Zwanzigster Datenschutz- und Informationsfreiheitsbericht

des

Landesbeauftragten für Datenschutz

und Informationsfreiheit

Nordrhein-Westfalen

Ulrich Lepper

für die Zeit vom 1. Januar 2009

bis zum 31. Dezember 2010

20. DIB LDI NRW

Herausgeber:

Landesbeauftragter für Datenschutz
und Informationsfreiheit
Nordrhein-Westfalen
Ulrich Lepper
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.

Zitiervorschlag: 20. DIB LDI NRW
ISSN: 0179–2431
Düsseldorf 2011

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

1 Vorbemerkungen

Mit dem vorliegenden Bericht gebe ich zum ersten Mal nach meiner Wahl zum Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen einen Überblick über die Tätigkeit meiner Behörde und über Entwicklungen des Datenschutzes und der Informationsfreiheit.

Der Berichtszeitraum ist in mehrfacher Beziehung von Umbrüchen gekennzeichnet:

Obwohl das "informationstechnische Jahrhundert" mit seinen Chancen und Risiken längst begonnen hat, wächst allmählich erst das Bewusstsein für die drängenden Fragen zur Sicherung der Privatsphäre. Der insbesondere im Berichtszeitraum zuweilen heftig geführte gesellschaftliche Diskurs zu grundsätzlichen Fragen – ob aus Anlass der Veröffentlichung von Hausfassaden im Internet oder zu Bewertungsportalen, sozialen Netzwerken oder zur Vorratsdatenspeicherung, zum Umgang mit Kontendaten oder zum Beschäftigtendatenschutz – lässt hoffen, dass in unserer Gesellschaft das Recht auf informationelle Selbstbestimmung mehr noch als bisher wie selbstverständlich als eine der grundlegenden Bedingungen für staatliches und privates Handeln angesehen wird.

Im Focus des Datenschutzes steht nicht mehr schwerpunktmäßig die Verarbeitung personenbezogener Daten durch den Staat. Vielmehr verschieben sich die Schwerpunkte hin zur Wirtschaft, die mit weiter zunehmender Dynamik in außergewöhnlich vielfältiger Weise personenbezogene Daten von Kundinnen und Kunden sowie von Verbraucherinnen und Verbrauchern verarbeitet.

Als Akteur der Datenverarbeitung ist neben den Staat und die Unternehmen – fast unbeachtet – nunmehr auch das Individuum getreten. Überall auf der Welt kann jeder freie Mensch mit Zugang zum Internet ohne nennenswerten Aufwand personenbezogene Daten über sich und Andere räumlich und zeitlich ohne jede Begrenzung verbreiten oder zu deren Verbreitung beitragen. Hier fühlt sich kaum jemand an Standards oder Regelungen gebunden, auch was den Umgang mit eigenen Daten anbelangt. Die sich ständig weiter entwickelnden Möglichkeiten zur Informationsverarbeitung mit hohem Verbreitungsgrad lassen das Spannungsverhältnis zwischen der Freiheit der Meinungsäußerung

oder der allgemeinen Handlungsfreiheit und dem Recht auf informationelle Selbstbestimmung in einem ganz anderen Licht erscheinen.

Nicht erst die Aufsehen erregenden Veröffentlichungen von WikiLeaks werfen ein Schlaglicht auf die Informations- und – damit einhergehend – auf die Gestaltungsmacht von Einzelnen oder von Gruppen. Zugleich beleuchtet der Vorgang das sich deutlich stärker entwickelnde Bedürfnis in der Gesellschaft nach Informationszugang.

Schließlich hat der Europäische Gerichtshof am 9. März des vergangenen Jahres eine für den Datenschutz wichtige Entscheidung getroffen, die mit Blick auf die EU-Datenschutzrichtlinie weitergehende Anforderungen an die Unabhängigkeit der Datenschutzbehörden in Deutschland stellt. Danach müssen die Datenschutzbehörden ihre Aufsichtstätigkeit auch in Bezug auf private Stellen in völliger Unabhängigkeit wahrnehmen können. Weder eine Rechts- noch eine Fachaufsicht, wie sie nach geltendem Recht das Ministerium für Inneres und Kommunales im nicht-öffentlichen Bereich mir gegenüber ausüben kann, entsprechen danach den Vorgaben der Richtlinie. Der Europäische Gerichtshof unterstreicht damit die Sonderstellung der Datenschutzkontrolle im System des staatlichen Aufgabenvollzugs.

Je mehr unser Leben von Kommunikation und Vernetzung in immer neuen, sich ständig verändernden Erscheinungsformen und Ausprägungen bestimmt ist, desto mehr ist auf den Schutz personenbezogener Daten zu achten. Datenschutz verhindert nach meinem Verständnis weder Wettbewerb noch Innovation, sondern kann selbst zu einem Wettbewerbsfaktor werden und neue Lösungen ermöglichen. Datenschutz als Ausdruck eines modernen, sich den Anforderungen des "informationstechnischen Jahrhunderts" stellenden Rechtsstaates bildet auch nicht die Kehrseite der Inneren Sicherheit, sondern ergänzt diese. In diesem Sinne sehe ich den Datenschutz und den sich um dieses Thema rankenden öffentlichen Diskurs als eine kulturelle Errungenschaft, die unser Land besonders auszeichnet. Daher kann ich nur dazu ermutigen, die hierzulande gewonnenen konstruktiven Erfahrungen proaktiv in Überlegungen der EU-Kommission einzubringen, die den Datenschutz in den Mitgliedstaaten der Europäischen Union weiter zu entwickeln beabsichtigt.

Vor diesem Hintergrund richte ich auch an die Unternehmen im Land den dringenden Aufruf, den Schutz der Daten von Kundinnen und

Kunden – wenn nicht aus Überzeugung, dann jedenfalls aus eigenem geschäftlichen Interesse – als Unternehmensziel ernst zu nehmen und sichtbar zu machen und nicht als lästiges, nur Kosten verursachendes Beiwerk zu verstehen. Mit Nachdruck muss ich dies auch in Bezug auf den Schutz der Daten von Beschäftigten in den Unternehmen fordern.

Datenschutz schreibt den Bürgerinnen und Bürgern nicht vor, Geschäftsideen, Produkte, Innovationen oder neue Dienstleistungen gutzuheißen oder zu verwerfen. Dies zu entscheiden ist Sache der einzelnen Person. Datenschutz stellt wohl aber sicher, dass die Bürgerinnen und Bürger bzw. Kundinnen und Kunden im Umgang mit ihren Daten nicht fremdbestimmt sind, sondern ihr Recht auf informationelle Selbstbestimmung in eigener Verantwortung auch wahrnehmen können. Daher ist Aufklärung gerade in Zeiten von Neuerungen ein zentrales Anliegen meiner Behörde.

Datenschutz und Informationsfreiheit sind zwei Seiten einer Medaille. Die Medaille steht für die Freiheit der Bürgerinnen und Bürger. Im öffentlichen Bereich gilt es, aus dem Blickwinkel des Datenschutzes die Informationsverarbeitung des Staates auf das für die jeweilige Aufgabe erforderliche Wissen zu begrenzen und die Zweckbindung gesammelter Daten sicherzustellen, während ein – geordneter – Informationszugang darauf angelegt sein muss, die mündigen Bürgerinnen und Bürger in die Lage zu versetzen, sich ein eigenes Bild von Entscheidungsprozessen im öffentlichen Bereich zu machen. Auf diesem Feld ist noch viel zu tun.

Die Entscheidung des Europäischen Gerichtshofes zur Unabhängigkeit der Datenschutzbehörde kann ich nur begrüßen. Die gebotene Novellierung des Datenschutzgesetzes des Landes muss schon wegen meiner auch Landesministerien umfassenden Kontrollzuständigkeit den derzeitigen organisatorischen Status der Datenschutzkontrolle als einer auf der Ebene einer obersten Landesbehörde agierenden Verwaltungseinheit erhalten. Ferner müssen im Interesse einer geordneten Personalentwicklung und eines lebensnahen Datenschutzes Rotationsmöglichkeiten für das hier tätige Personal in die Landesverwaltung und umgekehrt beibehalten werden. Schließlich ist darauf zu achten, dass nicht zu Lasten der Kernaufgaben in meiner Behörde eigene Strukturen für Aufgaben in den Bereichen Personal und Verwaltung aufgebaut werden müssen, obwohl diese Aufgaben bislang das Ministerium für Inneres und Kommunales für mich wahrnimmt. Nicht zuletzt die Steu-

erzahlerinnen und Steuerzahler hätten für einen mit einer solchen Doppelstruktur verbundenen Stellenmehrbedarf kaum Verständnis.

Den so skizzierten Umbruch mit zu gestalten wird meine Aufgabe auch in den nächsten Jahren sein. Dies kann ich nur mit Hilfe engagierter Mitarbeiterinnen und Mitarbeiter erreichen, denen ich an dieser Stelle für die bisher geleistete Unterstützung danke. Dank gilt auch meiner Vorgängerin, Frau Bettina Sokol, die im Jahre 2009 ein wohl bestelltes Haus hinterlassen hat.

Ulrich Lepper Düsseldorf, im Frühjahr 2011

2 Neuausrichtung der Behörde

Datenschutz in einer von Technik bestimmten Welt fordert die staatliche Aufsicht, die Daten verarbeitenden Stellen und die von der Verarbeitung betroffenen Personen gleichermaßen, wenn die Privatsphäre effektiv geschützt bleiben soll.

Der rasante technische Fortschritt unserer Zeit greift kaum irgendwo so spürbar und zunehmend in unser alltägliches Leben ein wie in der Datenverarbeitung. Die Videokamera hängt bereits über dem Kinderbett und überträgt funkgesteuert und hoffentlich verschlüsselt Bild und Ton auf das Empfängergerät bei den Eltern. Über mitgeführte Handys, Laptops oder Navigationssysteme werden wir geortet und erlauben unter Umständen unseren Freundinnen und Freunden im sozialen Netzwerk, stetig unseren Aufenthaltsort nachzuvollziehen. Wenn wir krank sind, werden unsere Daten bei der medizinischen Versorgung erfasst und wir wissen oft nicht, wer mit wem vernetzt ist, wie und welche Daten zwischen Ärztin oder Arzt, Krankenhaus, Krankenkasse oder -versicherung, Apotheken und Abrechnungszentren ausgetauscht werden. Wann und wo wir bargeldlos bezahlen, wird gespeichert und ermöglicht tiefe Einblicke in unsere Lebensweise. Wir erhalten nun einen elektronischen Personalausweis, unsere Einkommens- und Steuerdaten werden vom Arbeitgeber automatisiert übermittelt und auch Behördengänge sollen zukünftig virtuell möglich werden. An einem herkömmlichen Büroarbeitsplatz ist theoretisch jeder Tastaturanschlag nachvollziehbar.

Gleichzeitig stellt sich die Datenverarbeitung in den über 700.000 Unternehmen und den Verwaltungen in NRW immer differenzierter dar. Datenverarbeitungsprozesse werden in Teilprozesse unterteilt und auf zahlreiche Unternehmen verteilt, die ihre Daten unter Umständen in einer "Wolke" ablegen. Bei der Datenverarbeitung in einer Wolke, dem Cloud Computing, werden in einer Netzwerkstruktur Serverkapazitäten an beliebig vielen Standorten jeweils nach momentaner Verfügbarkeit und optimaler Lastausnutzung für eine Datenverarbeitung verwendet. Die für die Datenverarbeitung Verantwortlichen wissen unter Umständen selbst nicht mehr, an welchem Ort ein Datenverarbeitungsvorgang zu einem bestimmten Zeitpunkt durchgeführt wird.

Inzwischen ist die einzelne Person nicht mehr nur im Fokus des Datenschutzes, weil es sie zu schützen gilt. Mehr und mehr verarbeitet sie selbst personenbezogene Daten von sich oder anderen und ist mit dieser Verarbeitung in Netzwerke eingebunden. In der Regel beginnen Kinder heute im Grundschulalter wie selbstverständlich mit Rechnersystemen umzugehen. Für die Hausaufgabe wird im Internet recherchiert, der Text wird auf dem Computer geschrieben und mit Klassenkameradinnen und -kameraden per E-Mail ausgetauscht. Privat werden mit der Handy-Kamera erstellte Fotos in offenen oder geschlossenen Netzen weitergegeben. Auf demselben Weg werden Verabredungen getroffen und Informationen über Dritte ausgetauscht. Nebenbei lesen manche der Unternehmen, die Netzwerke anbieten, das elektronische Adressbuch des Kindes aus und gewinnen so neue Mitglieder für das Netzwerk. Die Aktivitäten von Schülerinnen und Schülern sind im Blickwinkel großer internationaler Unternehmen. Sie bieten den Schulen kostenfrei oder sehr günstig eigene Kommunikationsstrukturen für die Vernetzung zwischen Lehrerinnen und Lehrern sowie Schülerinnen und Schülern an. Manchmal besteht die Währung für eine solche Dienstleistung in den Daten, die über das Netzwerk ausgetauscht werden und an einem Ort irgendwo auf der Welt gespeichert sind.

Ich will damit nur einen kleinen Teil der Lebenssachverhalte anreißen, die meine Behörde beschäftigen. Schon diese wenigen Beispiele machen deutlich, welche Herausforderung die Gewährleistung des Datenschutzes angesichts des aktuellen technischen Standes und der großen Zahl von Personen ist, die in Nordrhein-Westfalen aktiv Daten verarbeiten oder deren Daten zumindest in Verarbeitungsprozesse einbezogen sind.

Um bei dieser Ausgangslage einen guten Datenschutz zu gewährleisten, muss ich daher mit meiner Behörde neue Wege beschreiten. Eine staatliche Aufsicht allein reicht nicht, um die aktuellen, durch moderne technische Möglichkeiten entstehenden Gefahren für die Privatsphäre einzudämmen. Es muss vielmehr ein Zusammenspiel aller Akteurinnen und Akteure geben, die in einem Bezug zu konkreten Datenverarbeitungsprozessen stehen. Ich sehe mich dabei durch die in Aussicht gestellte personelle Verstärkung unterstützt.

➡ Im Wesentlichen will ich mit meiner Behörde darauf hinarbeiten, dass der Datenschutz in NRW durch drei stabile Säulen getragen wird:

- Eine stärkere Eigenverantwortung der Daten verarbeitenden Stellen, die durch eine leistungsfähige betriebliche und behördliche interne Datenschutzkontrolle unterstützt wird,

- eine verbesserte Datenschutzkompetenz, damit informierte und kompetente Individuen ihre Datenschutzrechte verantwortungsbewusst wahrnehmen können und

- eine intensivere Aufsicht, die von mir und meinen Mitarbeiterinnen und Mitarbeitern vor Ort wahrgenommen wird.

2.1 Eigenverantwortung

Behörden, Unternehmen und sonstige Daten verarbeitende Stellen müssen die Rechtmäßigkeit ihrer Datenverarbeitung gewährleisten und finden dabei Unterstützung durch betriebliche und behördliche Datenschutzbeauftragte vor Ort.

In keinem anderen europäischen Staat ist die Eigenkontrolle der Datenverarbeitung durch interne Datenschutzbeauftragte so gut ausgeprägt wie in Deutschland. Dies stellt sich nun, da Datenverarbeitung ein allgegenwärtiges Phänomen wird, als erheblicher Vorteil heraus. Die Europäische Kommission erwägt daher, die interne Datenschutzkontrolle auf der Grundlage der in Deutschland gewonnenen Erfahrungen bei ihrer aktuell angekündigten Überarbeitung der europäischen Datenschutzgesetzgebung europaweit verpflichtend einzuführen.

Auch das, was gut ist, kann und sollte verbessert werden. Das Datenschutzrecht ist stark geprägt von Abwägungsprozessen, die die Interessen von Betroffenen im Verhältnis zu öffentlichen oder betrieblichen Interessen gewichten. Es ist entscheidend für einen guten Datenschutz, dass diese Abwägung in den Betrieben und Behörden konsequent und einheitlich die Interessen der Betroffenen berücksichtigt.

Das kann erreicht werden, wenn sich der Informationsfluss zwischen der Datenschutzaufsicht und den verantwortlichen Stellen verbessert. Fälle, die von allgemeinem Interesse sind und in meiner Behörde bereits bewertet wurden, sollen den verantwortlichen Stellen und den dortigen Datenschutzbeauftragten schnell und unbürokratisch zur Kenntnis gelangen. Die Arbeit meiner Behörde kann so über den Einzelfall hinaus als Richtschnur für vergleichbare Sachverhalte in Behörden und Unternehmen genutzt werden. Zu diesem Zweck biete ich einen Newsletter an, der über meine Internetseite bestellt werden kann. Dieses Instrument erlaubt eine schnelle Verbreitung von Informationen, die eine einheitliche Rechtsanwendung vor Ort fördern. Der Newsletter hat einen hohen Zuspruch erfahren und wird hoffentlich weiterhin gut angenommen. Daneben bietet natürlich meine Homepage ständig aktuelle Informationen auch für verantwortliche Stellen. Aus intensiver Zusammenarbeit meiner Behörde mit dem Innenministerium entstand bzw. eine Mustervereinbarung für das betriebliche Eingliederungsmanagement Beschäftigten nach längerfristiger Erkrankung. In diesem sensiblen Bereich können sich nun alle Behörden und Unternehmen im Lande an dem Muster orientieren.

Des Weiteren habe ich begonnen in Tagungen und Konferenzen bereichsspezifische Datenschutzfragen mit den Vertretungen von verantwortlichen Stellen zu erörtern. Zu nennen sind hier die Polizei und die kommunalen Spitzenverbände, mit denen ein fachlicher Austausch vereinbart wurde. Die schon von meiner Vorgängerin im Amt initiierten Besprechungen mit Datenschutzbeauftragten von Konzernen und Hochschulen werden vertieft fortgeführt. Weiter sind Besprechungen auf Regierungsbezirksebene für den Bereich Schulen projektiert. Es sollen weitere verantwortliche Stellen identifiziert werden, in denen es gleichartige Datenschutzprobleme gibt, um mit deren Leitungen, Datenschutzbeauftragten oder Verbänden in einen fachlichen Dialog zu treten. Die Veröffentlichung von Artikeln zum Datenschutz in Fachorganen von Kammern und Verbänden ist ein weiteres Mittel, das

das Verständnis für die Anwendung des Datenschutzrechts vor Ort stärken kann.

Schließlich hat meine Behörde gemeinsam mit der Fortbildungsakademie des Ministeriums für Inneres und Kommunales ein Lernprogramm zum Datenschutz entwickelt, das von den Beschäftigten in öffentlichen Stellen genutzt werden kann, um sich das Basiswissen zum Datenschutz anzueignen, das auf einem Behördenarbeitsplatz notwendig ist, an dem mit personenbezogenen Daten umgegangen wird.

Neben diesen Maßnahmen für eine einheitliche Rechtsanwendung im Datenschutz in den Betrieben und öffentlichen Stellen strebe ich eine stärkere Zusammenarbeit mit den betrieblichen und behördlichen Datenschutzbeauftragten an. Sie sind ein wichtiger Faktor im Beschwerdemanagement der Daten verarbeitenden Stellen. Es hat sich vielfach als effizienter erwiesen, wenn Anliegen in Datenschutzfragen unmittelbar vor Ort geklärt werden. Vielen Bürgerinnen und Bürgern, die sich an mich wenden, ist nicht bewusst, dass sie durchaus auch erst einmal bei den Datenschutzbeauftragten in den verantwortlichen Stellen Hilfe suchen können. Diese können die Probleme oft schneller und unbürokratischer lösen als meine Behörde, weil sie die Abläufe bereits kennen. Da der stetige Zuwachs an Beschwerden bei mir nicht mehr durch Arbeitsverdichtung allein bewältigt werden kann, bin ich dazu übergegangen, die behördlichen und betrieblichen Datenschutzbeauftragten in die Beschwerdenerledigung einzubeziehen, wo der konkrete Fall das erlaubt. Dieser Ansatz ist bei Unternehmen und Behörden sehr positiv aufgenommen worden, weil er der verantwortlichen Stelle selbst die Möglichkeit einräumt, Fehler zu beseitigen und so die Zufriedenheit von Kundinnen und Kunden oder Bürgerinnen und Bürgern wiederherzustellen. Zudem sind die Beschwerden auch für die verantwortlichen Stellen ein wertvoller Hinweis darauf, wo das eigene Datenschutzmanagement verbesserungswürdig ist.

Dieser Ansatz könnte im Landesdatenschutzgesetz verstärkt werden. Die behördlichen Datenschutzbeauftragten beraten bisher nach ihren gesetzlichen Aufgaben unmittelbar nur die Beschäftigten öffentlicher Dienststellen, nicht aber die Bürgerinnen und Bürger. Es ist wünschenswert, dass sich die gesetzliche Beratungsaufgabe generell auf alle Personen erstreckt, deren Daten die jeweilige öffentliche Stelle verarbeitet – so wie es bei betrieblichen Datenschutzbeauftragten schon lange üblich ist.

