005 unter 4.4 und Bericht 2007 unter 4.5) nicht im Klaren. Eine dauerhafte verdachtsunabhängige Videoüberwachung von Beschäftigten ist nach der arbeitsgerichtlichen Rechtsprechung unverhältnismäßig und als ungerechtfertigter Eingriff in das grundrechtlich geschützte allgemeine Persönlichkeitsrecht der Beschäftigten zu werten. Zur Vermeidung einer unzulässigen ständigen Erfassung der Beschäftigten an ihren Arbeitsplätzen dürfen Videoüberwachungen, die zur Sicherung komplexer Betriebsabläufe in Ausnahmefällen gerechtfertigt sein können, nur so erfolgen, dass Kameraerfassungsbereiche, in denen sich Beschäftigte ständig aufhalten, elektronisch durch Verflimmerung oder Verpixelung ausgeblendet werden.

Unmittelbar nach einem unangemeldeten Informations- und Kontrollbesuch hat das Unternehmen reagiert und durch Abbau von Videokameras insbesondere in den Pausenräumen überwachungsfreie Zonen geschaffen. Zwischenzeitlich wurde auch hier ein Konzept über die aktuellen Videokamera-Standorte vorgelegt. Die unbestritten wichtigen Ziele, wie Beachtung der Hygiene-, Lebensmittel- und Tierschutzbestimmungen, Schutz vor Sabotagehandlungen und Diebstählen, sind durch die beschäftigtendatenschutzrechtlichen Erfordernisse nicht in Frage gestellt sind. Das Verfahren wurde mit einem Bußgeldbescheid gegen das Unternehmen über 80.000 Euro abgeschlossen.

Auch nach der jüngsten Rechtsprechung des Bundesarbeitsgerichts bleiben Videoüberwachungen von Beschäftigten nur ausnahmsweise und in engen Grenzen zulässig (Beschluss vom 26. August 2008 - 1 ABR 16/07 -). Vor Durchführung solcher Kontrollen empfiehlt es sich, ihre Voraussetzungen unter Beachtung dieser arbeitsrechtlichen Grundsätze in einer Betriebsvereinbarung mit dem Betriebsrat festzulegen.

➧ Persönlichkeitsrechte und Datenschutz sind insbesondere durch neue Techniken der Überwachung des Arbeitsverhaltens vielfältig bedroht. Diese und andere bedenkliche Entwicklungen verlangen nach gesetzlichen Regelungen zum Beschäftigtendatenschutz.

12.2 Keine Diagnoseangabe auf Rezepten – das muss auch die Beihilfestelle akzeptieren

Nach Beschwerden eines Arztes und zahlreicher Beihilfeberechtigter musste die Praxis der Beihilfegewährung einer Bezirksregierung unter die Lupe genommen werden. Ihre Beihilfestelle hatte die Erstattung eines Arzneimittels mehrfach mit dem Hinweis auf die in dem Privatrezept fehlende Diagnose verweigert. Den Betroffenen kamen hier zu Recht Bedenken.

Nach Einschaltung des Finanzministeriums NRW konnte die Angelegenheit geklärt und der Mangel abgestellt werden. Bei der Beihilfebearbeitung dürfen keine Diagnoseangaben auf den von den Beihilfeberechtigten eingereichten Rezepten verlangt werden. Eine Rechtsgrundlage hierfür besteht nicht. Eine Indikation lässt sich der in der Regel ebenfalls vorgelegten ärztlichen Rechnung entnehmen. Sofern die Beihilfestelle ein Rezept nicht anerkennen will, wäre zur Klärung medizinischer Zweifelsfragen der amtsärztliche Dienst einzuschalten.

Das Finanzministerium NRW hat den Beihilfestellen des Landes verdeutlicht, dass sich eine Forderung nach einer nachträglichen ergänzenden Angabe der vorliegenden Diagnosen auf einem Rezept bereits aus Gründen des Datenschutzes verbietet. Da fachliche Weisungen des Finanzministeriums NRW erfahrungsgemäß auch im Bereich der kommunalen Beihilfestellen bekannt werden, kann davon ausgegangen werden, dass auch dort künftig datenschutzkonform verfahren wird, sollte dies bisher nicht der Fall gewesen sein.

➡ Auf ärztliche Rezepte gehören keine Diagnoseangaben. Beihilfestellen dürfen die Kostenerstattung nicht davon abhängig machen, dass solche Angaben auf ärztlichen Rezepten vermerkt werden.

12.3 Beurteilungsdaten von Praktikantinnen und Praktikanten im Internet

"Wer sollte dieses Mädchen – 16 Jahre alt – noch einstellen?"

Mit diesem Hinweis wurde in einer Beschwerde auf die Homepage-Veröffentlichung eines EDV-Unternehmens aufmerksam gemacht. Dort wurde eine Praktikantin mit Angabe ihres Namens sowie mit kurzem

Lebenslauf und Lichtbild wie folgt beurteilt: "C.R. wirkte leider (zu) häufig sehr übermüdet und unkonzentriert. Viele von uns vermittelten Dinge sind einfach nicht hängengeblieben. Falls dieser Beruf gewählt wird, raten wir zu sehr viel mehr Arbeit und Lernen mit dem PC, anstelle damit zu spielen." Veröffentlicht wurden auch die Personaldaten der ehemaligen Praktikantinnen und Praktikanten des Betriebs. Die Veröffentlichungen erfolgten, ohne dass die Betroffenen darin eingewilligt hatten.

Das Unternehmen hat nach Einleitung der datenschutzrechtlichen Prüfung die Daten von seiner Homepage zügig entfernt und zugesagt, dass künftig jede Praktikantin und jeder Praktikant selbst über die Veröffentlichung der Daten zur eigenen Person entscheiden kann.

➧ Betroffene sollten sich sehr genau überlegen, ob sie ihre Personaldaten veröffentlicht sehen wollen. Ausbildungsbetriebe müssen in jedem Fall daran denken, dass die Wirksamkeit einer Einwilligung auch von der Einsichtsfähigkeit der Jugendlichen abhängt, die Risiken einer solchen Veröffentlichung zu überblicken.

12.4 "Schlechte Noten für Schulleiterin"

Ein Hauptpersonalrat hat auf einen so überschriebenen Zeitungsbericht aufmerksam gemacht, in dem ausführlich aus dem Entwurf eines Qualitätsberichts über eine Schule zitiert wurde. Durch die Bekanntgabe wurde das Recht auf informationelle Selbstbestimmung der Schulleitung verletzt. Zu prüfen war, wie diese Beschäftigtendaten an die Presse gelangen konnten und wie solche Vorfälle für die Zukunft verhindert werden können.

Bei Überprüfungen des Qualitätsstandards von Schulen sind die Vorschriften der Verordnung zur Qualitätsanalyse an Schulen (QA-VO) zu beachten. Sie erlauben keine Bewertung einzelner Lehrkräfte (§ 3 Abs. 4 Satz 4 QA-VO). Angaben dürfen nur gruppenbezogen in aggregierter Form erfolgen. Ein Personenbezug ist damit ausgeschlossen. Anders verhält es sich jedoch in Bezug auf die Schulleitung. Für sie enthält die Qualitätsanalyse-Verordnung keine vergleichbare Einschränkung. Dies bedeutet allerdings nicht, dass damit etwa Leistungs- oder sonstige Qualifikationsangaben über Mitglieder der Schulleitung frei verarbeit-

bar sind und solche Daten in einem Qualitätsbericht ohne Einschränkungen dokumentiert werden dürfen. Vielmehr gilt auch insoweit der das Datenschutzrecht tragende Grundsatz des Verbots der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt.

Zur Wahrung ihres Rechts auf informationelle Selbstbestimmung ist somit den Mitgliedern der Schulleitung vor einer Veröffentlichung des Qualitätsberichts gemäß § 3 Abs. 9 QA-VO sowie bei einem Antrag auf Informationszugang nach § 4 Informationsfreiheitsgesetz NRW mit folgender Maßgabe Gelegenheit zur Stellungnahme zu geben: Willigen alle Mitglieder der Schulleitung in die Bekanntgabe der in dem Qualitätsbericht über sie gespeicherten Informationen ein, stehen der Veröffentlichung des Berichts beziehungsweise der Gewährung eines Informationszugangs keine Bedenken entgegen. Besteht die Schulleitung aus zwei Personen, müsste, falls ein Mitglied in die Bekanntgabe der eigenen personenbezogenen Daten nicht einwilligt, auch von einer Bekanntgabe der Daten des anderen Mitglieds abgesehen werden. Nur so kann eine Identifizierbarkeit der erstgenannten Person vermieden werden.

Die Bezirksregierung hat diese Hinweise aufgegriffen und zum konkreten Fall mitgeteilt, wegen der Vielzahl der in Frage kommenden Beschäftigten in der Schule, beim Schulträger und bei der Bezirksregierung erschienen Ermittlungen zur Quelle der Presseveröffentlichung nicht Erfolg versprechend. Auf welchem Wege der Bericht in die Zeitung gelangt war, ließ sich damit nicht mehr zweifelsfrei feststellen.

Die Problematik wurde auch mit dem Ministerium für Schule und Weiterbildung NRW erörtert. Erreicht wurde folgendes datenschutzrechtlich akzeptables Verfahren: Im Zusammenhang mit der Veröffentlichung von Qualitätsberichten sowie bei Anträgen auf Informationszugang ist den Bezirksregierungen aufgegeben worden, nach einem Ablaufplan vorzugehen. Zu veröffentlichen sind nur Qualitätsberichte in der endgültigen Form. Die Dezernate 4Q sind nochmals darauf hingewiesen worden, wie entsprechend den aufgezeigten Erfordernissen in Bezug auf das besonders sensible Qualitätskriterium "Führungsverantwortung der Schulleitung" zu verfahren ist. Eine Information der Schulen wird dadurch erreicht, dass das Vorwort zu den Qualitätsberichten um Hinweise zu den Belangen des Datenschutzes ergänzt wird. Dabei wird noch einmal ausdrücklich klargestellt, dass eine Veröffentli-

chung des Qualitätsberichtes durch die Schule erst nach Zustimmung durch die Schulkonferenz erfolgen darf (§ 3 Abs. 9 Satz 1 QA-VO).

➧ Bereits bei der Erstellung von Qualitätsberichten in Schulen ist auf die Persönlichkeitsrechte aller Betroffenen zu achten. Folgen einer möglichen Veröffentlichung sind zu bedenken.

12.5 Mitwirkung der Beschäftigten – A und O des betrieblichen Eingliederungsmanagements

Länger erkrankten Beschäftigten soll das betriebliche Eingliederungsmanagement eine Wiederaufnahme der Arbeit ermöglichen und erneuten Erkrankungen vorbeugen. Firmen und Behörden müssen klären, wie eine Arbeitsunfähigkeit überwunden und Fehlzeiten verringert werden können. Die insoweit in Frage kommenden Maßnahmen bedürfen dabei der Zustimmung der Beschäftigten.

Ein betriebliches Eingliederungsmanagement (BEM) ist nach § 84 Abs. 2 Sozialgesetzbuch Neuntes Buch (SGB IX), vorgesehen, wenn Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind. Ausschließlich mit Zustimmung und Beteiligung der betroffenen Person klärt die Arbeitgeberin oder der Arbeitgeber nach der gesetzlichen Festlegung sodann mit der zuständigen Interessenvertretung, bei schwerbehinderten Menschen außerdem mit der Schwerbehindertenvertretung, wie die Arbeitsunfähigkeit möglichst überwunden, erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann.

Die betroffene Person oder ihre gesetzliche Vertretung müssen zuvor auf Art und Umfang der für dieses Verfahren erhobenen und verwendeten Daten hingewiesen werden. Insoweit ist vor Durchführung der Maßnahmen im Rahmen eines BEM eine umfassende Aufklärung erforderlich. Auch müssen die einzelnen Verfahrensschritte datenschutzgerecht ausgestaltet sein.

In diesem Zusammenhang wurden den Landschaftsverbänden Rheinland und Westfalen-Lippe zu ihren in einer Broschüre aufgelegten "Handlungsempfehlungen zum Betrieblichen Eingliederungsmanagement" zahlreiche datenschutzrechtliche Korrekturen empfohlen. Deren

Umsetzung ist deshalb wichtig, weil viele Unternehmen, aber auch Behörden und Dienststellen diese Handlungsempfehlungen zur Wahrung der gesetzlich gebotenen Wiedereingliederungsmaßnahmen zu Rate ziehen.

Im Einzelnen war insbesondere auf folgende Erfordernisse hinzuweisen: Die Einwilligung in die mit einem BEM verbundenen Verarbeitungen von Daten erfordert die rechtzeitige vorherige Information der betroffenen Person ("informed consent"), wobei unter Darlegung der Rechtsfolgen darauf hinzuweisen ist, dass eine Einwilligung auch mit Wirkung für die Zukunft widerrufen werden kann. In den Handlungsempfehlungen wurde nicht darüber aufgeklärt, welche Informationen über das BEM in die Personalakte aufzunehmen sind. Hierüber muss die betroffene Person bereits im Rahmen des Erstkontakts informiert werden.

Empfohlen wurden ferner datenschutzrechtlich korrekte Hinweise zu dem Informationsaustausch zwischen der betroffenen Person und der Betriebsärztin oder dem Betriebsarzt. Es geht nicht an, dass der Hinweis "Ärztliche Diagnosen sowie Daten zur Gesundheitsprognose sind von dem betroffenen Mitarbeiter mit dem Betriebsarzt zu erörtern" den rechtlich unzutreffenden Eindruck erweckt, eine betroffene Person sei zur Offenbarung ihrer höchstpersönlichen Gesundheitsdaten an eine Betriebsärztin oder einen Betriebsarzt verpflichtet. Neben weiteren aufklärenden Informationen wurde der Hinweis empfohlen, dass ärztliche Diagnosen sowie Daten zur Gesundheitsprognose von der betroffenen Person mit der Betriebsärztin oder dem Betriebsarzt erörtert werden können, soweit dies unabweisbar erforderlich ist, und von dieser oder diesem nicht ohne Einverständnis der betroffenen Person (Schweigepflichtentbindungserklärung) anderen am BEM Beteiligten zugänglich gemacht werden dürfen. Datenschutz und betriebsärztliche Schweigepflicht müssen auch im Rahmen des BEM strikt beachtet werden. Unbefugte Offenbarungen sind strafbewehrt (§ 203 Abs. 1 Nr. 5, Abs. 2 Nr. 1 bis 3 Strafgesetzbuch, § 120 Abs. 2 Betriebsverfassungsgesetz, § 155 Abs. 1 Sozialgesetzbuch Achtes Buch). Hierüber dürfen die Beteiligten eines BEM nicht im Unklaren gelassen werden.