- Mein Ziel ist ein verbesserter Informationsaustausch zwischen meiner Behörde und den verantwortlichen Stellen sowie, die Datenschutzbeauftragten vor Ort in die Beschwerdebearbeitung einzubeziehen, um die Qualität des Datenschutzes zu erhöhen.

2.2 Datenschutzkompetenz und Selbstdatenschutz

Wenn die Bürgerinnen und Bürger sich selbst nicht um den Schutz ihrer Daten kümmern, muss jede Datenschutzaufsicht zu spät kommen. Deswegen ist es enorm wichtig, dass Betroffene sowohl über ihre Datenschutzrechte als auch über die Konsequenzen eines laxen Umgangs mit den eigenen Daten gut informiert sind.

Manche Beschwerden, die ich erhalte, hätte es nicht geben müssen, wenn die Betroffenen vorher besser informiert gewesen wären. Im Grunde müssen die Bürgerinnen und Bürger den Umgang mit den vielen Rechnern und Speichermedien, die unseren Alltag begleiten, mittlerweile ähnlich wie die Teilnahme am Straßenverkehr erlernen. Es ist wichtig, dass die Menschen ihre Datenschutzrechte kennen und auch nutzen. Nur so erhalten sie Klarheit über den Umgang mit ihren Daten und vermeiden, dass sie Daten unnötig preisgeben. Das allein reicht aber nicht aus. Sie müssen auch eine Vorstellung entwickeln, an welchen Stellen sich überhaupt kritische Fragen ergeben. Denn schon längst ist nicht mehr jede Datenerhebung auf den ersten Blick als solche erkennbar, weil die Technik, mit der gearbeitet wird, immer kleiner und unauffälliger wird. Verbraucherinnen und Verbraucher müssen die Möglichkeit haben, sich über datenschutzfreundliche Dienstleistungen am Markt und über Schutzmechanismen gegen datenschutzfeindliche Techniken zu informieren, wenn sie sich effektiv schützen wollen. Schließlich verarbeiten auch die Bürgerinnen und Bürger selbst zunehmend Daten über andere und müssen dabei die Grenzen einer zulässigen Verarbeitung kennen, um nicht die Privatsphäre anderer zu verletzen.

Ich sehe ein wesentliches Element meiner Arbeit darin, die notwendige Informationsgrundlage für einen effektiven Selbstdatenschutz der Bürgerinnen und Bürger zu schaffen. Aktive Pressearbeit und ein breites Informationsangebot sind wesentliche Instrumente, um allgemein in-

teressierende Themen schnell einem breiten Publikum zur Verfügung zu stellen. Bzw. konnten viele Anfragen nach Inkrafttreten von neuen gesetzlichen Regelungen für Auskunfteien und Scoringverfahren umfassend befriedigt werden, weil ich zeitnah Informationen im Internet verfügbar gemacht habe. Ebenso wurden die Informationen zur Umsetzung des Widerspruchsrechts gegen die Veröffentlichung von Häusern in Google Street View sehr nachgefragt und als hilfreich empfunden. Ein bewährtes Mittel, über das die Bürgerinnen und Bürger erfahren, welche Datenschutzrechte sie haben und wie sie diese durchsetzen können, ist neben einer Reihe anderer Publikationen das Datenscheckheft, das ich online zur Verfügung stelle. Mein Wunsch ist, diese Aktivitäten auszubauen. Aus der Bearbeitung von Datenschutzfällen ergeben sich oft wertvolle Datenschutzhinweise, die ich so weit wie möglich der Allgemeinheit zur Verfügung stellen möchte.

Zu einer guten Informationsgrundlage gehört auch, dass die Bürgerinnen und Bürger die Möglichkeit erhalten, datenschutzfreundliche Produkte und Verfahren von solchen zu unterscheiden, die die Privatsphäre gefährden. Ein wichtiges Hilfsmittel sind Datenschutzaudits, die überprüfen, ob ein Produkt, ein Verfahren oder eine Anwendung das Datenschutzrecht beachtet. Leider gibt es dafür immer noch kein bundesweit anerkanntes Verfahren. Ein "Datenschutzengel" oder ein Gütesiegel, das die Verbraucherinnen und Verbraucher auf datenschutzfreundliche Produkte hinweist, wäre eine wichtige Entscheidungshilfe für ein datenschutzbewusstes Verhalten. Ein gut gestaltetes Auditierungsverfahren kann zudem die Datenschutzaufsicht erheblich entlasten, weil unter der fachlichen Verfahrensleitung der Datenschutzaufsicht kompetente externe Sachverständige einbezogen werden können. Damit können sich Anzahl und Umfang der Datenschutzüberprüfungen um ein Vielfaches erhöhen. Auch für die Eigenverantwortung der Daten verarbeitenden Stellen kann ein Gütesiegel ein Ansporn sein, weil es gegenüber Konkurrenzunternehmen einen Wettbewerbsvorteil darstellt. Ich werde mich deswegen aktiv einbringen, um Projekte auf den Weg zu bringen, die ein bundesweites Datenschutzaudit in der Regie der Datenschutzaufsichtsbehörden zum Ziel haben.

Neben den allgemeinen Informationen für die Bürgerinnen und Bürger ist mir die Sensibilisierung und Aufklärung junger Menschen für den Datenschutz ein besonderes Anliegen. Wie keine andere Generation zuvor sind sie fast ständig online und machen somit automatisch viele

Informationen über sich verfügbar. Ich teile nicht die Auffassung eines der Gründer des sozialen Netzwerkes Facebook, Mark Zuckerberg, der meint, dass Datenschutz ein Phänomen sei, das sich über die Zeit verändert und weniger wichtig wird. Ich denke im Gegenteil, dass die Erfahrungen mit der neuen Technik erst mittelfristig den Nutzerinnen und Nutzern die Bedeutung von Datenschutz vor Augen führen werden. Die Technik bringt viele Vorteile, die ganz besonders von Jugendlichen gerne angenommen werden. Entscheidend ist dabei, dass diejenigen, die sich für eine Techniknutzung entscheiden, sich auch der jeweiligen Konsequenzen für ihre Privatsphäre bewusst sind und dass sie Strategien erlernen, die ihren persönlichen Datenschutz verbessern. Eine speziell an Jugendliche gerichtete Öffentlichkeitsarbeit muss diese in ihrer Erlebniswelt erreichen und ein Verständnis für Sinn und Zweck des Datenschutzes wecken können.

Es gibt zwar bereits zahlreiche Initiativen, die sich ganz allgemein mit der Medienkompetenz von Jugendlichen befassen. Darin sind aber nur teilweise Aspekte des Datenschutzes enthalten. Es geht darum den "Nerv" der Schülerinnen und Schüler zu treffen und wertvolle Datenschutzangebote aus unabhängiger Sicht zu unterbreiten.

Daher möchte ich eine didaktisch gut aufbereitete an Jugendliche gerichtete Öffentlichkeitsarbeit zur Verbesserung der Datenschutzkompetenz entwickeln. Ich habe bereits Gespräche mit anderen Einrichtungen in NRW geführt, wie etwa der Landesmedienanstalt oder der Landeszentrale für politische Bildung. Dabei suche ich aktiv nach Kooperationen, die es mir erlauben, in einem Bundesland, das in der Vergangenheit gern als Medienland bezeichnet wurde, eine Initiative für mehr Datenschutzkompetenz zu beginnen. Ein bewusster und informierter Umgang mit den eigenen Daten bei der Mediennutzung verhindert, dass später ein staatliches Eingreifen gefordert wird.

➡ Nur gut informierte Bürgerinnen und Bürger können bewusst über den Schutz ihrer Daten entscheiden. Je früher Datenschutzkompetenz erworben wird, umso nachhaltiger ist der Effekt. Deshalb setze ich mich dafür ein, dass Kindern und Jugendlichen so früh wie möglich diese Kompetenz vermittelt wird.

2.3 Datenschutzaufsicht

Die betriebliche und behördliche Datenschutzkontrolle und informierte Bürgerinnen und Bürger sind wichtige Säulen des Datenschutzsystems. Ohne die dritte Säule, nämlich die Datenschutzaufsicht, steht das Gebäude des Datenschutzes nicht.

Betriebliche und behördliche Datenschutzbeauftragte berichten häufig, dass ihre eigene Überzeugungskraft in den Behörden und Unternehmen durch Maßnahmen der Datenschutzaufsicht deutlich unterstützt wird. Sie nutzen offizielle Stellungnahmen, die die Datenschutzaufsichtsbehörde veröffentlicht, um intern in den Unternehmen und Behörden ihre Datenschutzanforderungen durchzusetzen. Die betrieblichen Datenschutzbeauftragten haben vielfach mitgeteilt, dass die in den zurückliegenden Jahren wegen eklatanter Datenschutzverstöße verhängten Bußgelder dazu führten, dass das Thema Datenschutz in den Führungsetagen der Unternehmen angekommen ist. Neben daraus resultierendem ernsthaftem Bemühen um einen guten Datenschutz wird vereinzelt aber auch darüber berichtet, dass in Unternehmen danach gefragt wird, wie groß die Gefahr und wie hoch die Kosten seien, wenn ein Datenschutzverstoß entdeckt wird, um damit bewusst zu kalkulieren. Dies verdeutlicht, dass eine Datenschutzaufsicht spürbar bleiben muss. Ich würde deswegen die Präsenz in der Kontrolle gerne erhöhen. Ebenso, wie ohne gelegentliche Verkehrskontrollen Straßenverkehrsvorschriften kaum eingehalten werden, werden auch im Datenschutz sichtbare Kontrollen zwingend erforderlich sein. Mittelfristig möchte ich ein Team zusammenstellen, das auf Kontrollen vor Ort spezialisiert ist. Neben systematischen Regelkontrollen, die in Absprache mit den zuständigen Fachbereichen durchgeführt werden sollen, kann das Team bei Aufdeckung sogenannter Datenskandale schnell und professionell die zur Fallbeurteilung notwendigen Informationen erheben. Entscheidend ist, dass ein solches Team nicht nur gelegentlich Kontrollen durchführt, sondern eine Routine in derartigen Prüfungen entwickelt. Dies ist bei der bisherigen Behördenstruktur, in der alle Mitarbeiterinnen und Mitarbeiter in ihrem Fachgebiet von der Einzelpetition über Fachberatung, Kontrolle, Sanktion oder Begutachtung bis zur Gesetzesberatung alle Felder abdecken, leider nicht der Fall. Dadurch entstehen gerade im Kontrollbereich Reibungsverluste.

In einem ersten Schritt habe ich mit einer Stichprobenkontrolle bei 1.000 beliebig nach Branchenverzeichnissen ausgewählten nicht-öffentlichen Stellen überprüft, ob dort eine Verpflichtung zur Bestellung von Datenschutzbeauftragten besteht und ihr auch nachgekommen wird. Die Aktion wurde begleitet durch ein Angebot auf meiner Internetseite, mit dem Unternehmen prüfen können, ob sie zur Bestellung einer oder eines Datenschutzbeauftragten verpflichtet sind. Die Auswertung der Aktion hat ergeben, dass in einer Größenordnung von etwa 10 % die gesetzliche Verpflichtung, Datenschutzbeauftragte zu bestellen, nicht eingehalten wurde.

Diese Aktion hat sich herumgesprochen. Auch nicht angesprochene Unternehmen scheinen darauf aufmerksam geworden zu sein und haben sich bei meiner Behörde vermehrt erkundigt, ob für sie die Pflicht zur Bestellung einer oder eines Datenschutzbeauftragten besteht. Bei dieser Aktion kann es natürlich nicht bleiben. Dort wo Mängel festgestellt wurden, wird dem nachgegangen und unter Umständen werden auch Bußgelder verhängt.

➡ Meine Aufsicht soll spürbar und sichtbar sein, um über den Einzelfall hinaus Wirkung zu erzielen.

3 Entwicklung des Datenschutzrechts

3.1 BDSG-Novelle 2009

Nicht zuletzt als Reaktion auf eklatante Datenschutzskandale sind 2009 wichtige Änderungen des Bundesdatenschutzgesetzes (BDSG) beschlossen worden. Eine systematische Anpassung des Datenschutzrechts an die technische Entwicklung steht aber immer noch aus.

Einige Fälle, die von einem äußerst schlechten Datenschutzverständnis oder gar einer Missachtung des Datenschutzes zeugten, brachten in den letzten drei Jahren wiederholt auch namhafte Unternehmen in die Schlagzeilen. Es wurden vor allem die Rechte von Beschäftigten verletzt. Aber auch der Adresshandel und die Kontrolle von Subunternehmern, die in die Verarbeitung personenbezogener Daten eingeschaltet waren, sind wiederholt aus dem Ruder geraten.

Als Reaktion darauf sind Änderungen des BDSG am 1. September 2009 in Kraft getreten. Die wichtigsten Änderungen im Überblick:

- Gesetzliche Klarstellung der für eine Auftragsdatenverarbeitung notwendigen Weisungstiefe und Auftragskontrolle
- Stärkung der Position von betrieblichen Datenschutzbeauftragten durch einen Kündigungsschutz und einen Fortbildungsanspruch
- Neuerungen beim Adresshandel: Es gibt nun ein grundsätzliches Einwilligungserfordernis für die Nutzung von Daten für den Adresshandel, das aber leider so viele Ausnahmen kennt, dass de facto der Grundsatz die Ausnahme ist. Es wurde eine Kennzeichnungspflicht eingeführt, die den Adresshandel besser nachvollziehbar machen soll. Außerdem sind die Anforderungen an eine wirksame Einwilligung in den Handel mit einer Adresse formuliert worden.
- Eigenständige Vorschrift für die Datenverarbeitung zur Markt- und Meinungsforschung, die nunmehr auch die Nutzung besonderer Datenkategorien, wie etwa Gesundheitsdaten oder Daten über die politische Überzeugung, einbezieht
- Neue Vorschrift für den Umgang mit Daten im Beschäftigungsverhältnis

- Einführung einer Befugnis für Anordnungen bei materiellen Datenschutzverstößen: Anders als zuvor kann die Datenschutzaufsichtsbehörde nicht nur bei technischen Unzulänglichkeiten, sondern nun auch bei Rechtsverstößen konkrete Vorgaben für den zulässigen Umgang mit Daten bis hin zu einem Verarbeitungsverbot machen.
- Verpflichtung für Daten verarbeitende Stellen, den Verlust von im Gesetz bezeichneten sensiblen Daten bei der Aufsichtsbehörde anzuzeigen und Betroffene zu informieren
- Zusätzliche Bußgeldtatbestände, die vor allem eine Missachtung von neu im Gesetz eingeführten Verpflichtungen sanktionieren. Außerdem wurde der Bußgeldrahmen erhöht. Im Höchstsatz können nun Bußgelder in Höhe von 300.000 Euro anstatt bisher 250.000 Euro verhängt werden. Zudem kann ein durch einen Datenschutzverstoß entstandener Gewinn abgeschöpft werden.

Weitere Änderungen des BDSG traten zum 1. April und zum 11. Juni 2010 in Kraft. Sie betrafen die Datenverarbeitung durch Auskunfteien und schufen erstmalig konkrete Regelungen für Scoringverfahren. Unter anderem wurde außerdem klargestellt, dass Darlehensgeber aus anderen Mitgliedstaaten der Europäischen Union unter den gleichen Voraussetzungen wie inländische Darlehnsgeber Informationen von Auskunfteien erhalten können. Der praktischen Umsetzung der Vorschriften über Auskunfteien und Scoring ist ein eigenes Kapitel in diesem Bericht im Abschnitt Wirtschaft gewidmet (siehe Ziffer 6.1.).

Als weitgehend positiv für die Datenschutzpraxis können die Klarstellungen bei der Auftragsdatenverarbeitung, die Stärkung der Position betrieblicher Datenschutzbeauftragter, die Meldepflicht von Datenverlusten und die Verbesserung der Eingriffsbefugnisse der Aufsichtsbehörden bewertet werden. Die Änderungen im Adresshandel sind hingegen schon rein sprachlich nur schwer verständlich und werfen daher Fragen hinsichtlich der korrekten Umsetzung in der Praxis auf.

Die Interimslösung eines neuen § 32 BDSG zur Verarbeitung von Daten für Zwecke eines Arbeitsverhältnisses soll durch ausführlichere und differenziertere Regelungen zum Beschäftigtendatenschutz abgelöst werden. Der dazu vorliegende Gesetzentwurf wird in einem eigenen Kapitel dieses Berichts behandelt.

Die im Berichtszeitraum vollzogenen Gesetzesänderungen sind zum Teil hilfreich, letztlich bleiben sie aber ein Flickenteppich, der nur vage verdeckt, dass das Datenschutzrecht das Internetzeitalter verschlafen hat. Bereits im Jahr 2001 hatte die damalige Bundesregierung erkannt, dass eine grundlegende Überarbeitung des Datenschutzrechts notwendig ist, die den Anforderungen der modernen Technik Rechnung trägt. Es wurde daher ein Gutachten zur Modernisierung des Datenschutzrechts in Auftrag gegeben und Ende 2001 vorgelegt. Damals sollte in einer ersten Stufe das Bundesdatenschutzgesetz eilig an die EG-Datenschutzrichtlinie angepasst werden, da die fünfjährige Umsetzungsfrist der Richtlinie bereits verstrichen war. Das Gutachten sollte dann die zweite grundlegende Modernisierungsstufe des Datenschutzrechts vorbereiten. Dieser zweite Modernisierungsschritt wurde aber bis heute nicht vollzogen. Nach wie vor enthält das Bundesdatenschutzgesetz Regelungen zum technischen Datenschutz aus einer schon fast vergessenen Welt, in der Datenverarbeitung in verschlossenen Räumen auf Großrechnern durchgeführt wurde. Für heutige Datenverarbeitungen, die praktisch allerorts stattfinden und von einer umfassenden Vernetzung geprägt sind, enthält das Bundesdatenschutzgesetz keine zeitgemäßen und praxisgerechten Antworten.

➡ Die Änderungen des Bundesdatenschutzgesetzes haben einige Verbesserungen für die Aufsichtspraxis gebracht. Eine grundlegende Überarbeitung des Datenschutzrechts an die bestehenden technischen Herausforderungen muss nun aber dringend folgen.

3.2 Vorschläge zur Modernisierung des Datenschutzrechts

Um eine Diskussion über die Modernisierung des Datenschutzrechts in Gang zu setzen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eigene Vorstellungen entwickelt.

In ihrer Frühjahrssitzung am 18. März 2010 verabschiedete die Konferenz Eckpunkte für "Ein modernes Datenschutzrecht für das 21. Jahrhundert". Das gesamte Papier kann über meine Homepage (www.ldi.nrw.de) abgerufen werden. Ich möchte daraus vier Punkte hervorheben, die gesetzlich vollzogen werden müssen, damit wir ein

Bundesdatenschutzgesetz erhalten, das die Bezeichnung modern verdient.

- Der technische Datenschutz muss sich an Schutzzielen orientieren. Es mutet geradezu altertümlich an, wenn im Bundesdatenschutzgesetz die Zutrittskontrolle als erster Sicherheitsaspekt genannt wird. Daten werden auf mobilen Rechnern verarbeitet und auf kleinen Sticks oder über Netze transportiert und gar in "Wolken" gespeichert. Mit einer Zutrittskontrolle lässt sich das Datensicherheitsziel "Vertraulichkeit der Daten" bei diesen Szenarien kaum garantieren. Es muss je nach den Anforderungen des eingesetzten Systems festgelegt werden, wie der Schutz der Daten optimal gewährleistet werden kann. Das Datenschutzgesetz des Landes NRW ist im Hinblick auf die Regelung zum technischen Datenschutz vorbildlich und kann dem Bundesgesetzgeber als Blaupause dienen (siehe Nr. 3. der Eckpunkte).
- Die Wahrung des Rechts auf informationelle Selbstbestimmung jeder einzelnen Person kann angesichts der stetig zunehmenden Datenverarbeitungen nur gewährleistet werden, wenn die Daten verarbeitenden Stellen durch eine starke betriebliche Selbstkontrolle unterstützt werden. Anreize für einen guten Datenschutz sollten durch Auditierungsverfahren geschaffen werden. Eine staatliche Aufsicht kann die Kontrolle der Datenfluten alleine nicht sicherstellen. Sie muss aber unabhängig und schlagkräftig agieren können, um der betrieblichen Selbstkontrolle das notwendige Gewicht zu verleihen, und dort eingreifen, wo Selbstkontrollmechanismen versagen (siehe Nrn. 6. und 7. der Eckpunkte).
- Es müssen im Recht praxisgerechte Lösungen für Datenverarbeitungen mit mehreren beteiligten Stellen angeboten werden. Tatsächlich sind oft Datenverarbeitungssysteme im Einsatz, bei denen nicht nur eine einzige Stelle jeden Verfahrensschritt alleine verantwortet. Die Verantwortungen für die Datenverarbeitung in verbundenen Systemen sind häufig auf mehrere Akteurinnen und Akteure verteilt. Hier müssen Rollenkonzepte klare Verantwortungen für die einzelnen Verarbeitungsschritte und für die Umsetzung der Datenschutzrechte von Betroffenen widerspiegeln, damit die datenschutzrechtliche Verantwortung nicht von der einen auf die andere Stelle geschoben werden kann. Das Gesetz muss den Daten verarbeitenden Stellen mehr Spielräume zur

Errichtung verbundener Verfahren mit mehreren Beteiligten geben und gleichzeitig das Prinzip der Verantwortlichkeit für die Datenverarbeitung konturieren (Nr. 2.3 der Eckpunkte).

- Schließlich muss das Datenschutzrecht internetfähig werden. Dies hat auch die Bundesregierung zwar erkannt. Der Vorschlag des Bundesinnenministers, der Verbote lediglich für schwere Eingriffe in Persönlichkeitsrechte vorsieht, ist indessen ein Schritt in die falsche Richtung. Ein solcher Ansatz beinhaltet im Umkehrschluss, dass mittlere und leichte Persönlichkeitsrechtsverletzungen erlaubt sind. Dies kann angesichts der weltweiten und dauerhaften Verbreitung von Informationen im Netz zu erheblichen Nachteilen für Betroffene führen. Es sind weiter reichende Schutzmaßnahmen notwendig (Nr. 5 der Eckpunkte).

Vor allem ein internetfähiges Datenschutzrecht muss nach meiner Auffassung das Kernanliegen jeder grundlegenden Novellierung sein. Im Netz entstehen unermessliche Datenmengen, die Aussagen über einzelne Menschen oder deren Beziehungen ermöglichen und zu Profilen zusammengeführt werden können. Soziale Netzwerke etwa bilden Beziehungsprofile geradezu ab. Die Nutzerinnen und Nutzer geben in Netzwerken teils tiefe Eindrücke in ihre persönlichen Umstände und ihre Gedanken- und Erlebniswelt. In Bewertungsportalen werden nicht nur Hotels oder Dienstleistungen, sondern auch Lehrende an Schulen und Hochschulen ebenso wie Ärztinnen und Ärzte bewertet. Eine sehr spezielle Variante davon ist die Bewertung von Flirts etwa auch daraufhin, ob die oder der Andere gut küsst. Die technischen Möglichkeiten heute erlauben das Abbilden der gesamten Welt im Internet als Straßenansicht oder aus der Satellitenperspektive. In Blogs oder Foren können Einzelne über andere Personen alles verbreiten, was sie für zutreffend erachten. Die Datenverarbeitung im Netz ist weltumspannend und daher für die einzelne Person kaum mehr beherrschbar. Was einmal im Netz vorhanden ist, bleibt über Jahre erhalten. Suchmaschinen erlauben das schnelle Auffinden von Informationen zu jeder beliebigen Person. Diese Informationen können beispielsweise im Bewerbungsverfahren, vor dem Abschluss eines Mietvertrages oder aus purer Neugier eingesehen werden, ohne dass die Person davon etwas merkt. Große im Internet tätige Unternehmen schließlich bestimmen oft einseitig die Bedingungen für die Nutzung der bei ihnen zu einzelnen Personen entstandenen Daten.

Selbstregulierung kann hier allenfalls eine flankierende Maßnahme sein. Ohne klare rechtliche Vorgaben, die technikneutral einen Persönlichkeitsrechtsschutz auch im Internet gewährleisten, bleibt das Netz ein virtueller Wilder Westen. Ich halte daher insbesondere für dringlich,

- dass ein Mediennutzungsgeheimnis zur unbeobachteten Nutzung elektronischer Dienste rechtlich verankert und durch eine Pflicht flankiert wird, die anonyme oder zumindest pseudonyme Nutzung und Bezahlung von Online-Diensten anzubieten,
- dass Informationspflichten über die Nutzung personenbezogener Daten und die verwendeten Geschäftsklauseln gesetzlich fixiert werden und Verstöße sanktionierbar sind,
- dass Online-Dienste verpflichtet werden, in den Grundeinstellungen ein Optimum an Datenschutz zu gewährleisten, und dass die Verwendung der Daten im Übrigen durch den Umfang der Einwilligung der Nutzerinnen und Nutzer bestimmt wird,
- dass einfache Möglichkeiten zur Verfügung zu stellen sind, die es der einzelnen Person erlauben ihre Datenschutzrechte elektronisch wahrzunehmen,
- dass eine ausufernde Datennutzung durch Verfallsdaten und technische Schutzmechanismen, etwa gegen unerlaubtes Herunterladen von Daten, begrenzt wird und insbesondere Unternehmen, die Suchmaschinen betreiben, zur Beachtung solcher begrenzenden Maßnahmen verpflichtet werden.

Die Gesetzgebung in diesem Bereich muss durch Forschung begleitet werden, die die Möglichkeiten des technischen Persönlichkeitsrechtsschutzes vorantreibt. Es muss wegen der weltweiten Verbreitung des Netzes außerdem mindestens innerhalb Europas aber auch darüber hinaus ein internationaler Standard zum Schutz der Persönlichkeitsrechte angestrebt werden.

➡ Vorschläge für ein modernes Datenschutzrecht in Deutschland sind von meinen Kolleginnen und Kollegen und von mir vorgelegt worden. Jetzt müssen diese aufgegriffen werden. In einer anstehenden Diskussion über die Novellierung des europäischen Datenschutzrechts fehlt ansonsten eine klare deutsche Position.

3.3 Novellierung des europäischen Datenschutzrechtsrahmens

Die Europäische Kommission hat im November 2010 ein Gesamtkonzept für den Datenschutz in der Europäischen Union vorgestellt. Auf dieser Basis will sie im Sommer 2011 konkrete Regelungen unterbreiten.

Mit Inkrafttreten des Vertrages von Lissabon zum 1. Dezember 2009 hat die EU eine Grundrechtscharta erhalten, die in Art. 8 das Grundrecht jeder Person auf Schutz der sie betreffenden Daten anerkennt. Außerdem sind in Art. 16 und Art. 39 des Vertrages über die Arbeitsweise der Europäischen Union Regelungen eingeführt worden, die die Gesetzgebungsverfahren über Vorschriften zum Schutz persönlicher Daten beschreiben. Danach werden einerseits im Anwendungsbereich des Unionsrechts Datenschutzregelungen im ordentlichen Gesetzgebungsverfahren durch Rat und Parlament verabschiedet und andererseits im Bereich der Außen- und Sicherheitspolitik durch Ratsbeschluss.

Der Datenschutz im Anwendungsbereich des Unionsrechts ist zurzeit durch eine Richtlinie vorgegeben, die durch nationale Regelungen in den Mitgliedstaaten ausgefüllt wird. Der Datenschutz bei der justiziellen und polizeilichen Zusammenarbeit der EU-Mitgliedstaaten in Strafsachen wird aktuell durch den Rahmenbeschluss 2008/977/Js geregelt. Daneben gibt es jeweils eigene Datenschutzregime für Europol, Eurojust, das Schengener Informationssystem, das Zollinformationssystem und für den automatisierten Datenaustausch von DNA-Profilen, daktyloskopischen Daten und Daten aus Fahrzeugregistern. Begründet durch Art. 8 der EU-Grundrechtscharta strebt die EU-Kommission eine im Wesentlichen einheitliche Regelung zum Datenschutz auch für diese Bereiche an. Sie weist im Hinblick auf den Datenaustausch im Sicherheitsbereich außerdem darauf hin, dass die Abgrenzung von Datenverarbeitungen des internationalen Austauschs von rein nationalen Datenverarbeitungen praktisch schwierig sei.

Das Gesamtkonzept der Europäischen Kommission lässt insgesamt erkennen, dass ein neuer Datenschutzrechtsrahmen soweit wie möglich einheitlich für alle Politikbereiche gelten soll. Außerdem ist erklärtes Ziel des Gesamtkonzepts, bisher unterschiedlichen Umsetzungen der Datenschutzrichtlinie in den Mitgliedstaaten durch weitere Harmoni-

sierungen entgegenzuwirken. Eine Überlegung der Kommission geht dahin, Datenschutzregelungen nicht mehr durch eine Richtlinie, sondern durch eine Verordnung vorzugeben, die unmittelbar in den Mitgliedstaaten anzuwenden wäre und auch für rein nationale Datenverarbeitungsvorgänge Geltung beansprucht.

Eine Harmonisierung des Datenschutzrechts auf hohem Niveau wäre grundsätzlich wünschenswert. Dies gilt vor allem mit Blick auf die uneinheitlichen Datenschutzstandards und -kontrollmechanismen im Bereich der europäischen Sicherheitspolitik. Ob ein hohes Datenschutzniveau erreicht werden wird, dürfte entscheidend davon abhängen, wie das europäische Datenschutzgrundrecht in Art. 8 der EU-Grundrechtscharta ausgelegt werden wird. Dazu gibt es bisher keine Erfahrungen. Es besteht noch große Unsicherheit, ob dieses Datenschutzgrundrecht in einer Weise verstanden und gelebt werden wird, die dem durch das Grundgesetz gewährleisteten hohen Schutzniveau des Rechts auf informationelle Selbstbestimmung entspricht, das aus der Menschenwürde und dem allgemeinen Persönlichkeitsrecht hergeleitet wird. Die praktische Politik in Europa jedenfalls lässt daran erhebliche Zweifel aufkommen. Die Richtlinie zur Vorratsdatenspeicherung, die Handhabung von EU-Listen terrorverdächtiger Personen oder die Arbeiten an einem europäischen System für die Auswertung von Flugreservierungsdaten deuten nicht darauf hin, dass der Wahrung der informationellen Selbstbestimmung hohes Gewicht gegeben wird. Eine weitgehende Harmonisierung des Datenschutzrechts bedeutet vor diesem Hintergrund auch ein Wagnis. Aus meiner Sicht sollte das EU-Datenschutzgrundrecht zunächst in der Rechtspraxis der EU und durch die europäische Rechtsprechung Kontur gewinnen, bevor eine aus diesem Grundrecht abgeleitete weitgehende Harmonisierung des Datenschutzrechtsrahmens vorgenommen wird. Eine sich auf nationale Datenverarbeitungssachverhalte beziehende europäische Datenschutzregelung dürfte zudem mit dem Subsidiaritätsprinzip in Art. 5 des Vertrages über die Europäische Union kollidieren.

➡ Die Datenschutzgesetzgebung auf europäischer Ebene birgt Chancen und Gefahren. Sie kritisch zu begleiten, muss auch ein Anliegen der Landesregierung sein, da auch Landeskompetenzen betroffen sein können.

4 Schlaglichter auf die Aufsichtspraxis

4.1 Veröffentlichung digitaler Gebäudeansichten im Internet

Kein anderes Datenschutzthema wurde im Berichtszeitraum in der Öffentlichkeit so kontrovers diskutiert wie digitale Gebäudeansichten bei "Google Street View" und ähnlichen Angeboten. Für Kritikerinnen und Kritiker ist es unverständlich, weshalb ein Unternehmen ungefragt Fotos ihres Hauses ins Internet stellen darf und ihnen die Last aufbürdet, im Falle eines Widerspruchs ein aufwändiges und mit neuen Datenerhebungen verbundenes Verfahren zu durchlaufen. Dagegen reagieren viele, die das Projekt befürworten, auf die Kritik mit Kopfschütteln: Angesichts stetig wachsender staatlicher und privatwirtschaftlicher Sammlungen sensibler Daten innerhalb und außerhalb des Internets gebe es kaum Harmloseres als die Veröffentlichung von Gebäudefassaden, die vor Ort ohnehin für alle sichtbar seien.

Bereits im November 2008 hatten die obersten Datenschutzaufsichtsbehörden der Länder und des Bundes in einem Beschluss Anforderungen an die systematische Veröffentlichung digitaler Straßenansichten insbesondere im Internet formuliert (siehe Bericht 2009 unter Ziffer 6.4). Besonders wichtig sind danach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.
- Eigentümerinnen und Eigentümer sowie Mietparteien eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.
- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

Der wohl größte Anbieter Google sagte etwa gegenüber der zuständigen Aufsichtsbehörde in Hamburg zu, entsprechende Vorkehrungen zu treffen. Dies gilt auch für die Forderung der Datenschutzbehörden, dass die Löschungsverpflichtungen nicht nur für die Veröffentlichugen

im Internet gelten, sondern auch für die unter anderem in den USA gespeicherten Rohdaten der gefilmten Häuserfassaden .

Die Datenschutzbehörden verständigten sich mit der dargestellten Widerspruchslösung auf eine bundesweit einheitliche Auslegung der noch aus der Vor-Internet-Zeit stammenden und sehr allgemein gehaltenen Regelungen der §§ 28 und 29 Bundesdatenschutzgesetz (BDSG).

Die von Kritikern vertretene Auffassung, dass derartige Veröffentlichungen nur mit Einwilligung der betroffenen Personen zulässig seien, denen ein Haus gehört oder die es bewohnen, lässt sich zwar auf § 29 Abs. 2 BDSG stützen. Eine Verpflichtung, von allen Eigentümerinnen und Eigentümern sowie Bewohnerinnen und Bewohnern eine Einwilligung einzuholen, würde allerdings zur Folge haben, dass der Betreiber die Namen und Anschriften sämtlicher Bürgerinnen und Bürger benötigt. Dies wäre aus datenschutzrechtlichen Erwägungen ebenfalls problematisch.

Auf der anderen Seite entstehen durch die Veröffentlichung Gefahren für die informationelle Selbstbestimmung. Die systematische Erfassung, globale Verbreitung und Unauslöschlichkeit einmal im Internet veröffentlichter Daten sowie vor allem die unbegrenzten Verknüpfungsmöglichkeiten mit sonstigen Datenbeständen für unabsehbare Zwecke bergen Risiken, die nicht vergleichbar sind mit der Wahrnehmung einer Häuserfassade durch eine Person vor Ort. So besteht die Möglichkeit, dass Auskunfteien oder andere Unternehmen die Bilder nutzen, um sie systematisch auszuwerten. Die Erkenntnisse können etwa in die Bewertung der Bonität einer Person einfließen oder in die Einordnung zu einer Zielgruppe für Werbung.

Im Mai 2010 wurde nachträglich und erst auf Nachfrage der Hamburger Aufsichtsbehörde bekannt, dass Google-Fahrzeuge nicht nur in aller Welt Gebäudefassaden gefilmt, sondern auch flächendeckend unverschlüsselte WLAN-Daten der Bewohnerinnen und Bewohner gesammelt hatten. Der nach Angaben des Unternehmens versehentlich und unbemerkt aktivierte "Datenstaubsauger" hatte dabei auch E-Mails und aufgerufene Internetseiten erfasst. In Deutschland wie auch in mehreren anderen Staaten laufen seither staatsanwaltliche Ermittlungen oder Strafverfahren.

Die dadurch nochmals intensivierte öffentliche Diskussion führte zusammen mit dem Druck der Aufsichtsbehörden dazu, dass Google im

Sommer 2010 die Frist für die Veröffentlichung der Bilder aus den 20 größten Städten Deutschlands um einen Monat verlängerte. Nach Auskunft des Unternehmens erhoben in diesen Städten etwa eine Viertel Million Menschen Widersprüche. Dabei war das Verfahren aufwändig und mit neuen Datenerhebungen verbunden. Selbst wer bereits in den Monaten vorher per E-Mail der Veröffentlichung eines Gebäudes widersprochen hatte, musste nochmals ein kompliziertes "Verifizierungsverfahren" durchlaufen.

Unklar ist weiterhin, ob die im Rahmen dieses Verfahrens erhobenen Daten datenschutzgerecht verwandt werden. Immerhin ist Google nun im Besitz einer Liste der Street-View-Kritikerinnen und -Kritiker einschließlich ihrer Namen und Anschriften. Google speichert die Widerspruchsdaten wegen nicht auszuschließender Klageverfahren für drei Jahre und zwar nicht nur in Deutschland, sondern zumindest auch in den USA. Ich hatte gefordert, dass die Daten zur Gewährleistung der Zweckbindung ausschließlich bei einer Treuhandstelle in Deutschland verwahrt werden, um zweckwidrige Nutzungen bereits organisatorisch auszuschließen.

Die öffentliche Diskussion über "Google Street View" hat jedoch auch zu politischen Initiativen geführt, die über das einzelne Projekt hinausgehen. So brachte der Bundesrat im August 2010 einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes ein. Dieser sieht Rahmenbedingungen für die Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang mit der systematischen Veröffentlichung von Gebäudeansichten und vergleichbarer anderer Geodaten vor. Dieser Gesetzentwurf wiederum veranlasste den Bundesinnenminister dazu, im September 2010 ein Spitzengespräch einzuberufen, an dem auch ich teilnahm. Als Folge des Gesprächs legte die Internetwirtschaft Anfang Dezember 2010 den Entwurf eines selbstverpflichtenden Datenschutz-Kodexes vor.

- Ich setze mich für eine unbürokratische Widerspruchslösung vor Veröffentlichung der Gebäudeansichten ein. Dabei ist das Verfahren so zu gestalten, dass Unternehmen, die Gebäudeansichten anbieten, dann nicht mehr erfahren, wer den Widerspruch erhoben hat, sondern lediglich wissen, dass zu einer bestimmten Adresse ein Widerspruch vorliegt.

➡ Darüber hinaus fordere ich gemeinsam mit anderen Aufsichtsbehörden eine umfassende Modernisierung des Datenschutzrechts, die nicht allein auf die Veröffentlichung von Gebäudeansichten fokussiert ist, sondern insgesamt die Veröffentlichungen personenbezogener Daten im Internet regelt. Nur so wird das vielfach noch aus dem Zeitalter der Großrechner und Münzfernsprecher stammende Datenschutzrecht zukunftsfähig.

4.2 Unzulässige Verwendung von Kontobewegungsdaten durch eine Bank

Bevor sie Kundinnen und Kunden einer Bank ansprachen, um ihnen Finanzprodukte zu verkaufen, sollten die Beraterinnen und Berater einer Tochtergesellschaft dieser Bank die Kundschaft "aufbereiten". Eine Checkliste sah vor, welche Daten aus der Datenbank der Bank abgerufen werden sollten. Dazu zählten auch die Girokontoumsätze der letzten 100 Tage, insbesondere Geldeingänge, Versicherungsbeiträge, Steuererstattungen und Überweisungen an andere Banken.

Ein ehemaliger Berater der Tochtergesellschaft hatte die Stiftung Warentest über diese Praktiken informiert. Ich habe mir die entsprechenden Arbeitsanweisungen vorlegen lassen. Da die Bank den Beraterinnen und Beratern unzulässig sämtliche Daten von über einer Million ihrer Kundinnen und Kunden zum Abruf bereit gestellt hatte, habe ich ein Bußgeld in Höhe von 120.000 Euro verhängt.

Nach Bekanntwerden der Vorwürfe hat die Bank den Ablauf bei der Werbeansprache geändert. Insbesondere ist ein Zugriff durch die Tochtergesellschaft auf die Girokontobewegungen der Bankkundinnen und -kunden technisch nicht mehr möglich.

Daten aus Girokontobewegungen – also etwa Empfängerin oder Absender einer Überweisung und Verwendungszwecke – dürfen nicht zu Werbezwecken ausgewertet werden. Hier überwiegen stets die schutzwürdigen Interessen der Betroffenen. Denn Kontobewegungen sind sehr sensible Daten, die viel über unsere Lebensweise aussagen. Wer ein Einkommen von der Sozialbehörde bekommt, wer welche Zeitung abonniert oder wer welche Rechnung einer auf Herzkrankhei-

ten spezialisierten Klinik bezahlt, das und vieles mehr kann auf dem Konto ablesbar sein.

- Girokontobewegungsdaten dürfen nicht zu Vertriebszwecken genutzt werden – weder durch Vertriebsgesellschaften oder freiberufliche Handelsvertretungen noch durch ein Kreditinstitut selbst.

4.3 Speicherung und Verwendung von Daten im Online-Lastschriftverfahren

PIN oder Unterschrift? In der Regel wissen Verbraucherinnen und Verbraucher nicht, weshalb bei Zahlungen mit der EC-Karte manchmal die Eingabe der PIN und manchmal eine Unterschrift verlangt wird. Grund hierfür sind oftmals Datenverarbeitungsschritte, die in der jüngsten Vergangenheit in die Kritik der Datenschutzaufsicht geraten sind.