Die Beteiligung des zuständigen Personal- oder Betriebsrats und gegebenenfalls der Schwerbehindertenvertretung bei einem in Frage kommenden BEM ist nach § 84 Abs. 2 Satz 1 SGB IX an die Zustimmung und Beteiligung der betroffenen Person gebunden. Aus der gesetzli-

chen Regelung folgt allein, dass in den Fällen, in denen mit Zustimmung der betroffenen Person der Betriebs- oder Personalrat und gegebenenfalls die Schwerbehindertenvertretung beteiligt worden sind, diesen nur die vereinbarten Maßnahmen und die sich hieraus für die Arbeitgeberin oder den Arbeitgeber ergebenden Pflichten mitzuteilen sind, um deren Erfüllung überwachen zu können. Die gegenteilige, auch von den Landschaftsverbänden vertretene Auffassung, die Interessenvertretungen benötigten die Informationen über Arbeitsunfähigkeitszeiten zur Ausübung ihrer gesetzlichen Überwachungsaufgabe nach § 93 SGB IX, lässt unberücksichtigt, dass eine bloße Aufgabenzuweisungsnorm nicht zugleich eine Befugnisregelung zur Bekanntgabe personenbezogener Daten darstellt. Eine Beteiligung der Interessenvertretungen erfolgt nicht automatisch mit der Möglichkeit des Widerspruchs der betroffenen Person, sondern sie hängt von ihrer vorherigen freien Zustimmung ab. Den Landschaftsverbänden wurde daher empfohlen, ergänzend darüber zu informieren, dass die Betroffenen sich selbst zwecks entsprechender Unterstützung an den Betriebs- oder Personalrat und gegebenenfalls an die Schwerbehindertenvertretung wenden können. Einen auf Mitteilung der für ein BEM maßgeblichen Ausfallzeiten erhobenen Unterrichtungsanspruch von Personalvertretungen haben das Verwaltungsgericht Aachen (Beschluss vom 25. September 2008 - 16 K 836/08.PVL -) sowie das Verwaltungsgericht Düsseldorf (Beschluss vom 20. Oktober 2008 - 34 K 3001/08. PVL -) im Ergebnis ebenso abgelehnt.

Ferner dürfen keine Unterlagen mit medizinischen Daten bei der mit der Durchführung des BEM beauftragten Einzelperson oder einem Integrationsteam verbleiben. Eine solche Praxis widerspräche den datenschutzrechtlichen Erfordernissen. Diese Personen unterliegen regelmäßig nicht der ärztlichen Schweigepflicht. Da es für das Gelingen eines BEM entscheidend ist, dass ein Unternehmen oder eine Behörde garantiert, dass medizinische Daten, die ärztlicherseits nur in unumgänglich erforderlichem Umfang auf Grund einer Schweigepflichtentbindungserklärung der betroffenen Person ausschließlich den Beteiligten des BEM zur Kenntnis gelangen, sollte es genauso selbstverständlich sein, dass die Speicherung sämtlicher sensibler medizinischer Daten abgeschottet im betriebsärztlichen Bereich erfolgt.

Schließlich war besonders darauf hinzuweisen, dass eine Mitwirkungsverpflichtung der jeweils betroffenen Beschäftigten zur Teilnahme an

Maßnahmen eines BEM auch nicht auf eine Dienst- oder Betriebsvereinbarung gestützt werden kann. Handlungsempfehlungen dieses Inhalts können zu der irrigen Auffassung führen, eine solche Verpflichtung ließe sich durch derartige Vereinbarungen begründen.

Zu begrüßen ist die Bereitschaft der Landschaftsverbände, diese Hinweise nunmehr im Wesentlichen zu berücksichtigen und in die Handlungsempfehlungen aufzunehmen. Dies muss allerdings zeitnah erfolgen. Von einer weiteren Verbreitung der Handlungsempfehlungen in der bisherigen Broschüren-Fassung sollte zur Vermeidung von Datenschutzverstößen abgesehen werden. Da die Handlungsempfehlungen auch im Internet abrufbar sind, können interessierte Stellen die abschließend zu überarbeitende Fassung dort abrufen.

➡ In den "Handlungsempfehlungen zum Betrieblichen Eingliederungsmanagement" der Landschaftsverbände Rheinland und Westfalen-Lippe ist deutlich darauf hinzuweisen, dass eine Mitteilung der Arbeitsunfähigkeitszeiten an die Interessenvertretungen nur mit schriftlicher Einwilligung der Betroffenen zulässig ist.

12.6 Keine personenscharfen Beschäftigtendaten an Ratsausschuss

Eine Kommunalverwaltung wurde vom Rat beauftragt, dem Haupt- und Finanzausschuss halbjährlich einen personenbezogenen Bericht mit bestimmten Angaben über die Beschäftigungsverhältnisse ihrer Mitarbeiterinnen und Mitarbeiter sowie die jeweiligen Personalkosten vorzulegen. Begründet wurde dies damit, dass es nur auf der Grundlage einer transparenten Kostenstruktur möglich sei, Organisations- und Personalentwicklungsentscheidungen zu treffen und eine ausgewogene Finanzsteuerung vorzunehmen. Nach der Struktur des Neuen Kommunalen Finanzmanagements (NKF) sei ein umfassendes Berichtswesen und Controlling verpflichtend.

Im Hinblick auf die grundsätzliche Bedeutung der Anfrage wurde das Innenministerium NRW eingeschaltet. Es hat unter anderem darauf verwiesen, dass durch das mit Gesetz vom 14. Mai 2004 eingeführte NKF das Wirtschaften in den Gemeinden transparenter werde. Dadurch würden nicht nur verwaltungsintern, sondern auch für den Rat neue

Steuerungspotentiale eröffnet, die den Gemeinden eine effizientere Wahrnehmung ihrer Aufgaben ermöglichten. Im Rahmen der Beschlussfassung über die Haushaltssatzung, den Jahresabschluss und den Gesamtabschluss würden daher dem Rat jeweils die gesetzlich vorgesehenen haushaltswirtschaftlichen Unterlagen ohne personenbezogene Beschäftigtendaten vorgelegt. Die mit der Einführung des NKF einhergehenden Möglichkeiten der Neuen Steuerung verlangten zwar ein umfassendes Berichtswesen und Controlling, jedoch würden durch das NKF dazu keine den Datenschutz berührenden Vorgaben getroffen. Die Regelung in § 18 Gemeindehaushaltsverordnung NRW gebe zum Beispiel den Gemeinden die Befugnis, die Kosten- und Leistungsrechnung nach ihren Bedürfnissen zu führen. Die Gemeinde entscheide dabei aber eigenverantwortlich über den Umfang und die weitere Ausgestaltung der Kosten- und Leistungsrechnung im Rahmen ihrer kommunalen Selbstverwaltung sowie über die entsprechende Unterrichtung des Rates. Im Rahmen des NKF bestünden keine Notwendigkeiten, personenscharfe Beschäftigtendaten an den Rat zu übermitteln.

Diese fachliche Klarstellung ist aus datenschutzrechtlicher Sicht zu begrüßen. Zur Erreichung der Ziele des NKF sind offensichtlich Berichte an die zuständigen kommunalen Ausschüsse ausreichend, die lediglich aggregierte Daten aufweisen. Hieraus lassen sich strukturelle Entwicklungen im Personalbereich ebenfalls erkennen, ohne dass ein umfassendes Berichtswesen und Controlling in Frage gestellt ist.

- Es wäre zu begrüßen, wenn sich Inhalt und Umfang von Kontroll- und Informationsrechten unmittelbar aus den Regelungen des Kommunalen Finanzmanagementgesetzes NRW herleiten ließen.

12.7 Probleme bei der Mitversteuerung von Firmenrabatten

Ein Versicherungskonzern wollte die Vertragsdaten seiner Beschäftigten, die bei Konzerntochterunternehmen Versicherungsverträge zu günstigen Konditionen abgeschlossen hatten, für Zwecke der Lohnsteuerabrechnung erheben. Über die Modalitäten der Erhebungen waren sich Geschäftsführung und Betriebsräte nicht einig.

Die Beschäftigten des Versicherungskonzerns haben die Möglichkeit, Rabatte auf Sach-, Unfall-, Haftpflicht-, Kraftfahrt- und Rechtsschutzversicherungen in Anspruch zu nehmen. Die Vorteile, die durch solche Rabattgewährungen entstehen, werden steuerrechtlich wie zusätzliches Einkommen behandelt mit der Folge, dass dafür Lohnsteuer zu entrichten ist. Dieses zusätzliche Einkommen unterliegt der Lohnsteuer, wenn das Beschäftigungsunternehmen weiß oder erkennen kann, dass derartige Vergütungen erbracht werden (§ 38 Abs. 1 Satz 3 Einkommensteuergesetz (EStG)). Dies ist insbesondere in verbundenen Unternehmen im Sinne des § 15 Aktiengesetz wie in einem Versicherungskonzern anzunehmen.

Nach § 38 Abs. 4 Satz 3 EStG ist die Arbeitnehmerin oder der Arbeitnehmer selbst verpflichtet, dem Beschäftigungsunternehmen die von einem dritten Unternehmen gewährten Bezüge am Ende des Lohnzahlungszeitraum anzugeben. Werden hierbei keine oder erkennbar falsche Angaben gemacht, hat das Beschäftigungsunternehmen dies dem Betriebstättenfinanzamt anzuzeigen.

Dieser Vorschrift wollte das Beschäftigungsunternehmen durch Einrichtung eines automatisierten konzerninternen Datentransfers Rechnung tragen. Da § 38 EStG jedoch keine gesetzliche Grundlage für den geplanten konzerninternen Datentransfer darstellt und auch keine andere Befugnisregelung vorliegt, wurde der Versicherungskonzern darüber unterrichtet, dass eine solche Übermittlung nur mit Einwilligung der Beschäftigten oder auf Grund einer Betriebsvereinbarung zulässig wäre.

➡ Zusammen mit den Betriebsräten hat sich der Versicherungskonzern zwischenzeitlich über das Verfahren der Versteuerung von Firmenrabatten verständigt und eine entsprechende Konzernbetriebsvereinbarung abgeschlossen.

12.8 Heimliches Mithören bei telefonischen Interviews ist grundsätzlich unzulässig

Durch mehrere Beschwerden wurde bekannt, dass bei Markt- und Meinungsforschungsinstituten Telefongespräche zum Zwecke der Qualitätskontrolle ohne Kenntnis der mit den Inter-

views betrauten Beschäftigten und zum Teil auch ohne Wissen der angerufenen Personen mitgehört werden.

Diese Praxis des heimlichen Mithörens, die der vom Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM) herausgegebenen "Richtlinie für telefonische Befragungen" entspricht, berührt nicht nur den Schutzbereich des Art. 10 Grundgesetz. Sie verstößt zudem gegen Datenschutzrecht und könnte sogar strafrechtlich relevant werden (§ 201 Strafgesetzbuch: Verletzung der Vertraulichkeit des Wortes). Begründet wird das von den Beschäftigten unbemerkte Mithören telefonischer Interviews mit dem Zweck einer umfassenden, der auftraggebenden Stelle geschuldeten Qualitätskontrolle. Auch wegen des damit einhergehenden permanenten Überwachungsdrucks zu Lasten der Betroffenen drängen Datenschutzaufsichtsbehörden jedoch seit längerem auf eine Überarbeitung dieser Richtlinien.

Die Interviewerinnen und Interviewer müssen grundsätzlich vorab darin eingewilligt haben, dass ihre Gespräche mitgehört werden. Pauschale, unfreiwillig erteilte Einwilligungen der Beschäftigten bei Abschluss ihres Arbeitsvertrages in unbegrenzte Kontrollen durch Mithören ihrer Telefoninterviews sind allerdings unwirksam und unzulässig. Zudem sind sie vor jeder Maßnahme nochmals zu informieren. Die Interviews sollten stets erst einmal offen mitgehört werden. Parallel dazu oder alternativ sind auch Testanrufe (fingierte Anrufe von Supervisoren) möglich. Nur wenn diese Maßnahmen nicht den gewünschten Erfolg der Qualitätssicherung erzielten, wäre ausnahmsweise ein verdecktes Mithören zulässig. Auch hierüber müssen die Betroffenen allerdings vorab unter Eingrenzung des Kontrollzeitraumes informiert werden.

Die Datenschutzaufsichtsbehörden beraten derzeit geeignete Schritte, um eine datenschutzkonforme Fassung der ADM-Richtlinie zu erwirken.

- Ein datenschutzkonformes Verfahren erfordert neben den Informationen für die Interviewerinnen und Interviewer auch, dass die angerufenen Personen vor Gesprächsbeginn (zum Beispiel durch eine automatische Ansage) auf die Möglichkeit des Mithörens hingewiesen werden. Ihre Einwilligung kann beispielsweise durch das Drücken einer bestimmten Telefontaste erfolgen.

13 Finanzen

13.1 Das Recht der Steuerpflichtigen auf Akteneinsicht – künftig ohne Ermessen der Finanzbehörden

Der Vergangenheit wird die oft geübte Praxis der Finanzverwaltung angehören müssen, Steuerpflichtigen ihr Informationsrecht über die zu ihrer eigenen Person gespeicherten Daten aus Ermessensgründen einzuschränken oder gar zu verwehren.

Begründet wurden Auskunftsverweigerungen bisher damit, der Bundesgesetzgeber habe das steuerliche Verfahren in der Abgabenordnung abschließend geregelt und dort durch "absichtsvolles Unterlassen" bewusst auf eine Einsichts- oder Auskunftsregelung verzichtet. Nun hat das Bundesverfassungsgericht mit Beschluss vom 10. März 2008 (1 BvR 2388/03) im Fall eines gegen das ehemalige Bundesamt für Finanzen erhobenen Auskunftsanspruchs eines Steuerpflichtigen entschieden, dass diese Argumentation nicht mehr länger haltbar ist, und dem Betroffenen grundsätzlich einen Auskunftsanspruch nach § 19 Bundesdatenschutzgesetz (BDSG) zugestanden.

Damit ist die von den Datenschutzbeauftragten seit langem geforderte Klarstellung erreicht, den Betroffenen ihre datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen (siehe Entschließung vom 27./28. März 2003, abgedruckt im Bericht 2005 im Anhang).

Durch eine im Entwurf des Jahressteuergesetzes 2009 zunächst enthaltene Änderung der Abgabenordnung, die ein Auskunftsrecht für Betroffene nach Maßgabe des § 19 BDSG vorgesehen hat, sollte die Entscheidung des Bundesverfassungsgerichts umgesetzt werden. Der aktuelle Entwurf des Jahressteuergesetzes weist diese Änderung jedoch nicht mehr auf.

➡ Von einer gesetzlichen Klarstellung, dass ein datenschutzrechtlicher Auskunftsanspruch auch im steuerlichen Verfahren zu berücksichtigen ist, sollte keineswegs abgesehen werden. Auch die sonstigen Rechte der Betroffenen, insbesondere das Recht auf Löschung und Sperrung von Daten, sind bisher nicht geregelt. Das Finanzministerium NRW ist aufgerufen, sich hierfür einzusetzen.