Viele Handelsunternehmen wickeln EC-Karten zahlungen mit Hilfe von sogenannten Netzbetreibern im Wege des Online-Lastschriftverfahrens ab. Hierbei "zahlen" Kundinnen und Kunden mit ihrer Unterschrift, durch die sie dem Handelsunternehmen oder dem von ihm für die Abwicklung des Lastschriftverfahrens beauftragten Netzbetreiber eine Einzugsermächtigung zur Abbuchung des geschuldeten Betrages von ihrem Konto erteilen. Das Risiko, dass das Konto einer Käuferin oder eines Käufers nicht gedeckt ist, liegt dabei auf Seiten des Handelsunternehmens.

Deswegen entscheiden sich manche Handelsunternehmen bei der Abwicklung von EC-Kartenzahlungen für das sogenannte Electronic-Cash-Verfahren, bei dem die Zahlung durch die Eingabe der PIN erfolgt. Hierbei findet eine Online-Überprüfung des Kartenkontos bei dem Geldinstitut statt, das die Karte ausgegeben hat. Bei ausreichender Deckung und Kartengültigkeit erscheint nach wenigen Sekunden im Terminal-Display "Zahlung erfolgt". Damit ist der Zahlbetrag garantiert und die Zahlung wird abgewickelt. Dieses Verfahren birgt für das Handelsunternehmen im Gegensatz zum Online-Lastschriftverfahren kein Forderungsausfallrisiko, ist aber für das Handelsunternehmen auch das teurere Verfahren.

Aus Kostengründen entscheiden sich daher viele Handelsunternehmen für das Online-Lastschriftverfahren. Um das hierbei für sie bestehende Forderungsausfallrisiko zu minimieren und die Gefahr von Kartenmissbrauch durch Unberechtigte zu verhindern, ergreifen Netzbetreiber unterschiedliche Maßnahmen:

Im Fall einer Rücklastschrift werden Kontonummer und Bankleitzahl einer Kundin oder eines Kunden in eine Sperrdatei des Netzbetreibers aufgenommen und an andere Unternehmen, die ebenfalls an dem Online-Lastschriftverfahren teilnehmen, auf Anfrage übermittelt. Wird ein "Treffer" in der Sperrdatei festgestellt, wird dem Handelsunternehmen empfohlen, die Zahlung durch die Eingabe der PIN im Rahmen des sogenannten Electronic-Cash-Verfahrens abzuwickeln. Das Führen einer solchen Sperrdatei und die Übermittlung entsprechender Informationen daraus an angeschlossene Unternehmen sind wegen der berechtigten Interessen der Handelsunternehmen im Hinblick auf etwaige Forderungsausfälle nach überwiegender Auffassung der Datenschutzaufsichtsbehörden datenschutzrechtlich zulässig. Kundinnen und Kunden müssen hierüber jedoch entsprechend unterrichtet und aufgeklärt werden.

Zur Minimierung des Ausfallrisikos ermitteln Netzbetreiber aber auch, wie häufig die Karte innerhalb eines bestimmten Zeitraums im Online-Lastschriftverfahren genutzt wird oder ob festgelegte tägliche, wöchentliche oder monatliche Betragsgrenzen für das Online-Lastschriftverfahren überschritten wurden. Hierfür erheben und verwenden sie Daten wie die jeweilige Bonsumme, Zeitpunkt und Ort der Zahlungen (sogenannte Transaktionsdaten). Wird eine Überschreitung der festgelegten Limits festgestellt, wird dem Handelsunternehmen empfohlen, die Zahlung im Wege des Electronic Cash abzuwickeln.

Zurzeit stützen Handelsunternehmen und Netzbetreiber die Erhebung und Verwendung von Transaktionsdaten auf eine Einwilligungserklärung, die die Kundinnen und Kunden an der Kasse nach dem Auslesen der Karte unterzeichnen. Damit wird die Einwilligung erst zu einem Zeitpunkt erteilt, zu dem die entsprechenden Daten bereits erhoben und verwendet wurden. Die Einwilligungserklärung wird insoweit nicht rechtzeitig – d.h. vor der Datenerhebung und -verwendung – erteilt. Darüber hinaus bildet die Einwilligung nicht hinreichend transparent ab, in welche Datenverarbeitungsvorgänge eine Kundin oder ein Kunde einwilligt. Die verwendete Einwilligungserklärung stellt daher keine

wirksame Grundlage für die Erhebung und Verwendung der Transaktionsdaten dar. Die Obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich haben die am Online-Lastschriftverfahren aufgekommene Kritik nun zum Anlass genommen, in einer Arbeitsgruppe entsprechende datenschutzrechtliche Anforderungen zu entwickeln.

Darüber hinaus sorgte ein Netzbetreiber im Zusammenhang mit der Verwendung von Daten aus Online-Lastschriftverfahren aus einem weiteren Grund für erhebliches Aufsehen. Er geriet in Verdacht, die Daten kommerziell an dritte Unternehmen zur Nutzung für Marketingzwecke übermittelt zu haben. In einem Fall bestätigte sich, dass der Netzbetreiber Transaktionsdaten aus dem Online-Lastschriftverfahren an ein Tochterunternehmen übermittelt hatte. Das Tochterunternehmen hatte diese Daten anschließend statistisch aufbereitet und derart anonymisiert an ein drittes Unternehmen weiter veräußert. Da in der unzulässigen Datenübermittlung an das Tochterunternehmen nach meiner Auffassung ein strafbares Verhalten lag, stellte ich gegen den Netzbetreiber Strafantrag.

➡ Das Online-Lastschriftverfahren entspricht zurzeit nicht den datenschutzrechtlichen Anforderungen. Zusammen mit den anderen Datenschutzaufsichtsbehören werde ich mich dafür einsetzen, dass die Datenverarbeitungsvorgänge beim Bezahlen mit der EC-Karte für die betroffenen Kundinnen und Kunden transparenter werden und im Einklang mit den datenschutzrechtlichen Vorschriften stehen. Die Netzbetreiber sind aufgefordert, datenschutzkonforme Verfahren zu entwickeln.

4.4 Rechtswidrige Krankenlisten

Der Fund von Personalunterlagen in der Mülltonne einer Waschanlage veranlasste meine Behörde zur Überprüfung eines Lebensmittel-Discountunternehmens. Es handelte sich um handschriftlich geführte Listen über zahlreiche Beschäftigte, in denen eine Vielzahl zum Teil sensibler Angaben über deren Erkrankungen und gesundheitliche Beeinträchtigungen festgehalten waren.

Der Aktenfund deutete nicht nur darauf hin, dass Datensicherheitsmaßnahmen bei der Unterlagenvernichtung schlicht unbeachtet gelassen worden waren, sondern ließ insbesondere erkennen, dass den Personalverantwortlichen grundlegende Kenntnisse über den Umgang mit Daten von Beschäftigten, insbesondere in Erkrankungsfällen, fehlten.

Das Unternehmen wurde über die Voraussetzungen der Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten unterrichtet. Da Dokumentationen von Erkrankungen bzw. gesundheitlichen Beeinträchtigungen in einzelnen nachgewiesenen Fällen Verletzungen des Rechts der Betroffenen auf informationelle Selbstbestimmung zur Folge hatten, wurden diese mit einer gegen die Vertriebsgesellschaft festgesetzten Geldbuße in Höhe von 36.000 Euro geahndet. Nicht festgestellt werden konnte, ob die Verwendung der formularmäßig vorgegebenen Listen aufgrund unternehmensweiter Direktiven erfolgt war.

➡ Gerade beim Umgang mit sensiblen Gesundheitsdaten müssen Unternehmen besonders sorgfältig auf die Einhaltung grundlegender Regelungen des Datenschutzes achten.

5 Internationaler Datenverkehr

5.1 SWIFT-Abkommen

Am 01. August 2010 trat das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und Übermittlung aus der Europäischen Union in Kraft (sogenanntes SWIFT-Abkommen). Das Abkommen enthält einige gegenüber der vorherigen Situation positive Regelungen zum Datenschutz. Generelle Kritikpunkte an der Übermittlung der Banktransaktionsdaten bleiben aber bestehen.

In der Folge der Attentate vom 11. September 2001 hatte sich das US-Finanzministerium nach US-amerikanischem Recht Zugang zu Zahlungsverkehrsdaten des belgischen Finanzdienstleistungsunternehmens SWIFT (Society for Worldwide Interbank Financial Telecommunication) verschafft, um daraus im Rahmen des Terrorist Finance Tracking Program (TFTP) Erkenntnisse über die Finanzierung von terroristischen Aktivitäten zu gewinnen. Das Unternehmen SWIFT wickelt weltweit den größten Teil und nahezu den gesamten europäischen Überweisungsdatenverkehr zwischen den Banken ab. SWIFT unterhielt bisher ein Rechenzentrum in den Niederlanden und eines in den USA. In beiden Rechenzentren waren jeweils sämtliche Transaktionsdaten weltweit gespeichert, um bei Ausfall eines Systems eine Datensicherung an einem anderen Ort zu gewährleisten. So konnten die US-Behörden im Rechenzentrum in den USA auch auf Banktransaktionsdaten zugreifen, die keinerlei unmittelbaren Bezug zu den USA hatten oder gar rein innereuropäischen Zahlungsverkehr betrafen.

Nachdem dieser Datenzugriff bekannt wurde, errichtete SWIFT ein weiteres Rechenzentrum in der Schweiz, das in getrennten Bereichen die Spiegelung der Transaktionsdaten aus Europa und den USA übernehmen und somit die Speicherung europäischer Daten in den USA obsolet machen sollte. Zum Jahreswechsel 2009/2010 ging dieses Rechenzentrum in Betrieb. Der direkte Datenzugriff war den US-Behörden in der Folge verwehrt. Im Einzelfall konnten Daten über ein Rechtshilfeabkommen angefordert werden.

Das SWIFT-Abkommen ermöglicht dem US-Finanzministerium inzwischen wieder den Zugriff auf Datenpakete. Es verpflichtet die US-Seite

allerdings, die benötigten Datenpakete möglichst präzise zu beschreiben. Ein wesentlicher Kritikpunkt gegenüber dem Abkommen besteht darin, dass die Institution Europol kontrolliert, ob dieser Präzisierungspflicht genügt wird. Europol dürfte nicht unbedingt an einer restriktiven Übermittlungspraxis interessiert sein, da Europol gemäß dem Abkommen selbst Erkenntnisse aus dem TFTP erhalten kann. Unabhängige Richterinnen und Richter oder Datenschutzbeauftragte sind in die Überprüfung der Zulässigkeit der Datenübermittlungen nicht eingebunden.

In der Praxis wird sich die Datenanforderung des US-Finanzministeriums auf bestimmte Überweisungsvorgänge einer bestimmten Bank in konkrete Länder in einem festgelegten Zeitraum beziehen. Aus technischen Gründen wird ein Datenpaket mit allen Überweisungsdaten der betroffenen Bank in dem benannten Zeitraum übermittelt. Die konkret geforderten Daten werden in den USA aus dem Datenpaket extrahiert. Nicht extrahierte Daten sind spätestens nach Ablauf von fünf Jahren zu löschen.

Das Abkommen schließt die Übermittlung von Daten aus, die sich auf den Einheitlichen Europäischen Zahlungsverkehrsraum (SEPA = Single European Payments Area) beziehen. Da die technische Umstellung auf das SEPA-Verfahren noch nicht abgeschlossen ist, sollen derzeit noch rund 200 Millionen Zahlungsvorgänge in der Region Europa/Naher Osten/Afrika jährlich außerhalb des SEPA-Verfahrens abgewickelt und können grundsätzlich von den USA angefordert werden. Abfragen unterliegen einer strengen Zweckbindung. Daten dürfen nur zur Aufklärung terroristischer Aktivitäten angefordert werden. Eine Rückübermittlung von Erkenntnissen an europäische Polizeistellen ist ausdrücklich vorgesehen. Europäische Sicherheitsbehörden können ihrerseits das US-Finanzministerium bitten, konkrete Suchaufträge in den Daten durchzuführen. An Drittstaaten dürfen lediglich Erkenntnisse aus den Daten aber keine Rohdaten weitergegeben werden.

Betroffene haben zwar grundsätzlich einen Auskunftsanspruch, der aber aus Gründen nationaler Sicherheit oder im Interesse einer effektiven Strafverfolgung beschränkt sein kann. Der Auskunftsanspruch ist über die nationalen europäischen Datenschutzbehörden geltend zu machen. In Deutschland nimmt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zentral Auskunftsbegehren zur

Weiterleitung an den Datenschutzbeauftragten des US-Finanzministeriums entgegen.

Das Abkommen gilt für 5 Jahre und verlängert sich danach automatisch jährlich, sofern es nicht gekündigt wird. Eine erste Überprüfung des Abkommens ist nach einem halben Jahr vorgesehen.

➡ Die Evaluation des SWIFT-Abkommens muss den tatsächlichen Nutzen für das Terrorist Finance Tracking Program überprüfen. Pauschale Datenübermittlungen sind nicht zu rechtfertigen, wenn sich daraus keine nachweisbaren und deutlichen Erfolge in der Terrorismusbekämpfung ergeben. Der grundsätzlich angemessene Weg für Datenübermittlungen muss ansonsten die Rechtshilfe im konkreten Einzelfall bleiben.

5.2 Passagierdatenübermittlung

Ende 2010 hat die Europäische Kommission Mandate zur Verhandlung neuer Passagierdatenabkommen mit den USA, Kanada und Australien erhalten. Sie verfolgt nun eine globale Passagierdatenstrategie.

Diese Strategie zielt darauf, möglichst gleich gelagerte Vereinbarungen mit allen Staaten zu treffen, die von den Fluggesellschaften Reservierungsdaten der Reisenden für Zwecke der Terrorismus- und Kriminalitätsbekämpfung fordern. Es wird außerdem für Anfang 2011 erwartet, dass die EU-Kommission einen überarbeiteten Vorschlag für ein europäisches System zur Passagierdatenauswertung vorlegt. Derzeit schon fordern britische Sicherheitsbehörden von den Fluggesellschaften Reservierungsdaten für Flüge von und nach Großbritannien auch für innereuropäische Flugrouten. Da es für eine solche Datenübermittlung für in Deutschland gespeicherte oder erhobene Daten keine Übermittlungsgrundlage gibt, konnte dieses Ansinnen der britischen Behörden bisher von den deutschen Fluggesellschaften abgewehrt werden.

Die Arbeitsgruppe nach Art. 29 der EG-Datenschutzrichtlinie hat in ihrer Stellungnahme WP 178 vom 12. November 2010 die globale Passagierdatenstrategie der EU-Kommission zu Recht scharf kritisiert. Insbesondere wird moniert, dass der tatsächliche Nutzen der Auswer-

tung der Reservierungsdaten von Flugpassagieren niemals evaluiert wurde. Vielmehr wird im Gegenteil in der wissenschaftlichen Fachliteratur die Effektivität von Data-Mining-Verfahren für Sicherheitszwecke bestritten, wie sie bei der Passagierdatenübermittlung eingesetzt werden. Alle bisher geltenden und vorgeschlagenen Regelungen für Systeme zur Auswertung von Reservierungsdaten sehen zudem langfristige Speicherfristen von mindestens fünf Jahren vor. Eine solche Datenvorratshaltung ist überaus problematisch, weil sie Bewegungsbilder ermöglicht und eine zwingende Notwendigkeit für spätere Ermittlungsverfahren kaum gegeben sein dürfte. Da Buchungsdaten für Abrechnungszwecke bei den Reservierungsdatenbankbetreibern ohnehin bis zu zwei Jahre gespeichert bleiben, lassen sich in konkreten Ermittlungsverfahren bei Straftaten von erheblicher Bedeutung auch dort Buchungen rekonstruieren.

- Solange die Eignung und Erforderlichkeit der Reservierungsdatenauswertung für die Terrorismusbekämpfung nicht nachgewiesen ist, verbietet sich jede offensive Passagierdatenstrategie. Die als Ausnahmebefugnis zur Terrorismusbekämpfung zugelassene Passagierdatenauswertung darf nicht zum Standardmittel der Kriminalitätsbekämpfung werden.

5.3 Internationale Datenübermittlungen zwischen Unternehmen

Die Europäische Kommission hat am 5. Februar 2010 einen neuen Standardvertrag für die Auftragsdatenverarbeitung verabschiedet. Die Praxis hinsichtlich der Anerkennung von verbindlichen Unternehmensregelungen (Binding Corporate Rules – BCR) als Grundlage für Datenübermittlungen in das Ausland hat sich fortentwickelt.

Der neue Standardvertrag für die Übermittlung von personenbezogenen Daten an Auftragnehmerinnen und Auftragnehmer in Drittstaaten ohne angemessenes Datenschutzniveau ersetzt den Standardvertrag, der mit der Kommissionsentscheidung vom 27. Dezember 2001 veröffentlicht wurde. Laufende Standardverträge, die nach dem alten Vertragsmuster abgeschlossen wurden, bleiben bestehen. Werden allerdings bei Altverträgen Vertragsanpassungen vorgenommen, so ist

der bisherige Vertrag durch das neue Standardvertragsmuster zu ersetzen.

Wie schon der alte kann auch der neue Standardvertrag zugleich als Vertrag nach § 11 Bundesdatenschutzgesetz (BDSG) genutzt werden. Das setzt aber voraus, dass die Vorgaben des § 11 BDSG, soweit sie nicht ohnehin schon im Standardvertrag geregelt sind, in den Anlagen zum Vertrag konkretisiert werden.

Für die Anwendung des neuen Standardvertrags in der Praxis hat im Übrigen die Arbeitsgruppe nach Art. 29 der EG-Datenschutzrichtlinie in ihrem Arbeitspapier 176 vom 12. Juli 2010 wertvolle Hinweise gegeben. Darin wird unter anderem klargestellt, dass der Standardvertrag keine Anwendung auf rein innereuropäische Auftragsverhältnisse findet. Wenn sich ein Auftragnehmer in Europa für seinen europäischen Auftraggeber um Datenschutzgarantien bei einem Subunternehmen kümmern soll, bleibt es wie bisher dabei, dass der Auftraggeber den Auftragnehmer bevollmächtigen muss, für ihn den Standardvertrag oder ein vergleichbares Instrument mit dem Subunternehmen zu vereinbaren.

Verbindliche Unternehmensregelungen als Garantie für eine Übermittlung personenbezogener Daten in Drittstaaten innerhalb eines Konzernverbundes sind zwar nach wie vor ein für Konzerne interessantes Instrument. Es sind allerdings auch Klagen von Unternehmensvertreterinnen und -vertretern zu hören, dass die Anerkennung von BCR durch die verschiedenen europäischen Datenschutzaufsichtbehörden ein schwerfälliger und langwieriger Prozess sei.

Die Beschleunigung dieses Prozesses kann zum einen durch die Konzerne selbst betrieben werden. Die Arbeitspapiere der Arbeitsgruppe nach Art. 29 der EG-Datenschutzrichtlinie erläutern sehr präzise, welche Inhalte BCR haben müssen, um anerkennungsfähig zu sein. Leider wird dem in der Praxis noch zu wenig Beachtung geschenkt, der Korrekturbedarf war bei den BCR einiger Konzerne relativ hoch, was nicht unbedingt zur Beschleunigung des Verfahrens beitrug.

Durch die politische Erklärung der gegenseitigen Anerkennung der Prüfergebnisse (mutual recognition) konnte der Bearbeitungsprozess von Seiten der Datenschutzaufsichtsbehörden in den letzten anderthalb Jahren erheblich beschleunigt werden. Die Datenschutzbehörden von Belgien, Bulgarien, Deutschland, Frankreich, Großbritannien, Ir-

land, Island, Italien, Lettland, Liechtenstein, Luxemburg, Malta, Niederlanden, Norwegen, Österreich, Slowenien, Spanien und Tschechien haben die Erklärung unterzeichnet und damit ausgesagt, dass sie bei Anerkennung von BCR durch eine der Datenschutzaufsichtsbehörden dieses Ergebnis akzeptieren werden.

➡ Die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden im Bereich der Datenübermittlung durch Unternehmen an Stellen in Drittstaaten wird immer effektiver.

5.4 Dienstleistungsrichtlinie und Binnenmarktinformationssystem

Bis zum 28. Dezember 2009 musste die Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt (Dienstleistungsrichtlinie) in nationales Recht umgesetzt werden. Durch die Umsetzung entstehen neue und zum Teil sensible Datenverarbeitungsvorgänge bei sogenannten Einheitlichen Ansprechpartnern und im von der Europäischen Union vorgegebenen Binnenmarktinformationssystem. Die Einführung wurde von meiner Behörde begleitet und die Anwendung wird weiter beobachtet werden.

Die Dienstleistungsrichtlinie soll einen einheitlichen Rechtsrahmen für den freien Dienstleistungsverkehr im Europäischen Wirtschaftsraum schaffen. Insbesondere sind Verfahren vorgesehen, damit Genehmigungen, die zur Erbringung von Dienstleistungen auf dem inländischen Markt eingeholt werden müssen, unkompliziert auch von Personen aus anderen Mitgliedstaaten der Europäischen Union sowie aus Norwegen, Liechtenstein und Island gestellt werden können.