13.2 Zentrale Steuerdatei – weiter im Aufbau

Bereits während der Vergabe der neuen persönlichen Steueridentifikationsnummer (Steuer-ID) an alle Einwohnerinnen und Einwohner (siehe Bericht 2005 unter 19.1) wurde mit dem Jahressteuergesetz 2008 (Bundesgesetzblatt I S. 3150) eine Erweiterung der zentralen Steuerdatei bei dem Bundeszentralamt für Steuern um zusätzliche, teilweise sensible Daten beschlossen.

Auf der Grundlage des Steueränderungsgesetzes 2003 wurde im Jahr 2008 eine bundesweit geltende Steueridentifikationsnummer (Steuer-ID) und die Speicherung einer Vielzahl weiterer Daten (zum Beispiel: Familiennamen, frühere Namen, Vornamen, Tag der Geburt, Anschrift) in einer zentralen Steuerdatei eingeführt. Hiermit sind für Steuerpflichtige die erheblichen datenschutzrechtlichen Risiken eines zentralen Einwohnerregisters beim Bundesamt für Finanzen und eines einheitlichen Personenkennzeichens (siehe hierzu Bericht 2005 unter 19.1) verbunden.

Jetzt geht es noch einen Schritt weiter: Das Jahressteuergesetz 2008 sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren ab 2011 vor. Es erweitert die zentrale Steuerdatei etwa um Angaben zur Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID sowie über Steuerklassen. Der durch die Vergabe der Steuer-ID an alle Steuerpflichtigen entstehende Datenpool erhält damit eine neue Dimension. Zwar sind die Lohnsteuerabzugmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank wirft aber erhebliche datenschutzrechtliche Probleme auf. Die umfangreiche Datenspeicherung auf Vorrat berücksichtigt den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz nicht. In den zentralen Datenbestand sollen die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Daten werden zudem bundesweit annähernd vier Millionen Firmen und Unternehmen zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur eine autorisierte Arbeitgeberin oder ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist, wie dies sichergestellt werden kann.

Die Datenschutzbeauftragten haben auf diese und andere Kritikpunkte in ihrer Entschließung vom 25./26. Oktober 2007 (Abdruck im Anhang) hingewiesen.

- Die Vergabe der Steuer-ID führt zu einer vollständig neuen Dimension der Datenverarbeitung. Neben dem Risiko einer unzulässigen Datenspeicherung auf Vorrat besteht insbesondere Unklarheit, wie sichergestellt wird, dass Lohnsteuerabzugsmerkmale nur durch autorisierte Arbeitgeberinnen und Arbeitgeber abgerufen werden können.

13.3 "KONSENS" – noch nicht mit dem Datenschutz

Mit einem neuen Projekt wollen die Finanzverwaltungen der Länder für das Besteuerungsverfahren eine einheitliche Software einsetzen. Allerdings sind hierfür die gesetzlichen Grundlagen noch unklar.

Das Projekt KONSENS, abgeleitet aus den Wörtern koordinierte neue Software-Entwicklung der Steuerverwaltung, geht auf ein am 01. Juli 2007 in Kraft getretenes Verwaltungsabkommen zurück. Darin haben sich die Länder verpflichtet, die Beschaffung, arbeitsteilige Entwicklung, Pflege, Finanzierung und den Einsatz einheitlicher Software für das Besteuerungsverfahren sowie für das Steuerstraf- und Bußgeldverfahren zu realisieren. Es löst das Verwaltungsabkommen auf dem Gebiet der Informationstechnik im Besteuerungsverfahren "Projekt FISCUS" ab.

Entwicklungsstandorte sind in Baden-Württemberg, Bayern, Hessen, Niedersachsen und Nordrhein-Westfalen eingerichtet. Gemeinsam mit dem Bund tragen diese Länder die Verantwortung für die Umsetzung des Vorhabens KONSENS.

Das Land Nordrhein-Westfalen ist im Projekt KONSENS für das Vorhaben Risikomanagement zuständig. Vor dem Hintergrund des verfassungsrechtlichen Gebotes der gleichmäßigen Steuererhebung will die Finanzverwaltung das Risiko für einen Steuerausfall auf Basis der digital verfügbaren Steuerdaten automatisiert bewerten. Durch eine risikoorientierte Bearbeitungssteuerung – bis hin zur vollautomatischen Bearbeitung risikoarmer Fälle – sollen gezielt Betrugsfälle vermieden

oder zumindest aufgedeckt werden. Fraglich ist allerdings, nach welchen Kriterien (etwa Umsatz- und Gewinngrößen, Erklärungs- und Zahlungsverhalten Steuerpflichtiger) Risikoindikatoren eingesetzt werden und ob die Sachbearbeitung bei verstärktem Einsatz solcher Systeme überhaupt noch steuernden Einfluss auf den einzelnen Veranlagungsfall nehmen kann. Vor allem aber lassen sich der Abgabenordnung Verfahrensvoraussetzungen für ein Risikomanagement nicht entnehmen. Solche müssen dem Grunde nach gesetzlich festgelegt werden, wie dies der Gesetzgeber etwa für das Kreditgewerbe bereits geregelt hat.

Hohe datenschutzrechtliche Relevanz hat das geplante Data-Warehouse-Verfahren. Allgemein werden in einem Data-Warehouse alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. In einem gemeinsamen Projekt verfolgen nun die Länder das Ziel des Aufbaus eines einheitlichen, umfassenden und tagesaktuellen Data-Warehouses zur Informationsgewinnung für steuerrelevante Entscheidungen. Mittel- bis langfristig sollen die bestehenden Auswertungen der bisherigen Auswertungsverfahren durch eine neue technische Basis ersetzt werden.

Zu einem solchen Projekt ist auf die in der Entschließung vom 14./15. März 2000 (siehe hierzu Bericht 2001 im Anhang) betonten Grundanforderungen für ein Data-Warehouse-Verfahren hinzuweisen. Im Bereich der Steuerverwaltung dürfen Steuerdaten nach dem grundrechtlichen Gebot der Zweckbindung nur im Rahmen der gesetzlich zugelassenen Zwecke verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data-Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine unzulässige Speicherung auf Vorrat ohne Zweckbindung dar.

Darüber hinaus bleibt offen, inwieweit die Steuerdaten der Steuerpflichtigen innerhalb dieses Verfahrens für verschiedene Auswertungszwecke genutzt werden. Zu mehreren Gesichtspunkten eines Verfahrensauftrags, der den Aufbau eines umfassenden Auswertungssystems zur Informationsgewinnung und Darstellung im Rahmen des Vorhabens KONSENS konkretisiert, wurde das Finanzministerium NRW um Stellungnahme gebeten. Eine überzeugende Darlegung, wie die aufgezeigten datenschutzrechtlichen Erfordernisse berücksichtigt werden sollen, steht bisher aus.

- Eingriffsbefugnisse auf Grund eines Risikomanagements bedürfen normenklarer gesetzlicher, dem Verhältnismäßigkeitsgrundsatz genügender Regelungen. Die Steuerpflichtigen müssen erkennen können, wer was wann bei welcher Gelegenheit über sie weiß. Die Abgabenordnung enthält dazu nichts. Data-Warehouse-Verfahren sind besonders problematisch.

14 Verkehr und Umwelt

14.1 "Die Fahrscheine bitte" – übereifrige Kontrollen im Nahverkehr

Im öffentlichen Nahverkehr werden bei Abonnements heute in der Regel Chipkarten als Fahrberechtigung ausgegeben. Bei Kontrollen in den Fahrzeugen werden diese automatisch ausgelesen. Probleme treten auf, wenn dies – wie in der Praxis häufig – technisch nicht funktioniert.

Bei einer Fahrgastkontrolle hatte der Kontrolleur eines Verkehrsunternehmens die Chipkarte einbehalten, weil sie im Prüfgerät nicht ausgelesen werden konnte. Außerdem wurden Daten des Fahrgastes erhoben. Parallel zur Tätigkeit der LDI NRW war bereits eine zivilrechtliche Klage angestrengt worden. Das zuständige Gericht stellte in seinem Urteil fest, dass die erstmalige mangelnde Auslesbarkeit einer elektronischen Fahrberechtigung keinen Anlass gebe, die Chipkarte einzuziehen und es dem Fahrgast zu überlassen, sich dann ohne sein Ticket – mit zusätzlichen Kosten – zum Kundencenter des Verkehrsunternehmens zu bemühen. Vielmehr genüge beim Antreffen eines Fahrgastes mit einer nicht auslesbaren Chipkarte der Hinweis auf die mangelnde Auslesbarkeit mit einer angemessenen Fristsetzung zur Erneuerung der Fahrberechtigung bei der zuständigen Geschäftsstelle. Zulässig sei jedoch die Erhebung der Angaben zur Feststellung der Person, um überprüfen zu können, ob der Fahrgast mit einer gültigen Fahrberechtigung gefahren sei. Das Beförderungsunternehmen änderte zwar seine Verfahrensweise, bewahrte aber die Daten des Betroffenen ein Jahr auf, um nachzuhalten, ob die Chipkarte ausgetauscht wurde. Nach einer Beanstandung dieser unangemessen langen Speicherung konnte erreicht werden, dass künftig die Daten von Fahrgästen, deren Chipkarten bei Fahrgastkontrollen nicht ausgelesen werden können, unverzüglich nach dem Umtausch der Chipkarte gelöscht werden.

➡ Die mit einer Fahrscheinkontrolle verbundene Datenverarbeitung darf nicht zu Lasten von unbescholtenen Fahrgästen erfolgen.

14.2 "Gelber Sack" nur gegen Verbraucherdaten?

Um den Missbrauch "gelber Säcke" zu verhindern, hatten Entsorgungsunternehmen eine neue Idee: Die Säcke sollten nur noch Zug um Zug gegen die Namen und Adressen der Verbraucherinnen und Verbraucher ausgehändigt werden.

Die Erhebung personenbezogener Daten bei der Ausgabe von "gelben Säcken" war Gegenstand datenschutzrechtlicher Überprüfungen, nachdem das Duale System zum 1. Januar 2008 die Entsorgungsaufträge im offenen Wettbewerb neu vergeben hatte. Besorgte Bürgerinnen und Bürger trugen vermehrt Bedenken gegen die von mehreren lokalen Entsorgungsunternehmen bei der Ausgabe der Wertstoffsäcke praktizierte Datenerhebung vor. Diese hatten auf sogenannten Abholkarten unter anderem die Angabe von Name, Adresse und Unterschrift verlangt. Nur gegen ausgefüllte Abholkarten sollten die örtlichen Abholstellen "gelbe Säcke" aushändigen. Die Abholkarten wurden von den Entsorgungsunternehmen eingesammelt, über ein Jahr lang gespeichert, und es wurde stichprobenartig überprüft, wie viele Wertstoffsäcke pro Person abgeholt wurden. Mit dieser Kontrolle sollte die missbräuchliche Verwendung der Wertstoffsäcke verhindert und ihr extensiver Verbrauch einschränkt werden.

Bei der Ausgabe der gelben Säcke ist den Interessen der Betroffenen in angemessener Weise Rechnung zu tragen. Art und Weise der Entsorgung im Dualen System haben sich nach den Vorschriften der Verpackungsordnung zu richten. So können Verbraucherinnen und Verbraucher nicht nur verlangen, dass die Verkaufsverpackungen unentgeltlich zurückgenommen werden, sondern auch erwarten, dass sie regelmäßig bei ihnen abgeholt werden. Es ist deshalb mit der Verpackungsverordnung nicht vereinbar, wenn die Verteilung "gelber Säcke" eingeschränkt und mit unzumutbaren Bedingungen verknüpft wird. Die Regelungen der Verordnung sehen nicht vor, dass die Entsorgungsunternehmen personenbezogene Daten von Verbraucherinnen und Verbrauchern zum Zwecke einer Missbrauchskontrolle erheben und speichern dürfen. Daten der Betroffenen dürften daher allenfalls mit deren Einwilligung verarbeitet werden. Bei Verweigerung der Angaben muss die Ausgabe der Wertstoffsäcke trotzdem erfolgen. Mehrere Entsorgungsunternehmen haben inzwischen von ihrer Datenerhebungspraxis Abstand genommen und Abholkarten ohne Angabe personenbe-

zogener Daten verteilt, so dass "Gelbe Säcke" anonym bei den Ausgabestellen abgeholt werden können. Das Umweltministerium NRW ist in diesem Zusammenhang gebeten worden, sich dafür einzusetzen, dass die Verteilung der Abholkarten an die Haushalte mit der Ausgabe der jährlichen Abfallkalender durch die Kreise und kreisfreien Städte verbunden wird.

➡ Eine Erhebung und Speicherung von Verbraucherdaten ist bei der Verteilung von "gelben Säcken" nicht notwendig, allenfalls mit Einwilligung der Betroffenen zulässig. Die Ausgabe der Wertstoffsäcke darf bei Verweigerung der gewünschten Angaben nicht abgelehnt werden.

15 Statistik

15.1 Registergestützte Volkszählung (Zensus 2011)

Deutschland wird sich an dem für 2011 in der Europäischen Union vorgesehenen Zensus beteiligen, mit dem Daten zur Bevölkerung sowie ihrer Erwerbs- und Wohnsituation erhoben werden sollen. An die Stelle von Befragungen soll bei dieser Volkszählung überwiegend die Auswertung vorhandener Registerdaten treten.

Auch aufgrund der Erfahrungen mit dem erheblichen Widerstand vieler Bürgerinnen und Bürger gegen die Erfassung ihrer persönlichen Daten der zurückliegenden Volkszählungen wird künftig von einer direkten Befragung überwiegend abgesehen. Die benötigten Daten sollen vielmehr im Wesentlichen durch die Auswertung der Melderegister und anderer Verwaltungsregister gewonnen werden. Lediglich die Daten über Gebäude und Wohnungen werden bei den Eigentümerinnen und Eigentümern postalisch erfragt, weil es darüber keine flächendeckenden Verwaltungsregister gibt. Ergänzend sollen Stichproben mittels Fragebogen erfolgen.

Zur Vorbereitung des registergestützten Zensus hat der Bundestag das Zensusvorbereitungsgesetz vom 20. März 2007 erlassen. Dieses enthält Regelungen zum Anschriften- und Gebäuderegister, das unter Mitwirkung der Statistischen Landesämter vom Statistischen Bundesamt erstellt und geführt wird, sowie zu Verantwortlichkeiten und Verarbeitungsbefugnissen. Zur Erstellung dieses Registers sollen alle Personen, die Eigentum an Gebäuden oder Wohnungen innehaben, festgestellt werden. Dabei ist ergänzend vorgesehen, die Daten der Landesvermessungsbehörden, der Meldebehörden und der Bundesagentur für Arbeit zu nutzen. Diese enthalten die für den vorgesehenen Zweck erforderlichen Angaben flächendeckend in der benötigten Qualität und Aktualität, so dass eine vollständige Erhebung sichergestellt werden kann.

Zu einem ersten Entwurf eines Gesetzes zur Anordnung des registergestützten Zensus einschließlich der Gebäude- und Wohnungszählung 2011 (Stand: 16. April 2008) wurde das Innenministerium gebeten, die folgenden datenschutzrechtlichen Erfordernisse bei den weiteren Gesetzesberatungen zu unterstützen:

- Der übliche Aufenthaltsort einer Person soll Grundlage für die Feststellung der amtlichen Einwohnerzahl sein (§ 2 Abs. 2 Satz 1 des Entwurfs). Dieser wird als der Ort festgelegt, an dem diese Person gemäß den melderechtlichen Vorschriften des Bundes und der Länder mit alleiniger Wohnung oder Hauptwohnung gemeldet sein sollte. Soweit nach diesen Vorschriften der Aufenthalt in einem Sonderbereich (etwa in einer Justizvollzugsanstalt oder einem Krankenhaus) nicht meldepflichtig sein wird, ist dieser Aufenthaltsort nicht als üblicher Aufenthaltsort der betreffenden Person anzusehen. Da andererseits aber auch die Zählung der Personen mit üblichem Aufenthalt in Sonderbereichen Grundlage für die Feststellung der amtlichen Einwohnerzahl sein soll (§ 2 Abs. 4 in Verbindung mit § 8 des Entwurfs), bedarf es einer entsprechend präzisierten gesetzlichen Regelung.

- Hinsichtlich der Personen in sensiblen Anstaltsbereichen (etwa Justizvollzugsanstalten) bedarf es keiner personenbezogenen Datenerfassung. Vielmehr genügt es nach den im Volkszählungsurteil des Bundesverfassungsgerichts aufgestellten Maßstäben (BVerfGE 65, 1/49), die Anstaltsleitung zu verpflichten, die zahlenmäßige Belegung zum Zählungsstichtag ohne Personenbezug mitzuteilen, falls die Melderegister bis dahin die für die statistischen Erfassungen genügenden aussagekräftigen Daten aufweisen. Eine hundertprozentig zutreffende Datenlage ist ohnehin nicht erreichbar und für verlässliche statistische Aussagen auch nicht zwingend erforderlich. Im Übrigen ist auf die Begründung zu § 9 Zensusvorbereitungsgesetz zu verweisen. Danach soll der Aufbau eines vollständigen Registers von Sondergebäuden der Vorbereitung der Erhebungen bei den Bewohnerinnen und Bewohnern dieser Gebäude dienen und es ermöglichen, in sensiblen Anstaltbereichen die Erhebung anonym durchzuführen zu können (BT-Drucksache 16/5525, S. 18).

- Nach § 9 Abs. 2 des Entwurfs dürfen Erhebungsdaten und bestimmte Datensätze zur Feststellung von Über- und Untererfassungen in den Melderegistern sowie zur Erstellung erwerbs- und bildungsstatistischer Auswertungen zusammengeführt werden. Zweck und Ziel dieser Zusammenführung werden we-

der aus dem Gesetzestext noch aus der Begründung deutlich. Zudem ergibt sich aus § 9 Abs. 3 des Entwurfs und seiner Begründung, dass Daten für weitere Zwecke genutzt werden sollen. Die jeweiligen Zwecke sollten mindestens in der Begründung konkretisiert werden.

➡ Bei dieser grundlegend neuartigen statistischen Erhebungsmethode ist auf die strikte Einhaltung der statistikdatenschutzrechtlichen Anforderungen zu achten. Auch die Datenflüsse müssen sicher sein, um Pannen möglichst auszuschließen. Bei den Erhebungen muss insbesondere dem verfassungsrechtlichen Gebot der Abschottung der amtlichen Statistik vom Verwaltungsvollzug genügt werden.

15.2 Keine Schülerstatistik ohne Datenschutz – never ending story

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 verarbeitet werden sollen. Problematisch sind die Erhebungen, weil sie die gesamte Schullaufbahn jeder einzelnen Schülerin und jedes einzelnen Schülers transparent darstellen.

Zu dem ursprünglichen Konzept, auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte "Schulleben" einen umfangreichen Datensatz mit einer Identifikationsnummer anzulegen, haben die Datenschutzbeauftragten in ihrer Entschließung vom 26./27. Oktober 2006 (siehe Bericht 2007 im Anhang) äußerst kritisch Stellung genommen.

In einem überarbeiteten Konzept der Kultusministerkonferenz (KMK) wird zwar auf Identifikationsnummern verzichtet, vorgesehen ist jedoch eine zweistufige Verschlüsselung der Datensätze der Schülerinnen und Schüler, mit der bislang aber ebenfalls kein ausreichendes Datenschutzniveau erreicht wird. So enthält die Verfahrensbeschreibung der Verschlüsselung mehrere Unklarheiten, die sowohl die Verschlüsselungsmethode als auch den Ausschluss einer Reidentifizierbarkeit von Schülerinnen und Schülern in Frage stellen. Im Übrigen blei-

ben auch hinsichtlich des überarbeiteten Konzepts zentrale datenschutzrechtliche Fragen unbeantwortet.

So liegt keine detaillierte und nachvollziehbare Begründung vor, weshalb nicht anstelle der vorgesehenen Maßnahmen, die zukünftig bei den Schulen und Schulverwaltungen sowie den Statistischen Ämtern absehbar einen erheblichen technisch-organisatorischen, finanziellen und personellen Aufwand zur Folge haben werden, Untersuchungen im Bildungsbereich, die sich auf fundierte wissenschaftliche Analysen einzelner Problemfelder beschränken, denselben Zweck erfüllen. Allein der Verweis darauf, von wissenschaftlicher Seite werde eine erhebliche Verbesserung der Datenbasis gefordert und viele Fragen von politischer Relevanz könnten mit statistischen Daten nur mit unverhältnismäßig hohem Aufwand beantwortet werden, begründet noch keine Totalerhebung. Bisher ist nicht ersichtlich, weshalb gründliche fachwissenschaftliche, einen hinreichend großen Datensatz einbeziehende Untersuchungen bezogen auf eine kleine Stichprobe den anerkanntermaßen bestehenden Bedarf an Erkenntnissen für Verbesserungen im Schulwesen nicht ebenso befriedigen können. Auch das Argument, dass bei einer Stichprobenauswahl Gruppen für die Beurteilung verschiedener Zusammenhänge schnell zu klein würden, ist zur Begründung von Totalerhebungen nicht geeignet. Einem solchen Manko könnte durch eine valide, wissenschaftlichen Erfordernissen Rechnung tragende Stichprobenauswahl begegnet werden.

Auch weitere Fragen sind bisher nicht geklärt. So wären Datenverarbeitungen im Zuge einer Schulstatistik in dem beabsichtigten Umfang für die noch zu benennenden konkreten Zwecke nur durch Einführung einer amtlichen Statistik und ihrer Erhebungsinstrumentarien zulässig. Eine amtliche Statistik erfordert insbesondere folgende einheitliche Regelung im Gesetz: Festlegung der Erhebungs- und Hilfsmerkmale, Regelung der Auskunftspflicht, Festlegung der statistikrechtlich gebotenen technischen und organisatorischen Maßnahmen.

➡ Der KMK wurden die datenschutzrechtlichen Bedenken mitgeteilt. Das vorliegende Konzept wird ohne grundlegende Änderungen nicht datenschutzkonform umsetzbar sein.

.

16 Internationaler Datenverkehr

16.1 Reisefreiheit – leider nicht überwachungsfrei

Die Projekte zur Überwachung des Reiseverkehrs werden immer ausufernder. Nicht nur der transatlantische Flugverkehr ist betroffen. Es gibt auch Pläne zur Überwachung des Reiseverkehrs in Europa.

Die Angst vor Terroranschlägen hatte zunächst vor allem in den USA und Kanada zu umfassenden Überwachungsmaßnahmen im Reiseverkehr geführt, die teilweise schon in den beiden letzten Berichten dargestellt sind. Diese Entwicklung schritt seither stetig fort. So verlangt nun nach den USA auch Kanada von den Fluggesellschaften, dass diese ihre Passagierlisten mit sogenannten No-fly-Listen abgleichen. Auf diesen Listen sind hunderttausende von Personen vermerkt, die in die genannten Länder nicht einreisen dürfen. Die USA planen für das Jahr 2009 nicht mehr wie bisher, den Datenabgleich der Passagierdaten den Fluggesellschaften zu überlassen, sondern wollen ihn mit dem Programm "Secure Flight" selbst durchführen. Welche Überwachungsvarianten sich durch dieses Programm ergeben und welche Datensammlungen daraus entstehen, ist noch nicht absehbar.

Die USA haben außerdem im Jahr 2008 damit begonnen, von Reisenden, die im Rahmen des Visa-Waiver-Programms ohne Visum in die USA einreisen, vor Reisebeginn über eine Internetseite Antworten auf einen Fragenkatalog zu sammeln. Gefragt wird unter anderem nach körperlichen oder mentalen Erkrankungen, nach bestehender Drogenabhängigkeit, Verhaftungen oder Verurteilungen wegen krimineller Handlungen oder danach, ob die einreisende Person an einem Sabotageakt, einer terroristischen Aktivität oder einem Völkermord beteiligt war oder aktuell beteiligt ist. Die Beantwortung der Fragen in diesem sogenannten ESTA-Verfahren ist ab Beginn des Jahres 2009 verpflichtend für Deutsche, die in die USA einreisen wollen. Ähnliche Informationen wurden bisher auf der Flugreise in handschriftlicher Form erhoben. Durch die elektronische Erfassung und Speicherung der Angaben für 75 Jahre werden die Daten nun leicht zugänglich und können einfach elektronisch ausgewertet und zwischen Behörden ausgetauscht werden. Dieses neue Verfahren ermöglicht eine auf unverhältnismäßige Dauer angelegte Überwachung aller Reisen in die USA.

Ein weiteres Abkommen zur Übermittlung von Passagierdaten wurde nach Kanada und den USA nun auch zwischen Australien und der Europäischen Union vereinbart. Weiterhin werden von Südkorea und Indien Forderungen zur Übermittlung von Passagierdaten gestellt; entsprechende Vereinbarungen wurden mit diesen Staaten aber bisher nicht geschlossen.

Außerdem verlangen die Grenzkontrollbehörden in Großbritannien auch für innereuropäische Flüge in einem ersten Schritt Passdaten und in einem weiteren Schritt Reservierungsdaten der Reisenden von den Fluggesellschaften. Für Deutschland gilt hier, dass eine Rechtsgrundlage für eine solche Datenübermittlung an die britischen Behörden nicht existiert und die Übermittlung damit nicht zulässig sein dürfte.

Last but not least hat die EU-Kommission auf Anforderung des EU-Rates einen Entwurf für einen Rahmenbeschluss zur Erhebung von Reservierungsdaten von Passagieren auf Flügen in die und aus der EU vorgelegt. Nach diesem Entwurf sollen dieselben Datenkategorien erhoben werden, wie sie auch im Abkommen mit den USA zur Passagierdatenübermittlung festgelegt wurden. Die Daten sollen anlass- und verdachtsunabhängig 13 Jahre lang gespeichert werden, sie sollen für Risikoanalysen zur Verfügung stehen und auch mit Staaten außerhalb der EU ausgetauscht werden können. Auf die verfassungsrechtlichen Bedenken, denen dieser Entwurf begegnet, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer im Anhang abgedruckten Entschließung vom 3./4. April 2007 eindringlich hingewiesen.

Im Rat der Europäischen Union wurden Überlegungen diskutiert, den Rahmenbeschluss auch auf andere Verkehrsarten, insbesondere den Zugverkehr, den Überlandbusverkehr und den Schiffsverkehr auszudehnen und innereuropäische Reisen mit in den Überwachungsplan einzubeziehen.

Die Gesamtheit dieser Forderungen wirft die Frage auf, ob der Kampf gegen den Terrorismus eine Übermittlung von Passagierdaten in alle möglichen Länder rechtfertigen kann und damit mittelfristig die umfassende verdachtsunabhängige Passagierüberwachung zur Norm wird. Was einmal mit der außergewöhnlichen Situation nach den Attentaten vom 11. September 2001 gerechtfertigt wurde, entwickelt sich mehr und mehr und entgegen aller verfassungsrechtlichen Grund-

sätze zu einem Regelinstrument der Überwachung von Reisenden. Hier muss noch einmal in Erinnerung gerufen werden, dass nicht bloße Identitäts- oder Passdaten übermittelt werden, sondern es können Informationen über Erkrankungen von Passagieren, Essenswünsche, Konto- oder Kreditkartendaten sowie Informationen über Hotelbuchungen und vieles mehr zu den Datensätzen gehören. Angesichts der Tatsache, dass nun die EU selbst solche Überwachungspläne verfolgt, wird es zukünftig kaum mehr möglich sein, derartige Forderungen anderen Staaten zu verwehren, wenn diese in einem Abkommen gewisse Datenschutzgarantien abgeben. Passagiere werden sich also daran gewöhnen müssen, dass – wohin auch immer sie reisen – in Zukunft möglicherweise schon einmal die Kreditkartendaten oder die Kontonummer den staatlichen Behörden übermittelt werden. Wie gut diese Behörden dann garantieren können, dass Unberechtigte diese Daten nicht erhalten, wird sicher weltweit und länderspezifisch sehr unterschiedlich sein.

➡ Das deutsche Verfassungsrecht dürfte einer Beteiligung der Bundesrepublik Deutschland an den weitreichenden Plänen der Europäischen Union zur Passagierüberwachung entgegen stehen.

16.2 Antiterrorlisten – gibt es doch einen Rechtsweg?

Dass es keinen effektiven Rechtsschutz für Personen gibt, die auf einer Liste der Vereinten Nationen als terrorverdächtig eingestuft sind, wurde im Bericht 2007 dargestellt. Nun hat der Europäische Gerichtshof eigentlich eine Selbstverständlichkeit ausgesprochen und entschieden, dass die Europäische Union bei der Umsetzung von Resolutionen der Vereinten Nationen über Sanktionslisten in europäisches Recht rechtsstaatliche Grundsätze beachten muss.

Gegen Personen auf sogenannten Antiterrorlisten der Vereinten Nationen können empfindliche Sanktionen verhängt werden. Insbesondere können Einreiseverbote ergehen und Vermögenswerte eingefroren werden. Dies ist besonders dann äußerst kritisch, wenn es wegen Gleichheit oder Ähnlichkeit von Namen zu Verwechselungen und damit zu Maßnahmen gegen Personen kommt, die tatsächlich nicht terrorverdächtig sind. Das Gericht 1. Instanz der Europäischen Gemein-

schaften hatte 2005 eine gerichtliche Überprüfung einer EG-Verordnung zur Umsetzung von Maßnahmen gegen Personen auf Antiterrorlisten der Vereinten Nationen in europäisches Recht abgelehnt. Das Gericht war der Auffassung, dass die Verordnung wegen einer vorrangigen völkerrechtlichen Verpflichtung nicht gerichtlich überprüfbar sei.