Hierzu waren Einheitliche Ansprechpartner zu installieren, die Antragstellenden aus dem Ausland den Weg zur zuständigen Genehmigungsbehörde in Deutschland weisen und die zügige Abwicklung des Genehmigungsverfahrens überwachen. Der Informationsfluss zwischen den Behörden des Europäischen Wirtschaftsraumes im Zusammenhang mit der Dienstleistungsrichtlinie wird über das internetbasierte

Binnenmarktinformationssystem – Internal Market System (IMI) – abgewickelt, das die Europäische Kommission bereitstellt.

Das Institut des Einheitlichen Ansprechpartners wurde in Nordrhein-Westfalen mit dem Gesetz zur Bildung Einheitlicher Ansprechpartner (EA-Gesetz NRW) und einer Ergänzung des Verwaltungsverfahrensgesetzes in das Landesrecht übernommen. Meine Behörde hatte in dem Gesetzgebungsverfahren empfohlen, die datenschutzrechtlichen Grundsätze der Zweckbindung und Datensparsamkeit im EA-Gesetz NRW ausdrücklich hervorzuheben. Da die Einheitlichen Ansprechpartner sämtliche Genehmigungsunterlagen weiterleiten, ist in der Praxis die Gefahr relativ hoch, dass sie aus diesen Unterlagen mehr Daten nutzen oder speichern, als für ihre Aufgabe der Weiterleitung von Anträgen und Überwachung von Fristen tatsächlich benötigt werden. Es sollte in jedem Fall vermieden werden, dass bei den Einheitlichen Ansprechpartnern Parallelakten zu den Vorgängen der Genehmigungsbehörden entstehen.

Die Landesregierung ist der Empfehlung nicht gefolgt. Ihre Begründung, dass sich die Grundsätze der Zweckbindung und Datensparsamkeit bereits aus dem Datenschutzgesetz Nordrhein-Westfalen ergeben, ist zutreffend. Da diese Grundsätze aber nicht auf jedem Arbeitsplatz im Lande stets präsent sind und gerade bei Koordinierungsfunktionen in der Praxis häufig verletzt werden, hätte ein Hervorheben im Fachgesetz die Einheitlichen Ansprechpartner unmittelbarer auf die Problematik aufmerksam gemacht. Im Ergebnis bleibt es allerdings dabei, dass sich die Einheitlichen Ansprechpartner auf die Verarbeitung der Daten beschränken müssen, die für die Weiterleitung der Anträge und Überwachung der Fristen im Genehmigungsverfahren erforderlich sind. Sie dürfen keine Daten speichern oder nutzen, die ausschließlich von den Behörden benötigt werden, die die Genehmigungen erteilen.

Das IMI soll die Kommunikation der Behörden im Europäischen Wirtschaftsraum untereinander erleichtern. Derzeit wird es außer bei Verfahren nach der Dienstleistungsrichtlinie bei der Anerkennung von Berufsqualifikationen gemäß der Richtlinie 2005/36/EG genutzt. Es ist geplant, weitere innereuropäische Behördenkommunikation über das IMI abzuwickeln, daher muss diesem System ein besonderes Augenmerk geschenkt werden.

Über das System dürfen nur solche personenbezogenen Daten ausgetauscht werden, für deren Übermittlung es eine Rechtsgrundlage gibt. Das IMI ist ein Mittel zum Datenaustausch, legitimiert aber nicht die Übermittlung im Einzelfall. Seine Funktionsweise verleitet indessen unter Umständen dazu, dass Behörden mehr Informationen austauschen, als im Ergebnis datenschutzrechtlich zulässig ist: Wenn beispielsweise eine deutsche Genehmigungsbehörde die Zuverlässigkeit einer Antragstellerin oder eines Antragstellers aus Portugal überprüfen muss, kann sie die in Portugal zuständige Behörde über das IMI ermitteln. Mittels eines im IMI vorgefertigten Fragenkatalogs kann die Genehmigungsbehörde dann die von ihr benötigten Angaben erfragen. Das IMI leitet die Fragen ins Portugiesische übersetzt an die zuständige Behörde weiter.

Die anfragende Behörde darf über das IMI nur die Angaben erfragen, die tatsächlich für die Antragsprüfung erforderlich sind. Wenn die deutsche Behörde etwa nach nationalem Recht keine Informationen über etwaige Strafverfahren der Antrag stellenden Person für die Entscheidung über die Genehmigung heranziehen darf, darf sie dies auch nicht über das IMI bei einer Behörde in Portugal abfragen, selbst wenn das IMI dies im Fragenkatalog anbieten sollte. Umgekehrt muss speziell eine nordrhein-westfälische Behörde nach dem Datenschutzgesetz Nordrhein-Westfalen bei Anfragen von Behörden aus anderen Mitgliedstaaten klären, ob die Anfrage von der zuständigen Behörde gestellt wird. Die Zulässigkeit der Übermittlung ist dann im Einzelfall zu prüfen, wenn sich Anhaltspunkte ergeben, dass eine Anfrage unzulässig sein könnte. Das wäre etwa dann der Fall, wenn Informationen eingefordert werden, die offensichtlich keinen Bezug zu dem konkreten Genehmigungsantrag haben.

Das IMI ist ein hoch komplexes Datenverarbeitungsverfahren, bei dem langfristig sichergestellt werden muss, dass insbesondere die Datenschutzrechte der Personen gewahrt werden, deren Daten in dem System gespeichert sind und ausgetauscht werden. In dem Verfahren muss insbesondere gewährleistet sein, dass nur aktuelle, korrekte und erforderliche Daten gespeichert sind. Erst die Praxis wird zeigen, ob das System das gewährleisten kann. Der Europäische Datenschutzbeauftragte hat daher mit Blick auf die für 2011 geplante Evaluierung des IMI in einer Presseerklärung vom 27. Oktober 2010 zu Recht darauf gedrängt, dass die Systemarchitektur den Datenschutz

einbaut (privacy by design) und das System in Kooperation mit den Datenschutzbehörden der Mitgliedstaaten fortentwickelt und gesetzlich verankert wird.

- Es muss in der Praxis sichergestellt sein, dass bei den Einheitlichen Ansprechpartnern kein zentraler Datenpool mit inhaltlichen Daten aus Genehmigungsverfahren entsteht.

- Das IMI muss datenschutzgerecht ausgebaut werden. Dieser Prozess ist von den Datenschutzbeauftragten weiter kritisch zu begleiten.

6 Wirtschaft

6.1 Neue Regelungen zu Auskunfteien und Scoring

Der Bundestag beschloss im Sommer 2009 neue Regelungen zu Auskunfteien und Scoring, die im April 2010 in Kraft traten. Scoring ist die Prognose eines zukünftigen Verhaltens, die mit statistischen Methoden erstellt und für Entscheidungen im Zusammenhang mit Verträgen herangezogen wird. Wie viel Datenschutz tatsächlich gewagt wurde, zeigt die folgende Übersicht über die wesentlichen Neuerungen.

"Mehr Datenschutz wagen!" lautete auch der Titel im Bericht 2009 zum Beitrag über den damaligen Gesetzentwurf der Bundesregierung zu Auskunfteien und Scoring (siehe Bericht 2009 unter Ziffer 6.1). Nachdem meine Behörde bereits 2004 gesetzliche Regelungen für mehr Transparenz und Fairness bei Auskunfteien und Scoring gefordert und der Bundestag 2005 über alle Fraktionsgrenzen hinweg gesetzgeberischen Handlungsbedarf zum Datenschutz bei Auskunfteien festgestellt hatte, folgten mehr als ein halbes Dutzend Gesetzentwürfe und ein langes Ringen der unterschiedlichen Interessengruppen. Im Wesentlichen ergeben sich folgende Änderungen:

- **Unentgeltliche Selbstauskunft von Auskunfteien einmal im Kalenderjahr (§ 34 Abs. 8 BDSG)**

Diese Änderung führte unmittelbar nach Inkrafttreten des Gesetzes zu einem – wie eine Auskunftei es ausdrückte – "Tsunami" an Auskunftsbegehren. Ein Nebeneffekt der erleichterten Transparenz ist auch die verbesserte Datenqualität der Auskunfteibestände. Denn die Betroffenen weisen die Auskunfteien nun häufiger auf veraltete oder sonstige unrichtige Daten hin und stellen damit einen Mangel ab, auf den Verbraucherstudien wiederholt aufmerksam machten: Die zu den einzelnen Personen gespeicherten Datensätze sind als Grundlage für die Score-Berechnungen der Auskunfteien nicht nur dünn, sondern oftmals auch fehlerhaft. Im Ergebnis führt der unentgeltliche Auskunftsanspruch daher auch zu akkurateren Datensätzen und einer solideren Datenbasis für das Scoring der Auskunfteien. Mehr zum Thema Selbstauskünfte wie auch zu allen anderen Datenschutzfragen zu Auskunfteien und Scoring finden Sie unter www.ldi.nrw.de.

- **Erweiterte Auskunftsrechte zu Score-Werten (§ 34 Abs. 2 und 4 BDSG)**

Eine zentrale Forderung des Daten- und Verbraucherschutzes war die nach mehr Transparenz bei den oftmals als "Black Box" bezeichneten Score-Verfahren (zu der entscheidenden Bedeutung der Transparenz für das Scoring und den rechtlichen und technischen Möglichkeiten, diese zu verbessern, siehe Bericht 2007 unter Ziffer 7.1). Der nun ins Gesetz aufgenommene Auskunftsanspruch umfasst

- die Score-Werte, die ein Unternehmen innerhalb der letzten sechs Monate erhoben oder erstmalig gespeichert hat bzw. – bei Auskunfteien – die aktuellen sowie die innerhalb der letzten 12 Monate übermittelten Score-Werte,
- die Datenarten, die zur Berechnung der Score-Werte genutzt wurden und
- eine einzelfallbezogene und nachvollziehbare Erklärung über das Zustandekommen und die Bedeutung der Score-Werte.

Bei der Umsetzung der letzten beiden Punkte tun sich viele Banken und Auskunfteien schwer:

Bei der Auskunft über die genutzten "Datenarten" dürfen nach der Gesetzesbegründung zwar einzelne Score-Merkmale zu Datenarten zusammengefasst werden. Die Begründung nennt als Beispiel die Zusammenfassung der Merkmale Postleitzahl, Stadt, Straße und Hausnummer zur Datenart "Adressdaten". Entscheidend ist jedoch nach der Gesetzesbegründung, "dass der Betroffene nachvollziehen kann, welche Merkmale in das konkrete Berechnungsergebnis eingeflossen sind". Die teilweise von den Banken und Auskunfteien gewählten Zusammenfassungen ("Persönliche Daten", "Allgemeine Kundendaten", "Finanzierungsrelevante Daten") sind zu allgemein und informieren die Betroffenen daher nur unzureichend.

Ein weiteres Umsetzungsdefizit gibt es bei den Erklärungen über das Zustandekommen der individuellen Score-Werte. Sie sollen den einzelnen Bürgerinnen und Bürgern die Frage beantworten, welches die wesentlichen Gründe für die konkreten Werte sind. Hier sind in der Praxis einige Auskünfte weder einzelfallbezogen noch nachvollziehbar. Ein Positivbeispiel für eine verständliche Darstellung ist die Ampel-Grafik einiger Banken zu den einzelnen für das Scoring genutzten Da-

tenarten. Dabei zeigen etwa rot gekennzeichnete Datenarten, dass diese den Score-Wert negativ beeinflusst haben.

- **Neue Bußgeldtatbestände für nicht erteilte Selbstauskünfte (§ 43 Abs. 1 Nr.8-8c BDSG)**

Bis zur Novelle waren die Unternehmen und sonstigen Stellen zwar zur Auskunftserteilung an die Verbraucherinnen und Verbraucher verpflichtet, aber diese Pflicht konnte ungestraft verletzt werden. Erst die Einschaltung der Datenschutzaufsicht führte dann im Einzelfall zur Gesetzestreue. Diese Gesetzeslücke wurde nun geschlossen. Jetzt ist bereits die unterlassene, nicht richtige, unvollständige oder nicht rechtzeitig erteilte Auskunft ein Bußgeldtatbestand .

- **Neue Norm zu Datenübermittlungen an Auskunfteien (§ 28a BDSG)**

Erstmals gibt es nun konkretere Regelungen, welche Informationen Unternehmen an Auskunfteien weitergeben dürfen.

- Übermittlung von Negativdaten zu Forderungen

Der neue § 28a Abs. 1 BDSG enthält einen abschließenden Katalog der fünf Fallgruppen, in denen die Übermittlung von Daten zu fälligen, nicht erbrachten Forderungen (Negativdaten) zulässig ist, soweit diese eindeutig Rückschlüsse auf die Zahlungsunfähigkeit oder -unwilligkeit der betroffenen Person zulassen (zu den einzelnen Voraussetzungen siehe unter www.ldi.nrw.de).

Neben titulierten, also etwa durch Urteil oder Vollstreckungsbescheid festgestellten Forderungen, ist in der Praxis insbesondere die Fallgruppe der untitulierten Forderungen von Bedeutung. Eine untitulierte Forderung darf nur dann bei einer Auskunftei eingemeldet werden, wenn sie unbestritten und mindestens zweimal erfolglos gemahnt worden ist (wobei zwischen der ersten Mahnung und der Übermittlung an die Auskunftei mindestens vier Wochen liegen müssen) und die betroffene Person rechtzeitig von der bevorstehenden Übermittlung unterrichtet worden ist. Insbesondere das Erfordernis der vorherigen Unterrichtung der Betroffenen, das in der Aufsichtspraxis von meiner Behörde entwickelt und nun auch gesetzlich festgeschrieben wurde, ist wichtig, um die Einmeldung strittiger Forderungen hinter dem Rücken der Betroffenen zu verhindern.

- Verbot, Konditionenanfragen einzumelden

Positiv hervorzuheben ist die nunmehr im § 28a Abs. 2 BDSG enthaltene ausdrückliche Klarstellung, dass Banken Anfragen von Kundinnen und Kunden zu Kreditkonditionen nicht in den Auskunftsbestand einer Auskunftei übermitteln dürfen. Bis Mitte 2006 und teilweise noch darüber hinaus wurde Kreditsuchenden das aus Sicht des Verbraucherschutzes sinnvolle Verhalten zum Verhängnis, sich vorab bei mehreren Banken nach den – oftmals bonitätsabhängigen – Konditionen zu erkundigen: Holten Kreditinstitute in derartigen Fällen eine Bonitätsauskunft ein, führten diese Anfragen regelmäßig zu einer Verschlechterung der von der Auskunftei berechneten Score-Werte. Das paradoxe Ergebnis: Wer viele Banken nach günstigen Zinsen fragte, verschlechterte mit jeder Anfrage die Aussichten auf einen Kredit mit günstigen Zinsen. Mit der neuen Regelung ist nun gesetzlich festgeschrieben, dass Informationen über sogenannte Konditionenanfragen nicht für Auskünfte oder Score-Berechnungen genutzt werden dürfen.

- Mitteilungspflicht bei nachträglichen Änderungen

Abs. 3 des neuen § 28a BDSG verpflichtet Unternehmen, die Daten an Auskunfteien übermitteln, die Auskunfteien auch über nachträgliche Änderungen der zugrunde liegenden Sachverhalte zu informieren. Dies soll dazu beitragen, dass die Datensätze der Auskunfteien tatsächlich aktuell und richtig sind.

- **Neue Norm zu Anforderungen an Scoring-Verfahren (§ 28b BDSG)**

Die neue Regelung beantwortet nun erstmals, wenn auch abstrakt, die Frage, welche personenbezogenen Daten in die Berechnung eines Score-Wertes einfließen dürfen. Für das Scoring dürfen nur Daten der Betroffenen genutzt werden, die

  - eine mathematisch-statistisch erwiesene Relevanz für das mit dem Scoring prognostizierte Vertragsverhalten – etwa die Rückzahlung eines Kredits – haben (§ 28b Nr. 1 BDSG) und
  - auch unabhängig von dem Score-Verfahren für den Zweck – etwa Bonitätsprüfung – genutzt werden dürften (§ 28b Nr. 2 BDSG).

Das erste Kriterium untersagt die Verwendung von Daten ohne statistisch nachweisbare Aussagekraft. Die zweite Voraussetzung verbietet die Verwendung von Daten, die unter rechtlichen Gesichtspunkten nicht für den mit dem Scoring verfolgten Zweck genutzt werden dürfen. So dürfen Auskunfteien Daten, die sie ausschließlich für die Identitätsprüfung erhalten haben (etwa Voranschriften der Betroffenen), nicht ohne Einwilligung zweckändernd für die Bonitätsprüfung nutzen (zur Verwendung der Voranschriften als Scoring-Merkmal "Anzahl der Umzüge" siehe Bericht 2005 unter Ziffer 5.7).

Beim Kredit-Scoring ist die Wertung des § 10 Abs. 1 Kreditwesengesetz zu berücksichtigen. Daher dürfen die Staatsangehörigkeit und die in § 3 Abs. 9 BDSG genannten sensitiven Daten, wie zum Beispiel Angaben zur Gesundheit, nicht genutzt werden. Zulässig sind dagegen zutreffende, signifikante Daten zum Zahlungsverhalten sowie zu den Einkommens-, Vermögens- und Beschäftigungsverhältnissen. Noch nicht abschließend geklärt sind die Auswirkungen des Allgemeinen Gleichbehandlungsgesetzes auf die Nutzung etwa des Merkmals "Geschlecht" für das Kredit-Scoring.

- **Nutzung von Anschriftendaten (Wohnumfeldbewertung) für die Score-Berechnung (§ 28b Nr. 3 und 4 BDSG)**

Dieser Punkt wurde zum Abschluss des Gesetzgebungsverfahrens besonders kontrovers diskutiert. Verbraucher- und Datenschützerinnen und -schützer hatten sich für ein Verbot der Wohnumfeldbewertung beim Kredit-Scoring ausgesprochen. Sie verwiesen zum einen auf die negativen Folgen für die einzelne Person, die in "statistische Sippenhaft" genommen werde mit den sonstigen Personen in ihrem Stadtteil und deren durchschnittlichem Ausfallrisiko. Zum anderen wirke eine derartige Diskriminierung wie eine sich selbst erfüllende Prophezeiung und könne zur sozialen Ausgrenzung ganzer Stadtteile führen: Um nicht länger höhere Zinsen zahlen zu müssen oder bestimmte Leistungen nur verteuert angeboten zu bekommen, weil die Zahlungsmoral in der Nachbarschaft tatsächlich oder vermeintlich schlecht ist, könnten Personen mit höherem Einkommen oder Vermögen das Viertel verlassen oder gar nicht erst dort hinziehen. Am Ende wohnten dann tatsächlich nur noch die Personen dort, die sich einen Umzug in einen besser bewerteten Stadtteil nicht leisten können.

Im Gegenzug argumentierten die Unternehmen, die von den zu bewertenden Personen häufig kaum mehr als das Geschlecht, das Alter und die Anschrift kennen (wie etwa Versandhändler), dass sie darauf angewiesen seien, das Ausfallrisiko zu beurteilen und dass sie daher nicht auf die Wohnumfeldbewertung verzichten könnten.

Am Ende verabschiedeten Bundestag und Bundesrat eine Regelung, die zwar erhöhte Anforderungen an die Nutzung von Anschriftendaten stellt, das sogenannte Geoscoring damit aber grundsätzlich für zulässig erklärt. Danach dürfen Anschriftendaten für die Score-Berechnung genutzt werden, wenn

- die oben genannten allgemeinen Voraussetzungen des § 28b BDSG erfüllt sind,
- es weitere (wesentliche) Score-Parameter gibt und
- die Betroffenen vorher (!) über die Nutzung der Anschriftendaten für das Scoring unterrichtet wurden; die Unterrichtung ist zu dokumentieren.

➡ Im deutlichen Gegensatz zu den Änderungen beim Adresshandel (siehe unter Ziffer 3.1) hat der Gesetzgeber mit den neuen Regelungen zu Auskunfteien und Scoring mehr Datenschutz gewagt. Auch wenn nicht alle Forderungen der Daten- und Verbraucherschützer berücksichtigt wurden, ermöglichen die Neuerungen nennenswerte Fortschritte für die Bürgerinnen und Bürger. Mit Auslegungshinweisen, Beratungen, Verhandlungen und Kontrollen werde ich weiterhin auf fairere und transparentere Verfahren hinwirken.

6.2 Bonitätsauskünfte über Mietinteressierte

Vermieterinnen oder Vermieter holen oftmals vor Abschluss eines Mietvertrages Bonitätsinformationen über ihre potentiellen Mieterinnen und Mieter bei Auskunfteien ein, weil sie sich so vor möglichen Zahlungsausfällen schützen wollen. Manchmal verlangen sie auch die Vorlage einer sogenannten Selbstauskunft von den Bewerberinnen und Bewerbern.