Diese Rechtsprechung wurde nun vom Europäischen Gerichtshof (EuGH) mit Urteil vom 3. September 2008 (C-402/05P; C-415/05P) korrigiert. Der EuGH stellt fest, dass Maßnahmen der Europäischen Gemeinschaft, die der Umsetzung von Sanktionen gegen durch die Vereinten Nationen gelistete Personen dienen, gerichtlich überprüfbar sind. Dies gilt insbesondere, weil bisher kein Verfahren zur Verfügung steht, das die Garantien eines gerichtlichen Rechtsschutzes bietet. Der EuGH stellte außerdem fest, dass die Gründe mitgeteilt werden müssen, die zur Aufnahme eines Namens in eine Sanktionsliste geführt haben, damit ein effektiver Rechtsschutz überhaupt möglich ist. Nur wenn den Betroffenen die ihnen zur Last gelegten Umstände mitgeteilt werden, haben sie die Möglichkeit, dagegen sachlich vorzutragen. Auch setzt die Effektivität der gerichtlichen Kontrolle voraus, dass die wesentlichen Gründe der Entscheidung über die Aufnahme in eine Liste bekannt und damit der gerichtlichen Überprüfung zugänglich sind. Es ist allerdings nicht erforderlich, dass Betroffenen vor der Aufnahme in eine Sanktionsliste eine Mitteilung über die Gründe gemacht wird, da ansonsten Sanktionsmaßnahmen eventuell ins Leere zu laufen drohen. Die Betroffenen müssen aber so bald wie möglich informiert werden.

Die Europäische Kommission hat angekündigt, die vom EuGH geforderten Verfahrensanforderungen zu erfüllen.

➡ Die Entscheidung des Europäischen Gerichtshofes hat den Rechtsschutz in Europa für Personen, die auf den Terroristenlisten der Vereinten Nationen geführt werden, erheblich verbessert. Es bleibt abzuwarten, wie die Europäische Kommission die Vorgaben des Gerichts in der Praxis umsetzen wird.

16.3 Verbindliche Unternehmensregelungen – ein langer Weg, der sich lohnen soll

Datenübermittlungen an Stellen in Länder außerhalb des Europäischen Wirtschaftsraumes (EWR) sind oft nur möglich, wenn angemessene Garantien für die Persönlichkeitsrechte der von der Übermittlung betroffenen Personen eingeräumt werden. Für Konzerne kann das durch eine verbindliche Unternehmensregelung geschehen, die im gesamten Konzern gilt. Der Weg dahin ist oft mühevoll.

Verbindliche Unternehmensregelung oder Binding Corporate Rules (BCR), wie sie in der Fachsprache oft bezeichnet werden, sollen in allen Unternehmen eines Konzerns eine gute Datenschutzkultur einführen und Datenschutzgarantien schaffen, die auch die Übermittlung von Daten an Konzerntöchter ermöglichen, die ihren Sitz nicht im EWR haben. Im Konzern erleichtert die gemeinsame Datenschutzkultur die einheitliche konzerninterne Datenschutzkontrolle. Gleichzeitig wird nach außen dokumentiert, dass der Konzern die Persönlichkeitsrechte seiner Kundschaft und Belegschaft ernst nimmt, was sich als Wettbewerbsvorteil erweisen kann. In Deutschland konnten bereits die BCR einiger Konzerne insofern anerkannt werden, als die Datenschutzaufsichtbehörden gemeinsam feststellten, dass diese Regelungen die Voraussetzungen gemäß §§ 4b Abs. 2 und 3, 4c Abs. 2 Bundesdatenschutzgesetz für Datenübermittlungen in das Ausland schaffen. Dies bedeutet, dass durch die BCR ein angemessenes Datenschutzniveau in konzernangehörigen Unternehmen auch außerhalb der Europäischen Union hergestellt werden kann, mindestens aber ausreichende Garantien für die Persönlichkeitsrechte der von Datenübermittlungen an Konzernunternehmen im Drittstaat betroffenen Personen gegeben werden.

In Europa hat der Weg zu einer gemeinsamen Anerkennung von BCR durch die europäischen Datenschutzbehörden bisher noch nicht zu konkreten Ergebnissen geführt. Es wurden aber mit den Arbeitspapieren 153, 154 und 155 der Artikel–29–Arbeitsgruppe im Juni 2008 Dokumente veröffentlicht, aus denen sich Konzerne darüber informieren können, welche Anforderungen ihre BCR erfüllen müssen, damit sie als Grundlage für Datenübermittlungen an Stellen außerhalb des EWR europaweit Anerkennung finden. Die Dokumente können im

Internet abgerufen werden unter http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm.

Zusätzlich wollen die europäischen Datenschutzbehörden den Prozess der Anerkennung von BCR erheblich beschleunigen. In einer Testphase bis Mai 2009 sollen die rund zehn Regelungen, die Konzerne bisher für eine europaweite Anerkennung eingereicht haben, abgearbeitet sein. Ziel ist mittelfristig, dass die Anerkennung von BCR durch eine europäische Datenschutzbehörde von allen anderen akzeptiert werden kann.

- Eine verbindliche Unternehmensregelung zum Datenschutz kann auf die Bedürfnisse eines Konzerns abgestimmte Lösungen für internationale Datenübermittlungen bieten. Wegen des Verfahrens zur Anerkennung der Regelung deutscher Konzerne berät vorrangig die Datenschutzaufsichtsbehörde am Sitz der Konzernmutter.

17 Informationsfreiheit

17.1 Sind Qualitätsberichte über Schulen allgemein zugänglich?

Qualitätsanalyse dient dem Ziel, die Qualität von Schulen zu sichern und nachhaltige Impulse für deren Weiterentwicklung zu geben. Sie ist gekennzeichnet durch Transparenz, Verbindlichkeit und gegenseitige Rücksichtnahme (§ 1 Abs. 1 Qualitätsanalyseverordnung (QA-VO)). Aber wie steht's mit dem Informationszugang zu den Qualitätsberichten? Soll er verhindert werden, weil die Offenlegung zu einem Schulranking führen könnte?

Auf Bundes-, Landes- und örtlicher Ebene stehen Bildungsthemen auf der Tagesordnung. Maßgebliche Akteurin im Veränderungsprozess ist zum einen die Schulverwaltung. Sie verschafft sich mit der Durchführung von Qualitätsanalysen und der Erstellung von Qualitätsberichten das Datenmaterial für gezielte Maßnahmen der Qualitätsverbesserung in den einzelnen Schulen sowie für entsprechende Unterstützungsleistungen der Schulaufsichtsbehörden und Steuerungsmaßnahmen des Ministeriums (§ 1 Abs. 1 QA-VO). Aber auch in der Öffentlichkeit besteht großes Interesse an den Ergebnissen der Qualitätsanalysen: Namhafte Institute und Reportagemagazine versuchen, vor allem mit Rankings eine Übersicht über die Vielzahl von Lernaspekten und Unterrichtsmethoden zu schaffen. Nicht zuletzt sind es Schülerinnen, Schüler und deren Eltern, die sich von den Qualitätsberichten Hilfestellung für ihre Schulauswahl erhoffen.

Zwar enthält die für die Qualitätsanalyse geltende Verordnung einen Passus zum Recht einer Schule, "ihren" Qualitätsbericht zu veröffentlichen. Für den umgekehrten Fall aber, dass eine (außen stehende) Person Zugang zu den Informationen verlangt, trifft die Verordnung keine besondere Regelung. Ein solcher Informationsanspruch richtet sich daher nach den allgemeinen Zugangsregeln des Informationsfreiheitsgesetzes NRW. Danach steht dem Zugang zu den Qualitätsberichten allenfalls der Schutz personenbezogener Daten entgegen. Die Berichte sollen personenbezogene Daten von Lehrerinnen und Lehrern, von Schülerinnen und Schülern und von Eltern nur unter Beachtung der datenschutzrechtlichen Bestimmungen (§ 3 Abs. 7 QA-VO) enthalten.

In der Regel werden also von vorneherein keine personenbezogenen Daten in den Qualitätsberichten stehen. Die Passagen jedoch, die die Schulleitung betreffen und damit personenbeziehbar sind, dürfen nur mit Einwilligung der Mitglieder der Schulleitung zugänglich gemacht werden. Andernfalls wären diese Berichtsteile unkenntlich zu machen (siehe insoweit auch unter 12.4).

➡ Schulen können über die Veröffentlichung ihrer Qualitätsberichte selbst entscheiden. Im Falle eines Informationszugangsantrags sind die Berichte – mit Ausnahme des "Schulleitungsteils" – grundsätzlich zugänglich.

17.2 Bezirksregierung verweigert Schulinformationen

Statt unverzüglich die gewünschten Informationen zur Verfügung zu stellen, musste eine Bezirksregierung trotz gerichtlicher Verurteilung durch förmliche Beanstandung und ministerieller Weisung zur Informationserteilung veranlasst werden.

Unter ausdrücklicher Berufung auf das Informationsfreiheitsgesetz NRW (IFG NRW) beantragte ein Lehrer bei einer Bezirksregierung Auskünfte zu verschiedenen Aspekten der Stundenplangestaltung der Schule, an der seine Ehefrau unterrichtet. Die Bezirksregierung lehnte den Informationszugang mit dem interessanten, aber unhaltbaren Argument ab, er könne die Informationen doch über seine Ehefrau erhalten. Soweit diese wider Erwarten die bestehenden Fragen nicht abschließend mit ihrer Schulleitung klären könne, habe sie dann die Möglichkeit, sich unter Einhaltung des Dienstwegs an die Schulaufsichtsbehörde zu wenden.

Gegenüber der Bezirksregierung stellte die LDI NRW klar, dass dem Informationsbegehren des Lehrers nicht § 5 Abs. 4 Halbsatz 2 IFG NRW entgegen gehalten werden konnte. Nach dieser Vorschrift darf zwar ein Informationsantrag abgelehnt werden, wenn sich die gewünschte Information in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen lässt. Die Ehefrau des Antragstellers ist aber jedenfalls nicht als eine solche Quelle anzusehen. Ferner gewährt das IFG NRW den Informationszugang voraussetzungslos, sodass es grundsätzlich nicht angezeigt ist zu prüfen, aus welchen Gründen die

informationssuchende Person an der nachgefragten Information interessiert sein könnte.

Im weiteren Verfahren wurde zudem die Regelung des § 5 Abs. 1 Satz 4 IFG NRW thematisiert. Sie definiert die zuständige Behörde für Anträge auf Zugang zu amtlichen Informationen der Verwaltungstätigkeit von Schulen: Informationen über innere Schulangelegenheiten (insbesondere Unterricht, Erziehung und Schulleben) sind bei der Schulaufsicht zu beantragen, Informationen zu äußeren Schulangelegenheiten (Gebäude- und Sachausstattung sowie Verwaltungspersonal) beim Schulträger. Dies werde, so kritisierte die Bezirksregierung, der Selbständigkeit der Schulen nicht gerecht. Gleichwohl ist die gesetzliche Vorgabe eindeutig und dient wohl auch der Entlastung der Schulen von Problemen der Handhabung von Informationszugangsanträgen.

Trotz Empfehlung der LDI NRW gelangte der Streit über den Antrag des Lehrers vor das Verwaltungsgericht. Auf Vorschlag des Gerichts verpflichtete sich die Bezirksregierung, dem Antragsteller die gewünschten Informationen offen zu legen. Allerdings erfüllte sie ihre Verpflichtung nicht, so dass noch nach Abschluss des gerichtlichen Verfahrens eine förmliche Beanstandung auszusprechen war. Letztlich bedurfte es sogar noch einer Weisung des Innenministeriums an die Bezirksregierung, die beantragten Informationen offen zu legen.

➡ Werden Informationen zu inneren Schulangelegenheiten bei der Schulaufsicht beantragt, muss diese gewährleisten, dass die zugänglichen Informationen entweder durch sie beschafft oder der informationssuchenden Person durch die Schule zur Verfügung gestellt werden.

17.3 WDR verweigert Auskünfte über seine Aufträge an private Unternehmen

Kann der WDR für sich in Anspruch nehmen, dass das Informationsfreiheitsgesetz NRW auf ihn keine Anwendung findet, da er als Rundfunkanstalt staatsfern tätig und ausschließlich dem Rundfunkrecht unterworfen ist?

Ein Journalist beansprucht Auskünfte vom WDR über Aufträge, die an private Unternehmen vergeben wurden, mit Angaben über Auftrags-

volumen, Ausschreibung und über Mängel bei der Durchführung des Auftrags einschließlich einer daraus eventuell resultierenden Forderung. In der Liste der möglichen Auftragnehmerinnen und -nehmer sind bestimmte Banken, Versicherungen, Energieversorgungsunternehmen, Messeunternehmen und Abfallentsorgungsunternehmen, aber auch Produktionsfirmen der Medienbranche aufgeführt.

Der WDR lehnte jede Auskunft zu den gestellten Fragen ab, weil er als Rundfunkanstalt nur insoweit dem Anwendungsbereich des Informationsfreiheitsgesetzes NRW (IFG NRW) unterfalle, als er Verwaltungstätigkeiten allenfalls beim Rundfunkgebühreneinzug wahrnehme. Auf alle anderen Tätigkeiten des WDR finde das Gesetz grundsätzlich keine Anwendung. Zwar sei er eine Anstalt öffentlichen Rechts, damit aber noch keine öffentliche Stelle im Sinne des § 2 Abs. 1 IFG NRW. Soweit landesrechtliche Regelungen auf den WDR Anwendung finden sollten, sei dies ausdrücklich im WDR-Gesetz oder in speziellen Gesetzen, wie dem Landesbeamten- und dem Landesgleichstellungsgesetz, geregelt. Später berief sich der WDR unter Beibehaltung seiner grundsätzlichen Auffassung noch darauf, dass der Schutz von Betriebs- und Geschäftsgeheimnissen sowie der Schutz personenbezogener Daten eine Auskunftserteilung verbiete, ohne dies im Einzelnen zu begründen.

Diese Auffassung ist jedoch nicht zutreffend. Der WDR ist eine Einrichtung des Landes und der Rechtsaufsicht der Landesregierung unterstellt. Ihm sind durch das WDR-Gesetz Aufgaben auf dem Gebiet des öffentlichen Rechts übertragen worden, deren Erfüllung unter anderem durch haushaltsrechtliche Grundsätze bestimmt ist. Vor allem hat der WDR den Grundsatz der Wirtschaftlichkeit und der Sparsamkeit zu beachten. Es entspricht der Zielsetzung des Informationsfreiheitsgesetzes NRW, Transparenz in das Ausgabengebaren auch einer öffentlich-rechtlichen Rundfunkanstalt zu bringen, die sich aus öffentlichen Rundfunkgebühren finanziert. Zu den in diesem Zusammenhang gestellten Fragen ist der WDR grundsätzlich auskunftspflichtig. Dies ergibt sich schon aus dem Wortlaut des Gesetzes, weil § 2 IFG NRW den WDR nicht ausgenommen hat. Außerdem trifft keine vorrangige spezialgesetzliche Regelung eine Bestimmung, durch die die Anwendung des IFG NRW ausgeschlossen wäre.