Die Datenschutzaufsichtsbehörden haben nun im Oktober 2009 mit ihrem Beschluss "Bonitätsauskünfte über Mietinteressierte nur eingeschränkt zulässig" (Abdruck im Anhang) einheitlich und konkret festgelegt, unter welchen Voraussetzungen und in welchem Umfang Auskunfteien Vermieterinnen und Vermietern Bonitätsinformationen über Mietinteressierte übermitteln dürfen. Der Beschluss vereinheitlicht die bis dahin teilweise unterschiedlichen Ansichten der einzelnen Aufsichtsbehörden (zur bisherigen Auffassung meiner Behörde siehe Bericht 2007 unter Ziffer 7.6).

Vermieterinnen und Vermieter dürfen nur dann Bonitätsinformationen über Mietinteressierte bei Auskunfteien einholen, wenn der konkrete Abschluss eines Mietvertrages lediglich noch von dem positiven Ergebnis einer Bonitätsprüfung abhängt. Dabei muss die Vermieterin oder der Vermieter ein berechtigtes Interesse an den Bonitätsauskünften glaubhaft darlegen. Außerdem darf kein Grund zu der Annahme bestehen, dass die betroffenen Mietinteressenten ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

Da Vermieterinnen und Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass eine Mieterin oder ein Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit die Miete oder die Nebenkosten nicht begleicht, ist ein berechtigtes Interesse auf der Vermieterseite an Bonitätsinformation über Mietinteressierte durchaus anzuerkennen. Dem stehen die schutzwürdigen Belange der Mietinteressierten gegenüber. In die nach § 29 Bundesdatenschutzgesetz (BDSG) erforderliche Abwägung dieser Interessenlagen fließen insbesondere die existentielle Bedeutung von Wohnraum, die Vorgaben der gesetzlichen Regelungen im Bereich des Mietrechts (wie Kündigungsmöglichkeiten, Mietkautionen oder das Vermieterpfandrecht) und der mögliche Eintritt von Sozialbehörden in die Zahlungspflicht ein. Im Ergebnis dürfen Auskunfteien daher nur einen eingeschränkten Datenkatalog an Vermieterinnen und Vermieter übermitteln.

Um den Abwägungsanforderungen des § 29 BDSG gerecht zu werden, sind verschiedene Lösungswege denkbar. Die Aufsichtsbehörden hatten die Auskunfteien im Vorfeld ihres Beschlusses mehrfach aufgefordert, Vorschläge zu unterbreiten, die den genannten Anforderungen entsprechen und die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind. Die Auskunfteien haben diese Möglichkeit bislang nicht genutzt.

Daher haben sich die Aufsichtsbehörden in dem genannten Beschluss auf einen Datenkatalog verständigt, der den Anforderungen des § 29 BDSG genügt. Danach dürfen Auskunfteien folgende Daten an Vermieterinnen und Vermieter übermitteln:

- Informationen aus öffentlichen Schuldner- oder Insolvenzverzeichnissen
- sonstige Daten über negatives Zahlungsverhalten, bei denen
    - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und
    - eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

Die Beauskunftung erledigter Forderungen für die Dauer von nur einem Jahr eröffnet den Betroffenen die Möglichkeit einer "zweiten Chance": Wer alle ausstehenden Forderungen beglichen hat und sich ein Jahr lang als zahlungsfähig und -willig erwiesen hat, soll nicht durch erledigte Sachverhalte aus der Vergangenheit unvertretbar bei der Suche nach Wohnraum behindert werden.

Die festgelegte Bagatellgrenze soll verhindern, dass offene Kleinstbeträge wie zum Bespiel eine nicht beglichene Handyrechnung den Abschluss eines Mietvertrages unverhältnismäßig erschweren.

Auch die Übermittlung von Wahrscheinlichkeitswerten (sogenannten Scorewerten) ist unzulässig, sofern diese auf anderen als den von den Aufsichtsbehörden festgelegten Daten beruhen.

Zudem ist es unzulässig, die Vorlage einer Selbstauskunft zu verlangen, die Mietinteressierte bei den Auskunfteien selbst einholen können. Solche Selbstauskünfte können wesentlich mehr Angaben über die finanziellen Verhältnisse der Betroffenen enthalten, als sie etwa den Vermieterinnen oder Vermietern als Vertragspartei der Auskunfteien mitgeteilt würden. Ebenso unzulässig ist es, von den Mietinteressierten eine Einwilligung in die Einholung einer Bonitätsauskunft zu verlangen, da diese Einwilligung aufgrund der Zwangslage der Betroffenen regelmäßig nicht freiwillig erteilt werden kann und damit unwirksam ist.

- Wohnungswirtschaft und Auskunfteien sind aufgefordert, künftig nur noch Bonitätsinformationen über Mietinteressierte in einem Umfang zu erheben bzw. zu übermitteln, der die schutzwürdigen Belange der Betroffenen angemessen berücksichtigt.

6.3 Hinweis- und Informationssystem der Versicherungswirtschaft

Das Hinweis- und Informationssystem (HIS) ist die zentrale Warndatei der Versicherungswirtschaft, in die Versicherungsunternehmen rund 9 Millionen Personen und Kfz eingetragen haben. Nach Auffassung der einmeldenden Versicherungsunternehmen haben sich bei den Betroffenen in der Risikoprüfung oder Leistungsbearbeitung erhöhte Risiken oder Auffälligkeiten gezeigt. Andere Versicherungsunternehmen nutzen diese Informationen ihrerseits bei der Risikoprüfung oder Leistungsbearbeitung. Die Datenschutzaufsichtsbehörden halten das HIS in der bisherigen Form für rechtswidrig (siehe Bericht 2007 unter Ziffer 7.3).

Die Datenschutzaufsichtsbehörden hatten 2007 mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. (GDV) vereinbart, dass das HIS bis Ende 2008 datenschutzgerecht umgestaltet wird. Nach der neuen Struktur soll das HIS wie eine Auskunftei betrieben werden, damit zukünftig nicht mehr allen Versicherungen alle Einträge auf Vorrat übermittelt werden. Vielmehr muss sichergestellt sein, dass Versicherungsunternehmen nur Daten erhalten, wenn sie ein berechtigtes Interesse an der Kenntnis der Daten haben.

Kurz vor Ablauf der vereinbarten Umsetzungsfrist teilte der GDV mit, dass sich die Neugestaltung des HIS als sehr komplex erwiesen habe, so dass ihm ein Umbau nicht vor Mitte 2011 (!) möglich sei. Meine Behörde war nicht bereit, eine solche Verzögerung folgenlos hinzunehmen. Sie forderte daher vom GDV und von den Versicherungsunternehmen in NRW Maßnahmen, um unverzüglich die datenschutzrechtliche Position der Betroffenen zu verbessern.

Meine Behörde hat zum einen erreicht, dass seit dem zweiten Quartal 2009 die Versicherungsunternehmen die Betroffenen über eine Einmeldung informieren. Dies ermöglicht den Betroffenen, ihre Rechte

wahrzunehmen und möglicherweise ungerechtfertigten Einmeldungen zu widersprechen. Zum anderen wurden die Hürden für eine Einmeldung in der Sparte Rechtsschutz höher gesetzt. Erst ab vier Versicherungsfällen in den letzten 12 Monaten kommt es nunmehr zu einer Einmeldung – bisher ab zwei Versicherungsfällen in 12 Monaten oder drei in 36 Monaten. Des Weiteren erteilt der GDV den Betroffenen Auskunft, ob – und wenn ja von welchem Versicherungsunternehmen – sie in das HIS eingemeldet wurden. In der Vergangenheit mussten sich die Betroffenen an jedes einzelne in Frage kommende Versicherungsunternehmen wenden.

Das HIS wird im Übrigen ab Mitte 2011 nicht mehr von der Versicherungswirtschaft selbst betrieben. Verantwortliche Stelle ist dann die informa Insurance Risk and Fraud Prevention GmbH mit Sitz in Baden-Baden.

➡ Ich werde auch zukünftig im Rahmen der bundesweiten Abstimmung der Aufsichtsbehörden darauf hinwirken, dass das neue HIS datenschutzgerecht ausgestaltet wird.

6.4 Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft

Wer seine Unterschrift unter das "Kleingedruckte" eines Versicherungsvertrags setzt, ist sich oft nicht bewusst, dass damit regelmäßig eine weitreichende Entbindung von der Schweigepflicht und eine umfassende datenschutzrechtliche Einwilligung erteilt werden. In einem "Rundumschlag" wird häufig die Versicherung ermächtigt, personenbezogene Daten – auch über den Gesundheitszustand der Antragstellerin oder des Antragstellers bzw. der Versicherungsnehmerin oder des Versicherungsnehmers – an andere Versicherungen, Rückversicherungen, oder mit der Versicherungsvermittlung oder mit Gutachten betraute Stellen weiterzugeben oder dort zu erheben. Gleichzeitig werden behandelnde Ärztinnen und Ärzte von der Schweigepflicht entbunden, so dass die Versicherungen bei ihnen weitere Informationen einholen können.

Die bisher von den Versicherungsunternehmen verwandten Einwilligungserklärungen wurden in ihren Grundzügen Mitte der 1990er

Jahre mit den Datenschutzaufsichtsbehörden abgestimmt. Nach einer zwischenzeitlichen Novellierung des Bundesdatenschutzgesetzes (BDSG) und einer intensiven Erörterung durch Datenschutzaufsichtsbehörden, Verbraucherschutzverbände sowie die Versicherungswirtschaft setzte sich allseits die Erkenntnis durch, dass es einer neuen Klausel bedarf.

Diese darf nach Auffassung der Datenschutzaufsichtsbehörden nicht mehr so weitreichend sein, sondern muss sich auf die Datenerhebungen und -verwendungen beschränken, die nicht auf gesetzliche Tatbestände gestützt werden können. Das gilt insbesondere für den Umgang mit Gesundheitsdaten, die nach dem BDSG besonders geschützt sind und für deren Verwendung grundsätzlich eine Einwilligung erforderlich ist. Das BDSG und das Versicherungsvertragsgesetz allein bieten insoweit keine ausreichende Rechtsgrundlage.

Bedauerlicherweise konnten sich die Versicherungswirtschaft und die Datenschutzaufsichtsbehörden in den vergangenen Jahren nicht auf neue Formulierungen verständigen.

Im Herbst 2009 hat eine Unterarbeitsgruppe unter dem Vorsitz meiner Behörde einen neuerlichen Anlauf unternommen, einen Mustertext zu entwickeln. Die Erklärung ist nunmehr mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. (GDV) weitgehend abgestimmt.

Die neue Musterklausel beschränkt sich auf Regelungen zum Erheben, Verarbeiten und Nutzen von Gesundheitsdaten, die etwa bei der Antragsprüfung oder im Leistungsfall erforderlich sind. Die Antrag stellenden Personen und Versicherungsnehmerinnen und -nehmer sollen besser als bisher überblicken können, was mit ihren Daten geschieht.

In einem weiteren Schritt will der GDV in Abstimmung mit den Aufsichtsbehörden verbindliche Verhaltensregeln (Code of Conduct) für die Datenerhebungen und -verwendungen formulieren, die von den gesetzlichen Tatbeständen gedeckt sind und daher keiner Einwilligung bedürfen. Die Selbstverpflichtung der Versicherungswirtschaft soll die allgemein formulierten Anforderungen der Datenschutzgesetze branchenspezifisch konkretisieren. Da dabei vielfältige Datenverarbeitungsprozesse zu berücksichtigen sind – etwa unternehmensübergreifende Datenbestände innerhalb von Unternehmensgruppen, der Datenaustausch mit Vor- und Rückversicherungen, das Ausgliedern gan-

zer Aufgabenbereiche auf andere Unternehmen, das Nutzen der Versichertendaten für Werbezwecke sowie Bonitätsabfragen bei Auskunfteien – gibt es zu den Verhaltensregeln einen entsprechend großen Erörterungsbedarf. Grundlage der bundesweiten Gespräche mit dem GDV ist eine Stellungnahme meiner Behörde, in der die Probleme aus der Aufsichtspraxis benannt werden, die durch die Verhaltensregeln zu lösen sind.

➡ Ich bin zuversichtlich, dass in den nächsten Monaten die Arbeiten an einer neuen Musterklausel für die Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft abgeschlossen werden. Auch in den anschließenden Verhandlungen zu den verbindlichen Verhaltensregeln der Versicherungswirtschaft werde ich aktiv auf einen datenschutzgerechten Umgang mit Versichertendaten hinwirken.

6.5 Falsche Datenschutzangebote am Telefon

Im Sommer 2010 habe ich zusammen mit anderen Datenschutz-Aufsichtsbehörden vor falschen Datenschutzangeboten gewarnt, nachdem vermehrt Hinweise eingegangen waren, wonach sich vermeintliche Datenschutzinstitutionen am Telefon auf eine Kooperation mit den Datenschutzaufsichtsbehörden, dem Verbraucherschutz oder der Bundesnetzagentur beriefen.

Die Anrufenden meldeten sich in amtlicher Funktion, etwa als Landesdatenschutzamt, oder als in Kooperation mit amtlichen Stellen stehend – teilweise mit dem Zusatz NRW – oder unter ähnlich lautenden Bezeichnungen bei Bürgerinnen und Bürgern und boten ihnen vermeintliche Datenschutzdienste an. Angepriesen wurde den Angerufenen, man wolle ihre im Umlauf befindlichen Daten, insbesondere ihre Bank- und Kontodaten, gegen eine Gebühr löschen oder aber die Gesprächspartnerinnen und -partner gegen einen jährlichen "Servicebetrag" vor Datenmissbrauch schützen. Hierzu ist festzustellen, dass generell ein wirksamer Schutz von einmal im Umlauf befindlichen Daten, vor allem bei einer Verbreitung über das Internet, praktisch kaum geleistet werden kann.

Ein Verbraucherdatenschutzinteressen im Firmennamen hervorhebendes Angebot warb mit seinem Service auch im Internet. Wahrheitswidrig wurde behauptet, unter anderem mit der Bundesnetzagentur zu kooperieren. Zudem verfügte die Firma offenbar in mehreren Fällen über die Bank- und Kontodaten der angerufenen Personen, wodurch diese verunsichert und zu einem Vertragsabschluss verleitet werden sollten. Die Nachforschungen haben ergeben, dass es sich bei dem angeblichen Firmensitz nur um eine Postadresse gehandelt hat. Tatsächlich befindet sich der Firmensitz in einem nicht der Europäischen Union angehörigen osteuropäischen Staat.

Ungeachtet des Umstands, dass sich Rechtshilfeersuchen der Strafverfolgungsbehörden an Nicht-EU-Staaten als durchweg schwierig erweisen, konnte im vorliegenden Fall als Erfolg verbucht werden, dass das Unternehmen ebenso wie auch andere vergleichbar in Erscheinung getretene Firmen ihre Aktivitäten und Geschäftsgebaren aufgrund der Warnhinweise der Datenschutzaufsichtsbehörden und Verbraucherschutzorganisationen eingestellt haben. Ob das "Geschäftsmodell" der Pseudodatenschutzangebote ausgelaufen ist, bleibt abzuwarten.

➡ Datenschutzaufsichtsbehörden, Verbraucherschutzorganisationen sowie die Bundesnetzagentur kooperieren nicht mit Diensten, die Daten von Bürgerinnen und Bürgern gegen Gebühr schützen wollen. Bei derartigen Angeboten ist Vorsicht geboten.

6.6 Untergeschobene Verträge am Telefon

Daten werden oft unberechtigt verwendet, um Betroffenen am Telefon vorzutäuschen, sie würden bereits seit längerem an Gewinnspielen teilnehmen. Solche Gespräche münden oft in ein Angebot zu einer Vertragsverlängerung oder enden mit der Erklärung, im Falle der Kündigung sei eine Gebühr zu entrichten.

Bei den Anrufen, die meist im großen Stil über Call-Center erfolgen, stehen rechtswidrig erlangte Bankkontodaten der Angerufenen im Fokus. Diese werden – etwa im Zusammenhang mit telefonischen Verkaufsanbahnungsgesprächen oder vermeintlichen Gewinnmitteilungen

– immer wieder zu unberechtigten Abbuchungen mittels Lastschrifteinzug bei Betroffenen genutzt.

Nach einer anderen, nicht minder betrügerischen Methode werden Betroffene am Telefon gezielt falsch informiert und zu einem Vertragsabschluss verleitet, oder aber ein Vertrag wird schlicht untergeschoben. Bei der inzwischen weit verbreiteten sogenannten Kündigungsmasche wird Betroffenen zum Beispiel erklärt, sie hätten bisher an einem – meist kostenlosen – Gewinnspiel teilgenommen. Solle der angebliche Vertrag nicht gebührenpflichtig weiterlaufen, bestehe nur die Möglichkeit einer Kündigung mit einer Frist von drei Monaten. Als "Gebühr" müssten dann drei Monatsbeiträge erhoben werden. Auf diese Weise erlangten betrügerische Anrufer im gesamten Bundesgebiet mehrere Millionen Euro. Betroffene wurden auf in diesen Fällen noch nicht abgeschlossene staatsanwaltschaftliche Ermittlungen hingewiesen.

Beweispflichtig auch für einen telefonisch abgeschlossenen Vertrag ist immer, wer diesen behauptet. Das Fehlen eines Vertrages kann auch einem eingeschalteten Inkassounternehmen entgegengehalten werden. Unabhängig hiervon können Betroffene Auskunftsansprüche unter anderem über die zu ihrer Person gespeicherten Daten und deren Herkunft geltend machen (§ 34 Bundesdatenschutzgesetz).

➡ Hier ist Vorsicht geboten. Wer sicher ist, dass kein Vertrag geschlossen wurde, sollte auch keine Zahlungen leisten oder einem unberechtigten Lastschrifteinzug widersprechen.

6.7 Bewertungsportale – Beurteilung in jeder Lebenslage

Die Bandbreite der Bewertungsportale im Internet hat in den letzten Jahren stark zugenommen. Die Bewertungsmöglichkeiten beschränkten sich früher vor allem auf Produkte, um die Kaufentscheidung anderer potentieller Käuferinnen und Käufer zu erleichtern. In letzter Zeit erstrecken sie sich jedoch auch auf Personen.

Zunächst bewegten sich die personenbezogenen Bewertungen in beruflichen Bereichen. So wurden beispielsweise Lehrerinnen und Lehrer, Handwerkerinnen und Handwerker sowie Ärztinnen und Ärzte bewer-

tet. Der Bundesgerichtshof hat im Fall des Bewertungsportals für Lehrerinnen und Lehrer "spickmich.de" entschieden, dass die Meinungsfreiheit das Persönlichkeitsrecht der Bewerteten überwiegt, sofern sich die Bewertungen auf die konkrete Berufsausübung beziehen. Da die berufliche Tätigkeit in der sogenannten Sozialsphäre erfolge, sei das Persönlichkeitsrecht der einzelnen Person bereits dadurch beschränkt, dass sie ihre Persönlichkeit innerhalb der sozialen Gemeinschaft entfalte. Jedoch hat das Gericht auch klargestellt, dass dem Persönlichkeitsrecht Vorrang einzuräumen ist, sobald die Äußerungen zu einer Stigmatisierung, sozialen Ausgrenzung oder Prangerwirkung führen können.

Im Rahmen der Aufsichtspraxis musste ich eine besorgniserregende Entwicklung feststellen. Es wurden nicht mehr nur Personen in Ausübung ihrer beruflichen Tätigkeit bewertet, sondern mittels eines "Single-Bewertungsportals" auch innerhalb ihres Privat- und Intimlebens. Singles konnten mit dessen Hilfe ihre "Internet-Flirtpartner" bewerten, die sie im realen Leben getroffen hatten.

Bewertet werden konnten unter anderem das Erscheinungsbild, das Auftreten, das Kommunikationsverhalten und die "Kusstechnik" der Flirtpartnerin oder des Flirtpartners. Darüber hinaus konnte angeklickt werden, ob es zum Geschlechtsverkehr gekommen war. Zusätzlich gab es ein moderiertes Freitextfeld, in dem die bewertende Person eintragen konnte, was ihr wichtig erschien. Diese Funktion bot die Gefahr, dass Kommentare mit beleidigendem Charakter oder gar intime Details veröffentlicht wurden.

Entgegen den gesetzlichen Erfordernissen wurde weder die Einwilligung der Bewerteten eingeholt noch ist eine nachträgliche Benachrichtigung erfolgt. Daher kannte die betroffene Person die Bewertung regelmäßig überhaupt nicht.

Die Bewertungen bedeuteten einen erheblichen Eingriff in die Intim- und Privatsphäre der Betroffenen, weil Werturteile hinsichtlich des Erscheinungsbildes, des Kommunikations- und Sexualverhaltens geäußert wurden. Ferner bestand durch den Umstand, dass das erteilte "Date-Zeugnis" weltweit im Internet eingesehen werden konnte, für Betroffene die Gefahr der sozialen Ausgrenzung und der Prangerwirkung. Dadurch wurde derart tief in die Rechte der Betroffenen einge-

griffen, dass die Äußerungen offensichtlich nicht durch die Meinungsfreiheit gerechtfertigt werden konnten.

Nach der Kontaktaufnahme mit dem Unternehmen, das die Seite anbot, wurde das Bewertungsportal für mehrere Monate eingestellt. Seit kurzem ist es allerdings in abgewandelter Form wieder verfügbar. Sollte hier eine datenschutzgerechte Umsetzung nicht erfolgen, werde ich die notwendigen mir nach dem Gesetz möglichen Maßnahmen ergreifen.

Positiv davon hebt sich ein Portal ab, bei dem Patientinnen und Patienten unter einem Pseudonym Bewertungen über ihre behandelnden Ärztinnen und Ärzte abgeben können. Hierbei wird das Persönlichkeitsrecht der betroffenen Ärztinnen und Ärzte in höherem Maße als bei anderen Bewertungsportalen geschützt und zwar insbesondere durch

- objektivierbare und sachliche Bewertungskriterien, die weniger auf die persönlichen Eigenschaften der Ärztin oder des Arztes als auf generelle Aussagen über die Praxis abzielen,
- die Möglichkeit der Ärztinnen und Ärzte, Bewertungen zu kommentieren oder sich von der Bewertung ausnehmen zu lassen,
- den Ausschluss von Mehrfachbewertungen und den Verzicht auf Freitextfelder.

Dennoch bestehen auch hier Risiken, die zu einer Beeinträchtigung der Rechte der beteiligten Personen führen können. Beispielsweise ist nicht gewährleistet, dass die eine Bewertung abgebende Person tatsächlich bei der betroffenen Ärztin oder dem betroffenen Arzt in Behandlung gewesen ist. So ist auch nicht auszuschließen, dass Ärztinnen oder Ärzte selbst oder deren Beschäftigte oder Angehörige die Bewertung abgeben.

➡ Insgesamt halte ich die neuere Entwicklung der Bewertungsportale für bedenklich. Häufig werden der Schutz der einzelnen Person und die Gewährleistung ihres Rechts auf informationelle Selbstbestimmung nicht ausreichend berücksichtigt. Es ist daher dringend geboten, dass Stellen, die Bewertungsportale betreiben, ihren diesbezüglichen Verpflichtungen besser nach-

kommen und die datenschutzrechtlichen Vorschriften strikt einhalten.

6.8 Informationspflichten bei Datenpannen

Als Reaktion auf eine Vielzahl von Datenschutzskandalen in der jüngeren Vergangenheit wurde eine Informationspflicht bei Datenpannen in das Bundesdatenschutzgesetz (BDSG) aufgenommen. Nach dem Gesetz muss ein Unternehmen sowohl die Betroffenen als auch die zuständige Aufsichtsbehörde für den Datenschutz informieren, wenn sich bei ihm bestimmte, als besonders kritisch eingestufte Datenverluste ereignen. Die Informationspflicht besteht unabhängig davon, ob das Unternehmen den Datenverlust verschuldet hat.

Die bisher eingegangenen Meldungen über Datenpannen lassen erkennen, dass in konkreten Fällen noch eine große Unsicherheit bei den Unternehmen besteht, ob sie der Informationspflicht gemäß § 42a BDSG nachkommen müssen. Das Gesetz eröffnet hier einige Interpretationsspielräume, zu denen ich den anfragenden Unternehmen Hilfestellungen gegeben habe.

Beispielsweise sieht das Gesetz eine Meldepflicht nur in den Fällen vor, in denen schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Diese Einschränkung im Gesetzestext ist insofern überraschend, als die Datenkategorien, die eine Meldepflicht auslösen, ohnehin besonders schützenswert sind. Meldepflichtig sind Verluste personenbezogener Daten der folgenden Kategorien:

- Besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG, wie etwa Gesundheitsdaten, Daten über eine politische oder religiöse Überzeugung oder über das Sexualleben,
- Daten, die einem Berufsgeheimnis unterliegen,
- Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen,
- Bank- und Kreditkartendaten.

Sofern personenbezogene Daten dieser genannten Kategorien unrechtmäßig an Dritte gelangen, ist eine schwerwiegende Beeinträchtigung der Betroffeneninteressen eigentlich der Regelfall. Unternehmen sollten bei einem solchen Datenverlust also grundsätzlich davon ausgehen, dass sie meldepflichtig sind. Praktisch müsste das Unternehmen besondere Gründe nennen können, warum im Einzelfall keine schwerwiegende Beeinträchtigung der Betroffeneninteressen vorliegt, wenn es die Information gemäß § 42a BDSG unterlässt.

Von den bisher gemeldeten Fällen stellen Diebstahl bzw. der Verlust von Hardware (PC, Laptop, Netbook, USB-Stick, externe Festplatte) einen signifikant hohen Anteil dar. Hier stehen die Unternehmen regelmäßig vor der Frage, ob schon der Verlust der Hardware bedeutet, dass eine dritte Stelle oder Person unrechtmäßig Kenntnis von den Daten erlangt hat, denn nur in diesem Fall entsteht die Pflicht zur Information nach § 42a BDSG. In aller Regel wissen die Unternehmen aber nicht, ob von Dritten auf die Daten zugegriffen wurde, wenn etwa ein Firmen-Laptop oder ein USB-Stick von einer Mitarbeiterin oder einem Mitarbeiter im Taxi liegen gelassen und nicht wieder aufgefunden wurde. Die Unternehmen können einen unberechtigten Zugriff jedenfalls dann nicht ausschließen, wenn die Daten nicht hinreichend verschlüsselt auf den Medien gespeichert waren. Bei Verlusten unverschlüsselter Daten, kann dem Gefahren abwehrenden Ziel des § 42a BDSG nur durch eine Information der Betroffenen in diesen Fällen angemessen Rechnung getragen werden.

Manche Unternehmen meldeten die Datenpannen vorsorglich zunächst nur meiner Behörde, informierten die Personen aber nicht, deren Daten verloren gingen. Dort wo Zweifel daran bestehen, ob überhaupt eine Informationspflicht nach § 42a BDSG entstanden ist, ist das grundsätzlich sachgerecht. Ist aber die Informationspflicht nach § 42a BDSG eindeutig, muss zeitgleich zur Meldung bei meiner Behörde eine Information der von dem Datenverlust betroffenen Personen erfolgen. Nur so kann die Gefahrenprävention in Missbrauchsfällen effektiv sein. Nur wenn eine Sicherung der Daten oder eine Strafverfolgung durch die zeitnahe Information der Betroffenen gefährdet wäre, ist eine Zeitverzögerung akzeptabel. Es sind also etwa Lücken in einem Firmensystem zunächst technisch zu schließen, bevor der Verlust von Daten über diese Lücke publik gemacht wird.

➡ Zu der neuen Regelung über Informationspflichten bei Datenverlusten hat meine Behörde Unternehmen ausführlich beraten. Auf meiner Homepage stehen außerdem weitere Informationen dazu zur Verfügung

7 Beschäftigtendatenschutz

7.1 Gesetzliche Regelungen zum Beschäftigtendatenschutz in Sicht

Die Konferenz der Datenschutzbeauftragten fordert seit vielen Jahren gesetzliche Regelungen zum Beschäftigtendatenschutz. Nunmehr liegt ein Gesetzentwurf der Bundesregierung (vom 3. September 2010, BR-Drs. 535/10) vor. Neben begrüßenswerten Regelungen enthält der Gesetzentwurf allerdings noch verschiedene nachbesserungsbedürftige Vorschriften.

Aufgrund der in der letzten Zeit festgestellten rechtswidrigen Beschäftigtenüberwachungen in großen Unternehmen forderten die Datenschutzbeauftragten im Frühjahr 2009, unverzüglich entsprechende gesetzgeberische Schritte zu ergreifen (siehe unter anderem Bericht 2009 unter Ziffer 12.1; Entschließungen vom 26./27. März 2009 und 22. Juni 2010, Abdruck im Anhang). In einem ersten Schritt wurde das Bundesdatenschutzgesetz (BDSG) um den § 32 ergänzt, der als allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten die Grundsätze der Rechtsprechung zum Datenschutz im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Beschäftigtendatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll. Diese zum 1. September 2009 mit der BDSG-Novelle II in Kraft getretene Vorschrift birgt dennoch zahlreiche Zweifelsfragen (etwa hinsichtlich der Voraussetzungen für einen Datenabgleich bei Straftatverdacht) und ist als unvollkommene Regelung zu kritisieren. Der Ruf nach präziser gefassten Gesetzesvorschriften ist daher berechtigt.

Der vorliegende Gesetzentwurf der Bundesregierung vom 3. September 2010 wurde in einer Arbeitsgruppe verschiedener Aufsichtsbehörden sowie von Datenschutzbeauftragten des Bundes und der Länder eingehend beraten. Den zuständigen Ressorts der Landesregierung habe ich meine Stellungnahme zu dem Gesetzentwurf für die Beratung im Bundesrat zugeleitet. Während einige Regelungen (unter anderem zur Datenverarbeitung bei Ortungssystemen und zu biometrischen Verfahren) grundsätzlich zu begrüßen sind, begegnen besonders folgende Punkte datenschutzrechtlichen Bedenken:

- **Aufdeckung von potentiellen Straftaten oder anderen schweren Pflichtverletzungen**

Mit dieser Neuregelung soll eine zweckändernde Nutzung von Beschäftigtendaten zur Aufdeckung von potentiellen Straftaten oder anderen schweren Pflichtverletzungen (unter anderem zu Zwecken von Korruptionsbekämpfung und "Compliance") zugelassen werden.

Im Entwurf sind Datenabgleiche zum Zwecke der Korruptionsbekämpfung und der Durchsetzung von Compliance–Anforderungen vorgesehen, die auch in personalisierbarer Form erfolgen können. Soweit hierbei an flächendeckende pauschale Verdachtsschöpfungsmaßnahmen gedacht ist, ist zu kritisieren, dass diese sich auf Beschäftigte allgemein erstrecken, obwohl kein konkreter Tatverdacht gegen einen Einzelnen oder eine Gruppe von Beschäftigten besteht. Die Betroffenen werden damit einem Generalverdacht ausgesetzt. Kritisch ist auch, dass die zugrunde liegende Datenverarbeitung für sie oft nicht mehr nachvollziehbar ist. Diese Regelung führt damit zwangsläufig zu gravierenden Beeinträchtigungen der Datenschutzrechte der Betroffenen. Gerade die multifunktionale Verwendbarkeit der automatisiert gespeicherten Beschäftigtendaten realisiert sich in der beabsichtigten Regelung als besonderes Risiko für das verfassungsrechtlich gewährleistete Recht auf informationelle Selbstbestimmung.

Abgesehen hiervon erscheint generell zweifelhaft, ob ein umfassendes Screening von Beschäftigtendaten überhaupt zur Zweckerreichung geeignet ist. Bisher haben die bekanntgewordenen Fälle, jedenfalls nach den meiner Behörde vorliegenden Erkenntnissen, keine relevanten Ergebnisse zutage gefördert. Schließlich dürfen nicht zuletzt mit Blick auf rechtsstaatliche Schutzvorkehrungen derartige Regelungen nicht dazu führen, dass Ermittlungen mit strafrechtlichem Hintergrund gleichsam in Regie eines Unternehmens geführt werden und die Grenzen zwischen dessen Eigenverantwortung und dem staatlichen Ermittlungsauftrag verwischt werden.

Zudem ist fraglich, ob und wie herkömmliche Revisionen unter diese Neuregelung subsumiert werden können, insbesondere wenn es sich um die Überprüfung möglicher fehlerhafter Geschäftsvorfälle (z.B. Doppelbuchungen, Rechnungsfehler) außerhalb der genannten Aufdeckungszwecke handelt. Es fehlen auch insofern klare, nach dem Verhältnismäßigkeitsgrundsatz gebotene Abgrenzungskriterien, wie diese

Datennutzungen zu erfolgen haben. Für Zwecke der Revision und herkömmliche Geschäftsprüfungen reichen zunächst stichprobenweise Überprüfungen und Prüfungsmaßnahmen in fehleranfälligen Bereichen aus.

- **Videoüberwachung**

Zu begrüßen ist, dass eine Videoüberwachung ohne Kenntnis der Beschäftigten nicht erfolgen darf. Weiterhin fehlt jedoch ein klarstellendes Verbot im Gesetzentwurf, Beschäftigte auf ihren Arbeitsplätzen ständig zu überwachen. Soweit von den zugelassenen Videoüberwachungsmaßnahmen Arbeitsplätze von Beschäftigten laufend erfasst würden, wäre eine solche dauerhafte verdachtsunabhängige Beobachtung nach der Rechtsprechung des Bundesarbeitsgerichts regelmäßig unverhältnismäßig. Darüber hinaus sollte im Gesetz klargestellt werden, dass die Videoüberwachung nicht zu Zwecken der Leistungs- und Verhaltenskontrolle erfolgen darf.

- **Monitoring – Mithören und Aufzeichnen von Telefongesprächen**

Bei Beschäftigten von Call-Centern sollen stichprobenartige oder anlassbezogene Leistungs- und Verhaltenskontrollen möglich sein. Mit Blick auf den Verhältnismäßigkeitsgrundsatz müssen derart eingriffsintensiven Maßnahmen enge Grenzen gesetzt werden. Wenigstens sollen die Beschäftigten vorab informiert werden. Zudem soll der Kontrollzeitraum eingegrenzt werden.

- **Beschwerderecht**

Die Vorschrift schreibt den Beschäftigten vor, sich bei tatsächlichen Anhaltspunkten für Datenschutzverstöße zunächst an den Arbeitgeber zu wenden. Damit schränkt sie das Beschwerde- und Anrufungsrecht der Beschäftigten gegenüber der Aufsichtsbehörde ohne triftigen Grund ein und verstößt auch gegen Art. 28 Abs. 4 der EU-Datenschutzrichtlinie, wonach jeder Person das uneingeschränkte Recht gewährt wird, sich zum Schutz der sie betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an die zuständige Kontrollstelle zu wenden. Überdies würde die Vorschrift die Aufgaben der Aufsichtsbehörden beeinträchtigen. Beschäftigte haben gegenüber der Aufsichtsbehörde häufig ein hohes Interesse daran, sich an sie zu wenden, ohne ihre Identität gegenüber dem Arbeitgeber preiszugeben.

Zusätzlich sollte festgelegt werden, dass keine Arbeitnehmerin und kein Arbeitnehmer dafür gemaßregelt oder benachteiligt werden darf, dass sie oder er sich an die Aufsichtsbehörde gewandt hat.

Neben diesen nachbesserungsbedürftigen Vorschriften sollte der Gesetzentwurf besonders in folgender Hinsicht überarbeitet werden:

Im Bewerbungs- und Einstellungsverfahren dürfen nur abgestufte Datenerhebungen erfolgen. Präzisierungsbedürftig ist die Erhebung von Daten aus sozialen Netzwerken. Gleiches gilt für die Behandlung unverlangt zugesandter Bewerbungen. Im Bewerbungsverfahren muss das Prinzip der direkten Datenerhebung bei den Bewerberinnen und Bewerbern gelten. Einwilligung en sind bei der Vertragsanbahnung ebenso wie im Arbeitsverhältnis grundsätzlich problematisch, weil sie von faktischem Zwang geprägt sind, der die Freiwilligkeit der Erklärung ausschließt.

➡ Ich werde mich aktiv in die weitere Diskussion über ein Beschäftigtendatenschutzgesetz einbringen.

7.2 ELENA (Elektronischer Entgeltnachweis)

Bereits im Bericht 2009 (dort unter Ziffer 10.1) wurden die verfassungsrechtlichen Bedenken gegen die mit dem ELENA-Verfahren verbundene Vorratsdatenspeicherung dargestellt. Trotz dieser Bedenken wurde mit dem Verfahren begonnen.

Am 28. März 2009 wurde das ELENA-Verfahrensgesetz verabschiedet. Seit Januar 2010 sind die Arbeitgeber zur Abgabe ihrer Meldungen an die Zentrale Speicherstelle verpflichtet. Nach dem derzeitigen Gesetzesstand können die Daten ab Januar 2012 dort von den Sozialleistungsträgern abgerufen werden. Dieser Abruftermin soll nach einer Absprache im Koalitionssauschuss der Bundesregierung von November 2010 auf Januar 2014 verschoben werden. Bis dahin sollen Abrufe zu Testzwecken möglich sein. Ein entsprechender Gesetzentwurf steht noch aus. Meine datenschutzrechtlichen Bedenken werden dadurch nicht ausgeräumt, sondern bestehen fort. Beim Bundesverfassungsgericht wurde im März 2010 Verfassungsbeschwerde erhoben, die von etwa 22.000 Personen unterstützt wird. Die Entscheidung des Bundesverfassungsgerichts bleibt abzuwarten.

➡ Aus meiner Sicht darf das ELENA-Verfahren in der bestehenden Form nicht weitergeführt werden.

7.3 Videoüberwachung in Discountunternehmen

Anlässlich der im Jahr 2008 bekanntgewordenen datenschutzwidrigen Überwachungen von Beschäftigten eines Lebensmittel-Discountunternehmens (siehe Bericht 2009 unter Ziffer 12.1) wurde in einer Arbeitsgruppe der Datenschutzaufsichtsbehörden beraten, welche Maßnahmen geeignet sind, ausufernden Videoüberwachungen von Beschäftigten wirksam zu begegnen. Um möglichst bundeseinheitliche Standards zu erreichen, haben die Aufsichtsbehörden vereinbart, sich gegenseitig über Videoüberwachungskonzepte – speziell von Discountern – zu informieren, die ihnen im Rahmen ihrer Kontrolltätigkeit bekannt werden.

Die Befugnis privater Stellen, mit Kenntnis der Betroffenen eine Videoüberwachung in öffentlich zugänglichen Räumen wie zum Beispiel in einem Supermarkt durchzuführen, ergibt sich aus § 6b Bundesdatenschutzgesetz. Danach muss eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein, und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Befinden sich in den öffentlich zugänglichen Räumen Arbeitsplätze von Beschäftigten und werden diese von den Videokameras ständig erfasst, verletzt dies regelmäßig deren schutzwürdige Interessen. Nach der arbeitsgerichtlichen Rechtsprechung erzeugt bereits die bloße Möglichkeit der jederzeitigen Videoüberwachung von Arbeitsplätzen einen mit dem Anspruch der Beschäftigten auf Wahrung ihrer Persönlichkeitsrechte (§ 75 Abs. 2 Betriebsverfassungsgesetz) regelmäßig nicht zu vereinbarenden Überwachungsdruck. Eine solche Überwachung kann nur ausnahmsweise gerechtfertigt sein, wenn im Rahmen einer Verhältnismäßigkeitsprüfung die Interessen des Arbeitgebers überwiegen (siehe Beschlüsse des Bundesarbeitsgerichts vom 29. Juni 2004 - 1 ABR 21/03 - und vom 26. August 2008 - 1 ABR 16/07 -).

Im Hinblick auf die gewonnenen Erfahrungen habe ich unter anderem ein großes Lebensmittel-Discountunternehmen, das in Nordrhein-Westfalen seinen Hauptsitz hat, bei der Erstellung einer umfangreichen Verfahrensanweisung für den Betrieb von Videoüberwachungsanlagen beraten.

Grundstruktur und wesentliches Element der Regelungen für die Videoüberwachung durch das Unternehmen, das eine Vielzahl von Filialen in West- und Süddeutschland betreibt, ist ein abgestuftes Einsatzkonzept für die Videoüberwachung. Darin ist festgelegt, ob – und wenn ja, unter welchen Voraussetzungen und in welchem Umfang – die Videoüberwachung in einer bestimmten Filiale eingesetzt werden soll. Dabei sind insbesondere filialbezogene Vorereignisse, wie z.B. das Überfallrisiko und das Inventurmanko, heranzuziehen.

Das Unternehmen verpflichtete sich, die Videoüberwachung nicht zum Zweck der Verhaltens- und Leistungskontrolle der Beschäftigten zu nutzen. Eine Überwachung mit verdeckten Kameras und eine Kameraüberwachung der Sozialräume und der Toiletten sind nicht erlaubt. Bei der Verwendung sogenannter Dome-Kameras, die wegen ihrer kuppelförmigen Bauweise eine Rundum-Beobachtung erlauben, soll auf Anraten meiner Behörde mit Klarglaskuppeln eine größere Transparenz hergestellt werden. Darüber hinaus werden in den Kassenbereichen Privatzonen mit Hilfe sogenannter Privacy-Filter-Technik eingerichtet, die eine weitgehende Ausblendung der mit den Kassiereraufgaben betrauten Beschäftigten ermöglicht. Ebenso wird sichergestellt, dass Kundinnen und Kunden während der Eingabe ihrer Geheimzahl (PIN) in die Zahlungsterminals nicht durch Videokameras erfasst werden.