Da jede weitere Bewertung des geltend gemachten Informationsanspruches ohne nähere Erläuterungen durch den WDR nicht möglich war, wurde der WDR wiederholt um entsprechende Auskünfte gebe-

ten. Diesen Auskunftsersuchen hat der WDR allerdings unter Hinweis auf die oben dargestellten Ausführungen und auf das eingeleitete Klageverfahren vor dem Verwaltungsgericht nicht entsprochen. Auf die inzwischen ausgesprochene Beanstandung konnte auch angesichts des laufenden Verwaltungsgerichtsverfahren nicht verzichtet werden, weil es zur Aufgabenerfüllung der LDI NRW gehört, unabhängig zu prüfen, ob die Anwendung des IFG NRW bei allen öffentlichen Stellen des Landes sicher gestellt ist (§ 13 Abs. 1 IFG NRW).

➡ Im Rahmen seiner Verwaltungstätigkeit ist der WDR verpflichtet, der LDI NRW die notwendigen Auskünfte zu erteilen, die eine informationsfreiheitsrechtliche Beurteilung ermöglichen.

17.4 Förderbank des Landes verweigerte zunächst Offenlegung von Subventionen

Journalistinnen und Journalisten, die Ansprüche auf Informationsfreiheit geltend machen, begegnen nicht selten dem "Strohmann-Argument".

Als ein international tätiger Telekommunikationskonzern seinen Standort in NRW schloss, erregte das bundesweite Diskussionen unter anderem über die dem Unternehmen zuvor gewährten öffentlichen Subventionen. Um darüber zu berichten, beantragte ein freier Mitarbeiter eines Fernsehsenders bei der Förderbank des Landes Kopien der Verträge über die Investitionskostenzuschüsse. Für seine Schreiben nutzte er allerdings Briefkopf und -formatierung seines Senders, schrieb von "wir" und bezog sich neben den Informationsfreiheitsgesetzen des Bundes und des Landes auch auf das Presserecht. Auf die ablehnende Reaktion wurde der Informationsantrag ausdrücklich im alleinigen Namen des Journalisten erneuert. Gleichwohl kritisierten sowohl die Förderbank als auch das in einem Eilverfahren angerufene Verwaltungsgericht, dass der Antragsteller die Informationen nicht als natürliche Person begehre, sondern in seiner Eigenschaft als freier Mitarbeiter des Senders. Letztendlich sei daher auf die Rundfunkanstalt abzustellen, der jedoch als juristischer Person kein Informationsanspruch zustehe. Einschlägig sei daher allein ein Anspruch aus dem nordrhein-westfälischen Pressegesetz, das allerdings keine Akteneinsicht oder Kopien, sondern schlicht Auskunft gewähre.

Das Oberverwaltungsgericht NRW hat diese "Strohmann"-Argumentation zu Recht korrigiert: Im Informationszugangsantrag sei doch hinreichend deutlich geworden, dass der Journalist ein eigenes Informationsinteresse verfolge. Ob er dabei auch im Interesse der Rundfunkanstalt gehandelt habe, könne dahinstehen; dies sei nicht etwa rechtsmissbräuchlich. Denn das Informationsfreiheitsgesetz NRW (IFG NRW) stelle gerade nicht auf die Motive oder ein besonderes Interesse der Antragstellerin oder des Antragstellers ab. Es sei deswegen auch unerheblich, ob beabsichtigt sei, die Information weiterzugeben: "Wollte man auf diesen Umstand abstellen, liefe das der gesetzgeberischen Intention entgegen, den Anspruch gerade nicht vom Nachweis eines rechtlichen, eines berechtigten oder eines sonstigen Interesses abhängig zu machen. Deshalb ist es auch unerheblich, ob der Antragsteller im Sinne eines 'Strohmannes' lediglich von einer juristischen Person vorgeschoben wird." (OVG NRW, Beschluss vom 21. August 2008 - 8 B 913/08 -).

Allerdings sah das Gericht zum Zeitpunkt seines Beschlusses über den Eilantrag einen – zeitlich begrenzten – Ablehnungsgrund. Denn nach dem IFG NRW dürfe eine Information nicht erteilt werden, soweit und solange durch die Bekanntgabe der Erfolg einer behördlichen Maßnahme erheblich beeinträchtigt werde. Der Begriff der Maßnahme erfasse jegliche Tätigkeit der öffentlichen Stellen unabhängig von der Rechtsqualität des Handelns. Da zum Zeitpunkt der Entscheidung noch Verhandlungen über die Rückforderung der Investitionskostenzuschüsse liefen und das Gericht eine erhebliche Gefährdung befürchtete, lehnte es den Informationszugang zu diesem Zeitpunkt ab.

- Das IFG NRW stellt nicht auf die Motive oder ein besonderes Interesse der Antragstellerin oder des Antragstellers ab. Es ist grundsätzlich unerheblich, ob beabsichtigt ist, die erlangte Information weiterzugeben.

17.5 Privat und Staat

Im Bereich der Bau- und Liegenschaftsverwaltung sollen Public-Private-Partnership (PPP)-Projekte die öffentliche Hand aus finanziellen Kalamitäten befreien. Volumen und lokale Bedeutung solcher Vorhaben lösen häufig genug ein öffentliches In-

teresse aus. Leider wird dann zu oft dem Informationswunsch eine Vereinbarung zwischen öffentlicher Hand und dem Unternehmen über Vertraulichkeit entgegen gehalten.

Eine Großstadt hatte den Bau und den Betrieb einiger Mehrfachsporthallen als PPP-Projekt ausgeschrieben und nach der Vergabe- und Vertragsordnung für Bauleistungen (VOB) an einen privaten Investor vergeben. Nach Vertragsschluss wollte ein Bürger wissen, welche Vertragsleistungen die Stadt jährlich zu erbringen hat. Er fragte nach genauen Bankzinsen, Tilgungszahlungen sowie Details zu weiteren Entgeltleistungen. Die Stadt verweigerte den Informationszugang mit Hinweis auf die VOB-Vorschriften und die vereinbarte Vertraulichkeit.

Zwar erklärt eine Vorschrift der einschlägigen VOB die Angebote und ihre Anlagen ausdrücklich als "geheim". Der Zugangsantrag bezog sich aber gar nicht auf die Vergabeunterlagen, sondern auf Informationen aus dem nach der Vergabe geschlossenen Vertrag. Selbst wenn die VOB Angebotsunterlagen auch nach Abschluss des Vergabeverfahrens schützt, bildet die Vergabeentscheidung eine Zäsur, die den Schutzbereich der VOB-Bestimmung begrenzt. Der danach verhandelte Vertrag gehört nicht mehr in diesen Schutzbereich. Das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) umfasst mit dem Gebot transparenten Verwaltungshandelns auch jede sich in privatrechtlichen Vertragsformen vollziehende Verwaltungstätigkeit. Es würde Sinn und Zweck des Gesetzes widersprechen, wenn sämtliche Informationen ausgenommen wären, die in Folge einer Auftragsvergabe nach Durchführung des Vergabeverfahrens entstanden sind und ihren Niederschlag im Vertrag gefunden haben.

Greift danach die Spezialregelung in der VOB nicht, bleibt noch der Schutz von Betriebs- oder Geschäftsgeheimnissen. Dieser Schutz besteht aber nach Auftragsvergabe nicht mehr so umfänglich. Denn nach Auftragsvergabe und entsprechendem Vertragsschluss ist für das Unternehmen, welches den Zuschlag erhalten hat, regelmäßig kein Wettbewerbsnachteil zu mitbietenden Konkurrentinnen und Konkurrenten mehr zu befürchten. Dann ist auch kein berechtigtes wirtschaftliches Geheimhaltungsinteresse anzunehmen, und eine Offenbarung der Auftragsdaten kann zu keinem wirtschaftlichen Schaden führen. Nur unter besonderen Voraussetzungen könnten schutzwürdige Betriebs- und Geschäftsgeheimnisse entgegenstehen, etwa wenn zukünftig ein vergleichbarer Auftrag von der öffentlichen Stelle ausgeschrieben wird

und potentielle Mitbewerberinnen und Mitbewerber aus der Kenntnis der Vertragsdaten für das künftige Ausschreibungsverfahren wertvolle Informationen und damit auch einen wirtschaftlichen Nutzen gewinnen könnten. Hierzu wäre aber erforderlich, dass ein vergleichbares Verfahren konkret absehbar ist.

Selbst wenn ein Betriebs- oder Geschäftsgeheimnis vorläge, muss der Informationszugang gewährt werden, wenn dem Geheimhaltungsinteresse des Unternehmens ein überwiegendes Informationsinteresse der Allgemeinheit gegenüber steht und der eventuell eintretende Schaden nur geringfügig wäre. Anhaltspunkte für ein überwiegendes öffentliches Interesse können beispielsweise Berichte in der örtlichen Presse über das Projekt und erhebliche Auswirkungen für die Allgemeinheit sein. In Fällen, in denen öffentliche Gelder eingesetzt oder durch öffentliche Stellen vertragliche Verpflichtungen eingegangen werden, überwiegt das öffentliche Interesse in aller Regel. Für die Abwägung ist somit insbesondere der Gemeinwohlbezug der begehrten Informationen entscheidend.

- Es widerspricht der Zielsetzung des IFG NRW, wenn von vornherein Informationen ausgeschlossen sind, die sich nach Auftragsvergabe in einem Vertrag zwischen öffentlicher Hand und privatem Unternehmen niedergeschlagen haben.

17.6 Offenlegung von Gebührenkalkulationen

Gebühren für die Entsorgung von Abfall und Abwasser belasten das Budget der Einwohnerinnen und Einwohner zunehmend. Kein Wunder also, dass ein besonderes Interesse an der Offenlegung der Gebührenkalkulation besteht und entsprechend viele Informationsanträge zu verzeichnen sind.

Kommunen beauftragen häufig private Unternehmen mit der Müllabfuhr. Aus verschiedenen Gründen wird mit der Offenlegung von Informationen gezögert. In einem Fall gründete die Kommune ihre Ablehnung des Informationsantrages unter anderem darauf, dass der Antragsteller kein öffentliches, sondern nur sein berufliches Interesse verfolge. Der Antragsteller hatte tatsächlich in seinem Antrag unnötigerweise angegeben, bei einem Unternehmen tätig zu sein, das in

Konkurrenz zu der von der Kommune beauftragten Entsorgungsfirma stand. Diese Begründung vermag hingegen eine Ablehnung nicht zu tragen. Wie das Oberverwaltungsgericht NRW in einem anderen Fall (Beschluss vom 21. August 2008 - 8 B 913/08 -) klargestellt hat, ist es unerheblich, wie eine Antragstellerin oder ein Antragsteller die Information nutzen will.

Kommunen können sich auch nicht auf den Schutz von Betriebs- oder Geschäftsgeheimnissen berufen, wenn sie Kalkulationsunterlagen für öffentlich-rechtliche Gebühren nicht offen legen wollen. Bei solchen Kalkulationen handelt es sich nicht um Tatsachen, die mit der Ausübung eines wirtschaftlichen Geschäftsbetriebes zusammen hängen. Sie sind vielmehr Teil des Verwaltungshandelns, mit dem eine öffentlichen Aufgabe, hier die Abfall- oder Abwasserbeseitigung, erfüllt wird. Insoweit gibt es selbst dann keine wirtschaftliche Wettbewerbssituation, wenn sich die Kommune eines privaten Entsorgungsunternehmens bedient.

Die Offenlegung von Kalkulationsunterlagen kann schließlich auch nicht mit der Begründung abgelehnt werden, dass die Gebührenkalkulation Gegenstand eines Ratsbeschlusses war, der in nicht-öffentlicher Sitzung gefasst wurde und deshalb geheim gehalten werden müsste. Nach § 7 Abs. 1 Informationsfreiheitsgesetz NRW (IFG NRW) sind zwar neben Beschlussentwürfen auch Protokolle vertraulichen Inhalts bis zum Ende des jeweiligen Verfahrens geschützt; aus Protokollen vertraulichen Inhaltes ist nach Abschluss des Verfahrens jedenfalls das Beratungsergebnis mitzuteilen. Von Beschlussentwürfen und Protokollen vertraulichen Inhalts sind allerdings Arbeits- und Beratungsunterlagen zu unterscheiden, auf deren Grundlage die interne Beratung erfolgt. Diese Arbeitsunterlagen erlauben keinerlei Rückschluss darauf, welches Mitglied eines Gremiums bei der Entscheidung welche Position vertreten hat. Sie betreffen nicht den eigentlichen Prozess der Entscheidungsfindung und sind nicht geschützt. Eine Einbeziehung in den Schutzbereich des § 7 IFG NRW beispielsweise im Wege der Analogie ist nach Ansicht des Oberverwaltungsgerichts NRW (Urteil vom 17. Mai 2006 - 8 A 1642/05 -) wegen des Gebots einer engen Auslegung der gesetzlich klar festgelegten Ablehnungsgründe nicht zulässig.

➡ Bei der Erfüllung öffentlicher Aufgaben kann es kein Betriebs- oder Geschäftsgeheimnis geben. Kalkulati-

onsunterlagen sind Teil einer solchen Aufgabenerfüllung.

17.7 Gebühren für Zugangsgewährung

"Für Amtshandlungen, die aufgrund dieses Gesetzes vorgenommen werden, werden Gebühren erhoben." So schlicht formuliert es das Informationsfreiheitsgesetz NRW (IFG NRW). Abschreckende Gebühren hingegen lassen weder das IFG NRW selbst noch die einschlägige Verwaltungsgebührenordnung zu.

Als abschreckend sah es ein Bürger zu Recht an, dass er von der Landschaftsbehörde eines Kreises für eine schriftliche Auskunft in Form einer DIN-A3-Kopie nebst einem kurzem Anschreiben 100 Euro zahlen sollte. Die Behörde bedauerte zwar die Konfliktsituation, die daraus resultiere, dass das Gesetz den Bürgerinnen und Bürger einerseits einen weitgehenden Auskunftsanspruch gegenüber Behörden einräume, die Auskunftserteilung aber andererseits grundsätzlich kostenpflichtig mache, stellte jedoch minutiös sämtliche Bearbeitungsschritte zur Erledigung der Anfrage in Rechnung:

- Annahme und Sichtung der E-Mail - Weiterleitung wegen Unzuständigkeit - Überprüfung der Rechtmäßigkeit des Antrags	25 Min.
- Suche nach dem richtigen Aktenzeichen - Erteilung eines Suchauftrages an das Register - Suche nach der Akte im Register - Abholen der Akte aus dem Register	25 Min.
- Sichten der umfangreichen Akte und Markieren der Schriftstücke in der Akte	25 Min.
Kopieren der Schriftstücke aus der Akte	5 Min.
- Berechnung der Gebühr und Fertigung einer Gebührenberechnung	10 Min.
Fertigung eines Gebührenbescheides	10 Min.
Aufgabe zur Post	5 Min.
- Rückgabe der Akte an das Register - Ablage im Register	15 Min.

Die Rechtslage stellt sich demgegenüber so dar: Nicht in jedem Fall ist die Erteilung einer schriftlichen Auskunft nach der Verwaltungsgebührenordnung zum IFG NRW kostenpflichtig, sondern nur dann, wenn eine umfassende schriftliche Auskunft mit erheblichem Vorbereitungsaufwand erstellt wird.

Um einen erheblichen Vorbereitungsaufwand in Rechnung stellen zu können, muss der Frage nachgegangen werden, welcher zeitliche Aufwand für die Prüfung notwendig war, ob und welche öffentlichen oder privaten Belange einer Offenlegung entgegenstehen. Hierzu gehört etwa die Feststellung, welche Informationen in einer umfangreichen Akte Betriebs- und Geschäftsgeheimnisse sind. Oder wenn personenbezogene Daten zu schützen sind, so ist der Aufwand für deren Auffinden und Schwärzen dann "erheblich", wenn das länger als eine Viertelstunde dauert. Aus der oben stehenden Tätigkeitstabelle kommen dafür lediglich die Posten "Sichten der umfangreichen Akte und Markieren der Schriftstücke" mit der Zeitberechnung von 25 Minuten und "Kopieren der Schriftstücke" mit 5 Minuten in Betracht. Die übrigen Tätigkeitsberechnungen von 90 Minuten können als Vorbereitungsaufwand für die Auskunftserteilung nicht herangezogen werden. Außerdem stellt auch die rechtliche Prüfung, ob das IFG NRW Anwendung findet oder was unter dem Tatbestandsmerkmal Betriebs- und Geschäftsgeheimnis abstrakt zu verstehen ist, keinen die Auskunftserteilung vorbereitenden Aufwand dar.

Diese Differenzierung hatte die Kreisverwaltung nicht angestellt. Vielmehr hat sie sich ganz allgemein darauf berufen, dass Fragen der "Rechtsanwendung" bei allen behördlichen Entscheidungen Hauptbestandteil des Aufwandes sei, der sich in den Verwaltungsgebühren niederschlage. Mit dieser alles umfassenden Begründung wollte sie sogar die Zeit für die Gebührenberechnung und die Erstellung des Gebührenbescheids anrechnen.

Für die Erteilung der schriftlichen Auskunft in Form einer einzelnen DIN-A3-Kopie konnte somit ein erheblicher Vorbereitungsaufwand nicht ausgelöst worden sein. Letztendlich gelang es, dass die Gebühr von 100 auf 10 Euro gesenkt wurde.

➡ Bei der Erhebung von Gebühren darf nur die Prüfung berücksichtigt werden, ob die gewünschten Informationen offen gelegt werden können.

17.8 Umweltinformationsgesetz Nordrhein-Westfalen

Nach langwierigen Querelen bei der Umsetzung der europäischen Umweltinformationsrichtlinie und einer Phase der Direktwirkung dieser Richtlinie ist das Umweltinformationsgesetz NRW (UIG NRW) in Kraft.

Das UIG NRW verweist im Wesentlichen auf das Umweltinformationsgesetz des Bundes. Allerdings ist die Festlegung der nordrhein-westfälischen informationspflichtigen Stellen zu detailliert und in Teilen auch umständlich. Positiv ist, dass die Definition dessen, was Umweltinformationen umfasst, sehr weit reicht; sie bezieht sogar Angaben über den Zustand der menschlichen Gesundheit und Sicherheit, die Lebensbedingungen des Menschen sowie Zustandsbeschreibungen von Kulturstätten und Bauwerken mit ein. Die Umweltinformationen über Maßnahmen oder Tätigkeiten, die sich auf die Umweltbestandteile oder auf Faktoren wie zum Beispiel Stoffe, Energie, Lärm und Strahlung oder Abfälle auswirken oder wahrscheinlich auswirken, kann durch die Rechtsprechung weit ausgelegt werden. So ist beispielsweise die Gewährung einer staatlichen Exportkreditsicherung im Bereich der Energieerzeugung darunter subsumiert worden (siehe Verwaltungsgericht Berlin, Beschluss vom 10. Januar 2006, NVwZ 2006, 850 ff.). Auch hinsichtlich der Ablehnungsgründe ist positiv zu verzeichnen, dass der Wunsch nach Informationen über Emissionen nicht etwa unter Berufung auf den Schutz personenbezogener Daten oder den Schutz von Betriebs- oder Geschäftsgeheimnissen unerfüllt bleiben darf.

Beim Zugang zu Umweltinformationen ist zunächst der Informationsanspruch nach dem UIG NRW zu prüfen. Kann danach kein Informationszugang gewährt werden, greift daneben immer noch das allgemeine Informationsfreiheitsgesetz NRW. Sind die dort normierten Anspruchsvoraussetzungen gegeben und steht kein gesetzlicher Ablehnungsgrund entgegen, muss der Informationszugang gewährt werden.

- Das Umweltinformationsgesetz NRW geht dem Informationsfreiheitsgesetz NRW nur im ersten Schritt vor, so dass bei Ablehnung eines Informationszugangs nach dem Umweltinformationsgesetz NRW die Prüfung eines

Anspruches nach dem Informationsfreiheitsgesetz NRW bleibt.

17.9 Verbraucherinformationsgesetz

Wollen Sie wissen, welches Mehl Ihre Bäckerei benutzt oder wie frisch das Hackfleisch ist? Dann sollten Sie direkt danach fragen. Wird Ihre Frage nicht beantwortet, müssen Sie sich entscheiden, ob Sie woanders kaufen. Wollen Sie aber wissen, wann die Bäckerei oder Metzgerei das letzte Mal kontrolliert worden ist und mit welchen Ergebnissen? Dann muss Ihnen die Ordnungsbehörde Auskunft geben.

Nach dem Verbraucherinformationsgesetz sind leider nicht die Unternehmen selbst auskunftspflichtig, sondern nur die Verwaltungsbehörden und die von ihnen beauftragten Personen des Privatrechts, die mit dem Vollzug des Lebensmittel-, Futtermittel- und Bedarfsgegenständegesetzbuches betraut sind. In Nordrhein-Westfalen wurde die Auskunftspflicht auch auf die kommunalen Behörden erstreckt.

Alle Informationen sind zugänglich, die bei diesen Behörden vorliegen. Das sind vor allem Informationen über Verstöße gegen das Lebensmittel- und Futtermittelrecht und die dagegen ergriffenen Maßnahmen sowie Informationen über Gefahren oder Risiken, die von Lebensmitteln und Gegenständen des täglichen Bedarfs ausgehen. Alle natürlichen oder juristischen Personen des Privatrechts haben den Informationsanspruch. Allerdings können die befragten Stellen entscheiden, ob sie Auskunft geben, Einsicht in ihre Unterlagen gewähren oder Kopien aushändigen. Zudem gibt es – wie immer – Ausnahmen vom Informationsrecht. Diese gesetzlich festgelegten Ausnahmen sind zahlreich, dürfen zumindest aber nur eng ausgelegt werden.

Es ist unbestreitbar, dass der Anspruch auf gesundheitsbezogene Verbraucherinformationen einen ersten Schritt zu mehr Transparenz für die Verbraucherinnen und Verbraucher bedeutet. Aber der Informationszugang muss im Interesse der Verbraucherinnen und Verbraucher auf weitere Bereiche ausgeweitet werden. So fehlt beispielsweise ein unmittelbarer Informationsanspruch auch gegenüber den Unter-

nehmen selbst. Außerdem sollten alle Produkte des täglichen Lebens und Dienstleistungen in diesem Umfeld einbezogen sein.

➧ Im Interesse der Verbraucherinnen und Verbraucher müssen weitere Verbesserungen des Informationszuganges erreicht werden. Auch ohne gesetzliche Pflicht können schon jetzt die Verwaltungen zunehmend verbraucherrelevante Informationen ins Internet stellen.

17.10 Agrar- und Fischereifonds-Informationen-Gesetz

Wer sind die "dicksten Bauern", die die "größten Kartoffeln" aus öffentlichen Steuermitteln bekommen? Wer wie viele Agrarsubventionen erhält, wird demnächst im Internet veröffentlicht.

Zur Umsetzung europarechtlicher Vorgaben hat der Bundesgesetzgeber ein Agrar- und Fischereifonds-Informationen-Gesetz (AFIG) verabschiedet, dessen Ziel es ist, mehr Transparenz bei der Verwendung von europäischen Subventionen zu schaffen. Das Gesetz stellt unter Transparenzgesichtspunkten einen richtigen Schritt dar, weist aber noch Defizite im Hinblick auf den Umfang der Veröffentlichungspflichten auf.

Inhaltlicher Schwerpunkt des Gesetzes ist die Veröffentlichung von Informationen über die Empfänger oder Empfängerinnen von Mitteln aus dem Garantiefonds für die Landwirtschaft, dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raumes und dem Europäischen Fischereifonds. Behörden von Bund und Ländern sind verpflichtet, die Namen von Subventionsempfängerinnen und -empfängern, Informationen zur örtlichen Gemeinde, die Postleitzahl sowie die Höhe der Beiträge, die der Empfänger oder die Empfängerin im betreffenden Haushaltsjahr erhalten hat, auf einer gemeinsamen, von der Bundesanstalt für Landwirtschaft und Ernährung betriebenen Internetseite zu veröffentlichen. Die Zahlungsempfänger sind auf der Internetseite der Bundesanstalt unter www.agrar-fischerei-zahlungen.de veröffentlicht. In Nordrhein-Westfalen waren Angaben über Subventionszahlungen bereits nach dem Informationsfreiheitsgesetz NRW zugänglich gemacht worden.

Unter dem Blickwinkel der Informationsfreiheit ist die mit dem AFIG geschaffene Transparenz bei geleisteten Zahlungen an die einzelnen Empfänger oder Empfängerinnen zu begrüßen. Mit dem Gesetz wird der Gebrauch der Fondsmittel öffentlich nachvollziehbar. Allerdings ist dem Transparenzgedanken insoweit nicht ausreichend Rechnung getragen worden, als hinter den Angaben über die Direktbeihilfe aus dem Garantiefonds, über eine sonstige Direktbeihilfe oder über Mittel für die Entwicklung des ländlichen Raumes für die Bürgerinnen und Bürger nicht zu erkennen ist, welchem landwirtschaftlichen Zweck – etwa einer Umweltmaßnahme oder einer extensiven Dauergrünlandnutzung – die gewährte Beihilfe konkret dienen sollte. Eine kritische öffentliche Prüfung, inwieweit die Fördermittel ordnungsgemäß vergeben und verwendet wurden, erfordert deshalb immer noch eine Nachfrage bei der Landwirtschaftskammer Nordrhein-Westfalen nach dem IFG NRW.

➡ Eine differenzierte Veröffentlichung der mit den gezahlten Beihilfen verfolgten landwirtschaftlichen Zwecken wäre sehr zu begrüßen.

Anhang

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

73. Datenschutzkonferenz am 8./9. März 2007

◆ Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommu-nikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und

Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt

wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.
- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.
- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.
- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

◆ Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. "Trojaner" heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzge-

ber, es beim bisherigen Rechtszustand des "offenen Visiers" zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

◆ GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten

muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

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

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

◆ Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

◆ Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u.a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

Entschließung zwischen den Datenschutzkonferenzen

◆ Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln (8. Juni 2007)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrs-

daten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

74. Datenschutzkonferenz am 25./26. Oktober 2007

◆ Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um "Online-Durchsicht" als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z.B. die drohende

Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

◆ Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses

Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.
- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform "Elster" für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z.B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

◆ Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchen-

übergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

◆ Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Poli-

zei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können - auch wenn die Betroffenen über die Umstände informiert wurden - diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen - zusätzlich - zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u.a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

75. Datenschutzkonferenz am 3./4. April 2008

◆ Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme ("Online-Durchsuchung") in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den inter-nationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur "Online-Durchsuchung" vom 27. Februar 2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur "Online-Durchsuchung", sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

◆ Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.3.2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terro-

rismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

◆ Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzu-

decken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und –sparsamkeit Rechnung getragen werden.

◆ Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektroni-

sche Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms "Technologien für die Informationsgesellschaft" gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z.B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

◆ Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig

erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer "elektronischen Ausforschung" schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

    a. Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

b. Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

c. Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

d. Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

e. Für die Durchführung von "Quellen-Telekommunikations-überwachungen", die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z.B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

◆ Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte "Zentralstelle" übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z.B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter "allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und –Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe "ins

Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

◆ Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft ("fremdbestimmte Selbstauskunft") selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche "Einwilligung des Betroffenen" ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem "Führungszeugnis" dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum "Fragerecht des Arbeitgebers" getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein "Führungszeugnis" aufzunehmenden Daten – auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem "Führungszeugnis" nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

- **Medienkompetenz und Datenschutzbewusstsein in der jungen "online-Generation"**

  1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge "online-Generation", die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

  2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

  3. Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto "Datenschutz macht Schule" wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z.B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräfte.

  4. Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema "Datenschutz" aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

  5. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung

der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter - deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

Entschließung zwischen den Datenschutzkonferenzen

◆ Entschlossenes Handeln ist das Gebot der Stunde (16. September 2008)

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt - zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres - auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden. Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und

Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden."

76. Datenschutzkonferenz am 6./7.November 2008

◆ Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen - grundsätzlich auch alle öffentlichen Stellen - gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbe-

hörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

◆ Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem "Datenschutzgipfel" im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim "Datenschutzgipfel" gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22. Oktober 2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

◆ Besserer Datenschutz bei der Umsetzung der "Schwedischen Initiative" zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. "Schwedische Initiative") vom 18. Dezember 2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der "Schwedischen Initiative" verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.
- Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,
- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,
- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,
- vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,
- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

◆ Gegen Blankettbefugnisse für die Software-Industrie

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach "jede natürliche oder juristische Person mit einem berechtigten Interesse" berechtigt sein soll, Verkehrsdaten zu verarbeiten, um "technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung" zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die "Informationssicherheit" rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

◆ Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre.

Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (siehe ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z.B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staats-

anwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belastungen in der Praxis – unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen. Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik - unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage - auch im Vergleich zu anderen möglichen Maßnahmen - mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

◆ Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz-

und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

◆ Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen. Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.
- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.
- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.
- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder

nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

◆ Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25. Juni 2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden, (z.B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.
- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.
- Schlüssel zur Ver– und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver– und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.
- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.
- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs und Signaturverfahren genügen.
- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

◆ Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u.a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1. Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.
2. Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3. Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)

Sitzung vom 19./20. April 2007 (Düsseldorfer Kreis)

◆ Kreditscoring / Basel II

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich beurteilen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft wie folgt:

I. Welche personenbezogenen Merkmale dürfen für die Berechnung des Scores genutzt werden?

1. Es dürfen nur Parameter genutzt werden, deren Bonitätsrelevanz mittels eines den wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz eines Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.

2. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen daher nur Daten in ein Scoring-Verfahren eingestellt werden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des KWG oder des WpHG erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden. (Da sensitive Daten im Sinne des § 3 Abs. 9 BDSG nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben und verarbeitet werden, dürfen diese auch nicht in die Score-Berechnung einfließen.)

3. Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn das Kreditinstitut die Möglichkeit hat, konkrete, unmittelbar bonitätsrelevante Daten zu erheben, darf es nicht auf Daten zurückgreifen, die nur Indizcharakter haben. Soweit ein berechtigtes Interesse der Banken vorliegt, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen

normativen Prozess dar; die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen ist. Bei der Abwägung können die gesetzgeberischen Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG herangezogen werden. § 10 Abs. 1 KWG gilt zwar als bankenaufsichtsrechtliche Norm nur für die Erhebung und Verarbeitung personen- bezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potentiellen) Kundinnen und Kunden. Die Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG können allerdings als gesetzgeberisches Leitbild in die Auslegung des BDSG einfließen. Das gilt insbesondere für die Anforderungen an Scoring-Merkmale. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Abs. 1 Satz 6 KWG aufgeführten Regelbeispiele. So sind Angaben zur Staatsangehörigkeit bereits aufgrund des ausdrücklichen Verbots in § 10 Abs. 1 Satz 3 KWG als Score-Merkmale ausgeschlossen. Bei der Abwägung sind darüber hinaus Wertungen des Grundgesetzes wie auch des einfachen Rechts daraufhin zu überprüfen, ob eine Benachteiligung der (potentiellen) Kundinnen und Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.

4. Auch wenn sich Basel II vornehmlich mit der Eigenkapitalhinterlegung der Institute befasst, wird der Einsatz von Scoring-Verfahren zunehmend dazu führen, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und sind keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert.

II. Wie transparent müssen die Bewertungen für die Betroffenen sein?

Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,

1. welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen;

2. welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden;

3. welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung bzw. den Grad ihres Einflusses auf den konkreten Score- Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.

Darüber hinaus ist bei der Anwendung von Scoring-Verfahren der § 6a BDSG zu beachten.

◆ Internationaler Datenverkehr

1. Der Düsseldorfer Kreis beschließt das anliegende Positionspapier zum internationalen Datenverkehr. Der BlnBDI wird gebeten, das Papier als Vorsitzender der AG "Internationaler Datenverkehr" an die damals beteiligten Wirtschaftsvertreter zu versenden, die zugleich darauf

hingewiesen werden sollen, dass weitere Fallkonstellationen in einer allgemein zugänglichen Handreichung näher dargestellt werden.

Die im Positionspapier genannten Auffassungen können von den Aufsichtsbehörden bei der Beratung auch anderer Wirtschaftsvertreter genutzt werden.

2. Der Düsseldorfer Kreis beschließt ferner die anliegende Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Den Aufsichtsbehörden wird anheim gestellt, die Handreichung im Internet zu veröffentlichen oder auf andere Weise interessierten Unternehmen zugänglich zu machen.

◆ Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit die selben datenschutzrechtlichen Vorgaben zu beachten haben wie die "Verbraucherauskunfteien".

Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Abs. 1 BDSG erheben. Denn bei Positivdaten - das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben - überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihre Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

◆ Adressänderungen durch Versandhandelsunternehmen

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:

Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderung an angeschlossene Unternehmen zum Zwecke des Adressabgleichs, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß $ 4a BDSG zulässig.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandeslunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

◆ Mahnung durch Computeranruf

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig.

Sitzung vom 8./9. November 2007 (Düsseldorfer Kreis)

◆ Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener – auch mandatsbezogener – Daten durch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen. Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) – auch hinsichtlich mandatsbezogener Daten – auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43a Abs. 2 BRAO Schweigepflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Abs. 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG nicht eingeschränkt.

◆ Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.

Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein so genannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben er-

rechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.

Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring- Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen.

Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen. Nach Auffassung des Düsseldorfer Kreises bedarf der vorliegende Gesetzentwurf allerdings einer grundlegenden Überarbeitung, um das Ziel der Stärkung der Rechte der Betroffenen auch tatsächlich zu erreichen.

Dabei muss insbesondere sichergestellt werden, dass die bei Auskunfteien gesammelten Daten die Erstellung umfassender Persönlichkeitsprofile von Betroffenen nicht zulassen. Darüber hinaus ist gesetzlich eindeutig zu regeln, dass die Einholung einer Bonitätsauskunft auch in Zukunft an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die im Entwurf derzeit vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse einschließlich der Vermeidung allgemeiner Vertragsrisiken ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen unverhältnismäßig beeinträchtigen.

Des Weiteren muss eindeutig klargestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Scorewerts einbezogen werden dürfen. Im Übrigen dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden.

Sitzung vom 17./18. April 2008 (Düsseldorfer Kreis)

◆ Internet-Portale zur Bewertung von Einzelpersonen

1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.

2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.

3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht

der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

◆ Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nr. 1a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.

Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z.B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines "Kundenkontos" rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt. Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Hinweis:

Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

◆ Datenschutzkonforme Gestaltung sozialer Netzwerke

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind.

Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

- Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für

die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

- Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob – und wenn ja, welche – Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.
- Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.
- Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.
- Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.
- Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.
- Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen – z. B. für die Verfügbarkeit von Profildaten für Dritte – eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.
- Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest

automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

Sitzung vom 13./14. November 2008 (Düsseldorfer Kreis)

◆ Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden.

Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.

◆ Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren. Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, so dass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt, und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen.

Darüberhinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.

Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.

Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

◆ Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen stärken (11. Juni 2007)

Die Wahrung von Betriebs- und Geschäftsgeheimnissen hat für Unternehmen eine besondere Bedeutung. Betriebs- und Geschäftsgeheimnisse können den Wert eines Unternehmens und seine Stellung am Markt erheblich beeinflussen. Bei ihrer Aufgabenerfüllung erhalten öffentliche Stellen bisweilen Kenntnis von Betriebs- und Geschäftsgeheimnissen. Als Bestandteil amtlicher Aufzeichnungen unterliegen die Betriebs- und Geschäftsgeheimnisse den Informationsfreiheitsgesetzen, sie werden hier aber durch einen Ausnahmetatbestand geschützt.

Die Konferenz der Informationsfreiheitsbeauftragten stellt fest, dass die Auslegung und Anwendung des Ausnahmetatbestandes das Informationsfreiheitsrecht der Bürgerinnen und Bürger übermäßig einschränkt. So führt oft die beträchtliche Rechtsunsicherheit der Behörden bei der Anwendung dieser Bestimmung zu einer besonders restriktiven Auskunftspraxis. Aber nicht jedes Unternehmensdatum ist ein Betriebs- oder Geschäftsgeheimnis. Nach der Rechtsprechung des Bundesgerichtshofes zum Wettbewerbsrecht müssen hierfür folgende Voraussetzungen kumulativ vorliegen:

Es muss sich um Tatsachen handeln, die

- im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb stehen,
- nur einem begrenzten Personenkreis bekannt und damit nicht offenkundig sind,
- (subjektiv) nach dem erkennbaren Willen des Unternehmens und
- (objektiv) nach dessen berechtigten und schutzwürdigen wirtschaftlichen Interessen geheim gehalten werden sollen (insbesondere, wenn bei Offenbarung ein Schaden eintritt).

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb den Bundes- und die Landesgesetzgeber auf, die gesetzlichen Regeln zu ergänzen und zu präzisieren.

1. Es gibt Betriebs- oder Geschäftsgeheimnisse, bei denen das öffentliche Interesse an der Offenbarung den Schutzbedarf überwiegt. Soweit daher eine Abwägungsklausel in den gesetzlichen Grundlagen noch nicht vorhanden ist, soll sie aufgenommen werden. Dabei muss auch verdeutlicht werden, dass Verträge, die mit der öffentlichen Hand geschlossen werden, nicht grundsätzlich geheimhaltungsbedürftig sind: Wer mit dem Staat Geschäftsbeziehungen eingeht, muss sich darüber im Klaren sein, dass staatliches Handeln besonderen Kontrollrechten unterliegt und damit nicht alle Vertragsinhalte geheim bleiben können.

2. Nach dem Beispiel des Gentechnik- und Chemikalienrechts sollte in Form eines Kataloges klargestellt werden, welche Unternehmensinformationen keine Betriebs- oder Geschäftsgeheimnisse darstellen (z. B. rechtswidriges Verhalten).

3. Kennzeichnungs- und Darlegungspflichten des Unternehmens können die Prüfung des Geheimhaltungsinteresses erleichtern. Vergleichbare Regelungen existieren bereits in anderen Bereichen.

◆ Transparenz in der Finanzverwaltung (11. Juni 2008)

Die Informationsfreiheitsgesetze nehmen die Finanzverwaltung nicht von ihrem Anwendungsbereich aus. Deshalb gilt auch hier: Die grundsätzliche Offenheit der amtlichen Informationen gilt, sofern nicht eine in diesen Gesetzen geregelte Ausnahme (z. B. das Steuergeheimnis) greift.

In der Vergangenheit haben verschiedene Finanzbehörden häufig einen Anspruch der Bürgerinnen und Bürger auf Einsicht in eigene Steuerunterlagen sowie Verwaltungsvorgänge in das Behördenermessen gestellt. Der Bundesgesetzgeber habe mit dem Erlass der Abgabenordnung das steuerliche Verfahren abschließend geregelt und dort durch "absichtsvolles Unterlassen" bewusst auf eine Regelung verzichtet. Nachdem das Bundesverfassungsgericht mit seinem Beschluss vom 10. März 2008 (1 BvR 2388/03) den Anspruch auf Informationen aus der eigenen Steuerakte für verfassungsrechtlich geboten erklärt hat, ist diese Argumentation nicht mehr länger haltbar.

Nichts anderes kann für die Anwendung der Informationsfreiheitsgesetze gelten, die jedem Menschen einen Anspruch auf Zugang zu den bei öffentlichen Stellen vorhandenen Informationen sichern. Der Zugang zur Information und die Transparenz behördlicher Entscheidungen ist eine wichtige Voraussetzung für die effektive Wahrnehmung von Bürgerrechten.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Finanzverwaltungen des Bundes und der Länder auf, die Informationsfreiheitsgesetze anzuwenden und in ihren nachgeordneten Bereichen durchzusetzen.

◆ Die Europäische Union braucht nicht weniger, sondern mehr Transparenz (30. Juni 2008)

Mit der Verordnung 1049/2001 ist erstmals allen Unionsbürgerinnen und –bürgern der freie Zugang zu Dokumenten der Europäischen Union eröffnet worden. Die Verordnung hat unmittelbare Wirkung in allen Mitgliedstaaten, so dass auch deutsche Behörden, bei denen solche Dokumente vorliegen, sie beachten müssen.

Die Europäische Kommission hat nun allerdings Vorschläge vorgelegt, die – neben marginalen Verbesserungen - zu einer drastischen Einschränkung des Zugangs zu europäischen Dokumenten führen würden. Sie plant, den Zugang zu Dokumenten der EU-Institutionen künftig nur noch dann zu gestatten, wenn sie entweder bereits einem bestimmten Empfängerkreis übermittelt oder „registriert“ worden sind. Damit hätten die europäischen Behörden es selbst in der Hand, zu bestimmen, welche Dokumente sie herausgeben. Darüber hinaus sollen Informationen, die die EU-Institutionen von außen im Rahmen laufender Verfahren erhalten, auch nach deren Abschluss selbst dann unter Verschluss

gehalten werden können, wenn an ihrer Offenlegung ein überwiegendes öffentliches Interesse besteht. Schließlich sollen die EU-Institutionen Dokumente geheim halten dürfen, die sie zur Vorbereitung von Entscheidungen nur einem bestimmten Kreis extern Beratender zugänglich gemacht haben.

Die Informationsfreiheitsbeauftragten in Deutschland sehen die Gefahr, dass bei einer Annahme dieser Vorschläge eine massive Einschränkung der gebotenen Transparenz des Handelns europäischer Institutionen die Folge wäre. Sie teilen die Kritik, die der Europäische Bürgerbeauftragte in seiner Stellungnahme gegenüber dem Ausschuss für Bürgerrechte, Justiz und Inneres des Europäischen Parlaments am 2. Juni 2008 geübt hat (Presseerklärung deutsch. Text der Stellungnahme nur englisch). Die deutschen Informationsfreiheitsbeauftragten fordern deshalb das Europäische Parlament und den Rat auf, den Vorschlägen der Kommission nicht zu folgen und stattdessen das Transparenzniveau bei den Institutionen der Europäischen Union spürbar zu erhöhen.

◆ Die neue Konvention des Europarats zur Informationsfreiheit so bald wie möglich unterzeichnen und ratifizieren! (3./4. Dezember 2008)

Der Ministerausschuss des Europarats hat am 27. November 2008 den Entwurf einer Konvention über den Zugang zu amtlichen Dokumenten beschlossen. Mit ihrem Inkrafttreten wird die Konvention alle Vertragsstaaten verpflichten, jedem Menschen ein allgemeines Recht auf gebührenfreien Zugang zu Behördeninformationen einzuräumen, ohne dass dies begründet werden muss.

Es ist zu begrüßen, dass damit erstmals weltweit ein völkerrechtlich verbindlicher Vertrag zur Informationsfreiheit auf den Weg gebracht worden ist.

Jetzt ist die Bundesregierung aufgefordert, die Konvention so bald wie möglich zu unterzeichnen und dem Bundestag zur Ratifikation zuzuleiten, damit die Konvention schnell in Kraft treten kann. Die wenigen verbleibenden Bundesländer, die noch immer kein Informationsfreiheitsgesetze verabschiedet haben, müssen ihre Haltung jetzt dringend revidieren, damit die Bundesrepublik nicht zum Schlusslicht unter den Mitgliedstaaten des Europarats wird.

Stichwortverzeichnis

Hinweise auf Infomaterial

Neben den jeweiligen aktuellen und früheren Datenschutz- und Informationsfreiheitsberichten können Sie bei uns weiteres Infomaterial kostenlos anfordern. Dazu gehören Broschüren und Faltblätter allgemeiner und spezieller Natur, beispielsweise zu den Themen Videoüberwachung, Informationsfreiheit oder zu Datensicherheitsfragen.

Außerdem dokumentieren wir unsere jährlichen Tagungen. Die Dokumentationsbände aus früheren Jahren sind teilweise in Papierform vergriffen, aber elektronisch unter www.ldi.nrw.de verfügbar. Derzeit als Paperback erhältlich sind die Tagungsbände:

- "Die Gedanken sind frei... Hirnforschung und Persönlichkeitsrechte" (2006)
- "Persönlichkeit im Netz: Sicherheit – Kontrolle – Transparenz" (2007)
- "GPS, Internet und Video – Datenschutz am Arbeitsplatz" (im Erscheinen)

Eine vollständige Übersicht und ein Online-Bestellformular finden Sie auf unserer Homepage unter www.ldi.nrw.de.

Sie erreichen uns auch:

- per Post: Landesbeauftragte für Datenschutz
und Informationsfreiheit NRW
Kavalleriestr. 2-4
40213 Düsseldorf
- per E-Mail: pressestelle@ldi.nrw.de
- per Fax: 0211/3842410
- per Telefon: 0211/38424-0