Wie die auch auf Vorschlag meiner Behörde ergriffenen Maßnahmen zeigen, ist das Datenschutzbewusstsein in diesem Unternehmen erfreulich. Insbesondere die technischen Maßnahmen zur Ausblendung von Arbeitsplätzen können dazu beitragen, die Persönlichkeitsrechte der Beschäftigten angemessen zu berücksichtigen, ohne dass dabei die Interessen des Unternehmens vernachlässigt werden. Solche Datenschutzmaßnahmen sollten in Handel und Gewerbe Standard werden.

➡ Der mit der Umsetzung datenschutzfreundlicher Videoüberwachungskonzepte verbundene zusätzliche Aufwand wird verständlicherweise von Unternehmen nur

dann für vertretbar gehalten, wenn auch von Konkurrenzunternehmen vergleichbare Maßnahmen erwartet werden. Insofern lege ich bei meinen Beratungen Wert auf ein möglichst einheitlich geprägtes Einsatzkonzept für die Videoüberwachung in vergleichbaren Unternehmen.

7.4 Keine Bonität – Keine Beschäftigung?

Ein großer Textildiscounter hat über einen längeren Zeitraum systematisch Angaben über die persönlichen Vermögensverhältnisse seiner Beschäftigten erhoben, indem er Bonitätsauskünfte bei einer überregional tätigen Auskunftei eingeholt hat. Die von negativen Auskünften betroffenen Beschäftigten wurden im Kassenbereich und in Vertrauenspositionen nicht mehr eingesetzt.

Von Januar 2008 bis Anfang 2009 fragte das Unternehmen in mehr als 49.000 Fällen vierteljährlich die Vermögensverhältnisse seiner Beschäftigten bei einer Auskunftei ab. Die Beschäftigten waren über diese Abfragen lediglich informiert. Alle der Auskunftei über die betroffenen Personen vorliegenden Erkenntnisse wurden, sofern es sich um Einträge in öffentliche Schuldnerverzeichnisse, um Insolvenzverfahren sowie um laufende titulierte oder abgeschlossene Inkassoverfahren handelte, an das Unternehmen übermittelt und von diesem gespeichert. Es berief sich insoweit auf ein "berechtigtes Interesse" des Arbeitgebers. Aus den gleichen Gründen hielt auch die Auskunftei die Erteilung der Auskünfte für zulässig.

Arbeitgeber dürfen ihre Beschäftigten nicht in dieser Form durchleuchten. Da hier pauschal alle an den Kassen eingesetzten Beschäftigten auf finanzielle Zuverlässigkeit überprüft wurden, obwohl deren Tätigkeit auch durch adäquate Kassenprüfungsmaßnahmen hätte überwacht werden können, war die Einholung der Bonitätsauskünfte objektiv unverhältnismäßig. Ermittlungen der Staatsanwaltschaft führten zu dem Ergebnis, dass die erfolgten Datenabgleiche rechtswidrig, aber dem Arbeitgeber letztlich wegen einer in dieser Frage nicht ausreichend klaren Rechtslage nicht vorwerfbar waren.

Das Unternehmen hat mitgeteilt, solche Massenabfragen bei der Auskunftei nicht mehr vorzunehmen und die Zusammenarbeit mit dieser eingestellt zu haben.

- Bonitätsauskünfte über Beschäftigte dürfen nur bei besonderen Tätigkeiten mit erheblicher finanzieller Verantwortungsbreite (z.B. Bankkassiererinnen oder -kassierer, Finanzberaterinnen oder -berater) zum Zwecke der Begründung oder Durchführung eines Arbeitsverhältnisses eingeholt werden. Die Angaben über Vermögensverhältnisse sind dabei grundsätzlich bei den Betroffenen selbst zu erheben. Soweit der Arbeitgeber in besonders gelagerten Fällen noch Bonitätsauskünfte bei einer Auskunftei einholt, ist er zur Unterrichtung der betroffenen Bewerberinnen, Bewerber oder Beschäftigten verpflichtet. Eine pauschale Abfrage der Bonität aller Beschäftigten durch den Arbeitgeber ist jedenfalls unzulässig.

- Für Auskunfteien bedeutet das, dass diese Bonitätsauskünfte über Beschäftigte nur ausnahmsweise in den genannten Arbeitsbereichen mit finanzieller Verantwortungsbreite an einen Arbeitgeber übermitteln dürfen, sofern dieser die Beschäftigten vorher selbst über ihre Vermögensverhältnisse in zulässiger Weise befragt hat.

7.5 Überprüfung von Beschäftigtenkonten durch die Kreditinstitute

Haben Beschäftigte eines Kreditinstituts ein Konto bei diesem Institut, stellt sich die Frage, ob die Innenrevision Einsicht in diese Konten nehmen darf.

Die interne Revision einer Sparkasse prüfte im Rahmen ihrer Aufgaben, zu denen auch der Schutz des Vermögens einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen gehört, jährlich in ausgewählten Stichproben auch Umsätze auf Konten ihrer Beschäftigten. Hauptziel der Prüfung war insoweit in erster Linie die Ermittlung, ob die Beschäftigten die Regelungen einer internen Dienst-

anweisung zur Ordnung ihrer privaten wirtschaftlichen Verhältnisse und zur Konten- und Depotführung einhielten. Die Beschäftigten wurden von der internen Revision darüber informiert, dass ihre Konten Gegenstand des Prüfungsauftrages gewesen seien und sie die vorgenommenen Abfragen auf Anfrage einsehen könnten.

Die Beschäftigten waren hier aufgrund ihrer zweifachen vertraglichen Beziehung zur Sparkasse in die Überprüfungen einbezogen worden. Dabei hätten die Daten der Beschäftigten von der Sparkasse jedoch nur verarbeitet werden dürfen, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen erforderlich gewesen wäre und eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorgesehen hätte (siehe § 29 Abs. 1 Datenschutzgesetz Nordrhein-Westfalen). Hiernach konnte die interne Dienstanweisung die gezielte Untersuchung von Beschäftigtenkonten jedoch nicht rechtfertigen. Private Kreditinstitute unterliegen nach dem Bundesdatenschutzgesetz den selben Maßstäben.

➡ Kreditinstitute dürfen nicht die Privatkonten ihrer Beschäftigten für Revisionszwecke einsehen. Die Sparkasse konnte von der Unzulässigkeit ihres Vorgehens überzeugt werden und hat ihre Praxis eingestellt.

7.6 Ortung von Beschäftigten durch ihre Arbeitgeber

Der Einsatz von Ortungssystemen durch Arbeitgeber erweist sich oft wegen fehlender Transparenz für die Beschäftigten, ungewisser Dauer des Einsatzes der Geräte, überlanger Speicherung der Daten und unklar geregelter Nutzungszwecke als problematisch. Die beabsichtigten gesetzlichen Regelungen zum Beschäftigtendatenschutz können zu einem datenschutzkonformen Einsatz solcher in der Praxis weit verbreiteten Systeme führen.

Das Global Positioning System (GPS) ermöglicht eine satellitengestützte Positionsbestimmung. Sogenannte standortbezogene Dienste im Mobilfunk (Location Based Services) erlauben eine Orts- und Zeiterfassung eines Mobiltelefons anhand der Funkzelleninformationen des

Mobilfunkdienstanbieters. Diese beiden Ortungsmöglichkeiten können von Unternehmen zur Lokalisierung ihrer Beschäftigten und dabei auch zu Überwachungszwecken eingesetzt werden.

Durch die Satelliten- oder Mobilfunkortung wird erfasst, wo sich welches Firmenfahrzeug befindet. Da in der Regel im Unternehmen bekannt ist, wer mit dem jeweiligen Fahrzeug unterwegs ist, wird gleichzeitig der Aufenthaltsort der oder des jeweiligen Beschäftigten ermittelt. Gleiches gilt für die Ortung mitgeführter Firmenmobiltelefone. Begründet werden solche Maßnahmen oft mit der Notwendigkeit der Einsatzsteuerung, etwa in Speditionen oder gegenüber Beschäftigten im Außendienst, oder mit dem Ziel, das Firmenfahrzeug im Falle eines Diebstahls oder Unfalls auffinden zu können. Wie in einzelnen Fällen deutlich wurde, werden Ortungssysteme auch eingesetzt, um in der Vergangenheit liegende Arbeitsleistungen und -belastungen festzustellen, etwa um Zulagen für Außendiensttätigkeiten abzurechnen oder Pflegeleistungen durch Beschäftigte eines ambulanten Pflegedienstes nachzuweisen. Zuweilen liegt auch die Annahme nahe, dass Ortungssysteme eingesetzt werden, um das Arbeitsverhalten der Beschäftigten allgemein zu kontrollieren oder etwa Umwegfahrten zu ermitteln und zu sanktionieren.

Zu begrüßen ist, dass der Einsatz solcher Ortungssysteme nach dem Gesetzentwurf der Bundesregierung vom 3. September 2010 eigenständig geregelt werden soll. Danach soll es nur erlaubt sein, Beschäftigtendaten während der Arbeitszeit durch elektronische Einrichtungen zur Bestimmung eines geografischen Standortes (Ortungssysteme) zu erheben, zu verarbeiten und zu nutzen, soweit dies aus betrieblichen Gründen erforderlich ist

- zur Sicherheit der Beschäftigten oder
- zur Koordinierung des Einsatzes von Beschäftigten

und wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Beschäftigten am Ausschluss der Datenerhebung, -verarbeitung oder -nutzung überwiegen.

Der Gesetzentwurf stellt insbesondere klar, dass eine heimliche Ortung von Beschäftigten unzulässig ist, der Einsatz eines Ortungssystems für die Beschäftigten transparent zu machen ist, sie über die Nutzung der

Ortungsdaten zu informieren sind und die Zweckbindung der erhobenen Daten vorgeschrieben ist.

Die künftig vorgesehene Regelung stellt eine zu begrüßende Begrenzung des Einsatzes von Ortungssystemen in der Arbeitswelt dar, die einen angemessenen Schutz der Beschäftigten schafft und gleichzeitig betriebliche Belange ausgewogen berücksichtigt.

Bei der Ortung von Taxis durch Vermittlungszentralen, die nicht Arbeitgeber der Fahrerinnen und Fahrer sind, gelten zur Wahrung deren schutzwürdiger Interessen vergleichbare Standards:

- Die Ortung darf nur zum Zweck der Vermittlung von Fahrten und in Notfällen genutzt werden und nicht der Verhaltens- und Leistungskontrolle der Fahrer dienen.
- Die Ortung kann ausgeschaltet werden, beispielsweise in Pausen oder nach Dienstende. Taxis nehmen an der Vermittlung wieder teil, sobald das Gerät wieder eingeschaltet ist.
- Die Fahrerinnen und Fahrer werden darüber unterrichtet, dass eine GPS-Ortung stattfindet und wie sie diese unterbrechen können.
- Die gespeicherten GPS-Daten werden gelöscht, soweit sie nicht mehr benötigt werden.

➡ Ich empfehle Unternehmen, die Ortungstechnik einsetzen wollen, sich an diesen Maßstäben zu orientieren.

7.7 Fragerecht der Arbeitgeber in der Leiharbeitsbranche

Personalleasingfirmen weisen häufig darauf hin, dass sie hinsichtlich der von der arbeitsgerichtlichen Rechtsprechung entwickelten Grundsätze zum Fragerecht des Arbeitgebers anderen Maßstäben unterworfen seien als Unternehmen sonstiger Branchen.

Ein erweitertes Fragerecht soll sich nach Ansicht der Firmen zum einen aus der Tatsache ergeben, dass im Leiharbeitsbereich gerade der Frage nach der Flexibilität beim Arbeitseinsatz eine besondere Bedeutung zukomme. Darüber hinaus sei wegen der generellen Haftung des

Leiharbeitsunternehmens bei einem Auswahlverschulden eine gesteigerte Auswahlprüfung bei der Einstellung von Leiharbeitnehmerinnen und -nehmern durchzuführen.

Diese Auffassung wurde auch von einem bundesweit tätigen Leiharbeitsunternehmen mit Hauptsitz in Nordrhein-Westfalen vertreten. Konkret ging es dabei um einen Bewerbungsbogen, den das Unternehmen für die Suche nach geeigneten Arbeitskräften in dem sogenannten Helferbereich eingesetzt hatte. Dieser enthielt Fragestellungen, die gegen das Benachteiligungsverbot verstießen. Auch wurde ohne Rücksicht auf die Art des zu besetzenden Arbeitsplatzes pauschal die Frage nach Vorstrafen gestellt. Nach den Grundsätzen des Bundesarbeitsgerichts darf aber nur nach solchen Vorstrafen gefragt werden, die für den konkreten Arbeitsplatz von Bedeutung sind.

Das Leiharbeitsunternehmen stützte die erweiterte Fragepflicht auf die Regelung des § 12 Abs. 1 des Gesetzes zur Regelung der gewerbsmäßigen Arbeitnehmerüberlassung. Danach erfolgt der Einsatz der Beschäftigten durch ein Leiharbeitsunternehmen im Rahmen des zwischen diesem und der Entleiherfirma geschlossenen Vertrages, in dem unter Beschreibung des Arbeitsplatzes festgelegt wird, nach welchen Kriterien (wie Vor- und Ausbildung, berufliche Qualifikation) der Einsatz der jeweiligen Arbeitskraft bei dem entleihenden Unternehmen zu erfolgen hat.

Aus dieser Vorschrift kann jedoch lediglich die Verpflichtung des Leiharbeitsunternehmens abgeleitet werden, im Rahmen seiner Personalauswahl die Bewerbungsunterlagen der Kandidatin oder des Kandidaten sorgfältig mit den im Arbeitnehmerüberlassungsvertrag genannten Qualifikationserfordernissen abzugleichen. Eine Ausweitung des Fragerechts des Leiharbeitsunternehmens ist damit nicht verbunden.

Auch können für ein erweitertes Fragerecht des Leiharbeitsunternehmens nicht die Regelungen des Bundesdatenschutzgesetzes (BDSG) herangezogen werden. Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. § 3 Abs. 11 Nr. 7 BDSG zählt ausdrücklich auch Bewerberinnen und Bewerber zu den Beschäftigten. Danach dürfen im Bewerbungsverfahren nur die Fragen gestellt werden, die –

unter Beachtung der arbeitsgerichtlichen Maßstäbe zum Fragerecht des Arbeitgebers und der entsprechenden Benachteiligungsverbote – erforderlich sind, um die Eignung der Bewerberin oder des Bewerbers für die vorgesehene Tätigkeit festzustellen.

Das Leiharbeitsunternehmen ist meinen Empfehlungen zur datenschutzgerechten Ausgestaltung des Bewerbungsbogens gefolgt. Wegen der bundesweiten Tätigkeit des Unternehmens habe ich die Aufsichtsbehörden für den Datenschutz in den Bundesländern über meine Beurteilung unterrichtet.

- Leiharbeitsunternehmen sind hinsichtlich des Fragerechts des Arbeitgebers gegenüber Unternehmen anderer Branchen nicht privilegiert. Hierzu besteht auch keine Notwendigkeit, weil den Unternehmensinteressen einerseits und der schutzwürdigen Interessenlage der Betroffenen andererseits im Rahmen des geltenden Rechts ausreichend Rechnung getragen werden kann.

- Es ist wünschenswert, dass mit der Novellierung des Beschäftigtendatenschutzrechts auch insoweit klarstellende gesetzliche Regelungen getroffen werden.

7.8 Gesundheitsuntersuchungen bei Zurruhesetzungen

Bei Zurruhesetzungsverfahren im öffentlichen Dienst ist für den Dienstherrn die Gesundheitssituation der Betroffenen von besonderer Bedeutung. Ein Gesundheitsamt hatte es sich bei der Mitteilung der ärztlichen Erkenntnisse an die den Untersuchungsauftrag erteilenden Behörden zu einfach gemacht.

Soweit öffentliche Stellen Zurruhesetzungsverfahren durchführen, hat das mit der Durchführung der ärztlichen Untersuchung beauftragte Gesundheitsamt sich grundsätzlich auf die Mitteilung des Ergebnisses dieser Untersuchung an die personalverwaltende Stelle zu beschränken (§ 24 Abs. 3 Gesundheitsdatenschutzgesetz – GDSG NRW). Hierzu sieht die Verordnung über die amtliche Begutachtung der unteren Gesundheitsbehörde für den öffentlichen Dienst ein Musterformular vor, in dem die Grundlagen der Beurteilung, weitere Mitteilungen aus ärztlicher Sicht sowie die Empfehlungen zu dokumentieren sind.

Demgegenüber hatte ein Gesundheitsamt einer großen Kommune ein abweichendes Verfahren etabliert, indem es die Betroffenen eine Erklärung zur Entbindung von der ärztlichen Schweigepflicht unterzeichnen ließ und der Personal verwaltenden Stelle die vollständigen Gutachten übersandte. Der Empfehlung, dieses Verfahren einzustellen sowie Inhalt und Umfang der Datenübermittlungen anlässlich der Begutachtungen strikt an der Erlaubnisnorm des § 24 Abs. 3 GDSG NRW auszurichten, ist das Gesundheitsamt erst nach eingehenden Beratungen gefolgt. Es hat zwischenzeitlich mitgeteilt, die an die Behörden übersandten vollständigen Gutachten zurückgefordert und diese darauf hingewiesen zu haben, dass bei ihnen keine Kopien verbleiben dürften.

➡ In diesem Fall konnte meine Behörde erreichen, dass die Übermittlung von Gesundheitsdaten auf das erforderliche Maß beschränkt bleibt. Ich empfehle auch anderen Behörden, sorgfältig die Rechtmäßigkeit beim Umgang mit diesen sensiblen Daten zu prüfen.

8 Gesundheit

8.1 Elektronische Gesundheitskarte (eGK)

Die eGK soll nach vielen kontroversen politischen und fachlichen Diskussionen in der Vergangenheit nun zukünftig im Rahmen definierter Verfahren pilotiert werden.

Die eGK dient u.a. der Bereitstellung von personenbezogenen Daten der Versicherten bzw. der Patientinnen und Patienten, die bereits derzeit auf der Versichertenkarte gespeichert sind. Durch ein Foto auf der eGK soll zudem die Zurechenbarkeit der Karte zu einer Person erhöht werden. Neben dieser Grundfunktion soll die eGK auch weitere Offline- und/oder Online-Anwendungen unterstützen können. Auch wenn derzeit noch keine abschließende Liste mit Funktionsmerkmalen der neuen Karte existiert, sind folgende Anwendungen in der Diskussion:

- Hinterlegung von Notfalldaten,
- elektronische Rezepte und
- elektronische Patientenakte.

Als besonderes Leistungsmerkmal soll die eGK hinsichtlich der elektronischen Rezepte und der elektronischen Patientenakte die Patientenautonomie stärken. Basis hierfür bildet eine Verschlüsselung, die nur von der Person, die die Gesundheitskarte besitzt, unter Eingabe einer PIN aktiviert werden kann. Die Patientinnen und Patienten sollen vollumfänglich über den Umgang mit den eigenen Daten entscheiden. Die informationelle Selbstbestimmung soll in besonderer Weise garantiert werden.

Gelingt das auch?

Mit der Gesundheitskarte wird einerseits dem Sicherheitsprinzip von Besitz (Gesundheitskarte) und Wissen (Eingabe einer PIN) Rechnung getragen. Der auf der eGK befindliche geheime Schlüssel zur Entschlüsselung medizinischer Daten ist besonders gesichert. Damit er in einem Entschlüsselungsprozess frei geschaltet wird, muss die Patientin oder der Patient an einem Kartenleser – etwa in Praxen oder Apotheken – eine geheim zu haltende PIN eingeben.

Mit Hilfe von sogenannten Patiententerminals – etwa in Krankenhäusern oder Apotheken – soll die Patientin oder der Patient zukünftig grundsätzlich auch selbst Einblick in die über sie bzw. ihn gespeicherten medizinischen Daten – auf der eGK oder beispielsweise in einer elektronischen Patientenakte – nehmen. Patiententerminals sind technische Vorrichtungen – etwa Bildschirm, Tastatur –, die es den Patientinnen und Patienten ermöglichen, Zugriff auf medizinische Daten zu erhalten. Die Patiententerminals sollen es der Patientin oder dem Patienten auch ermöglichen, die Zugriffsrechte auf ihre bzw. seine etwaige elektronische Patientenakte – in Kombination mit der eGK – zu verwalten. Hierdurch hätten es Patientinnen und Patienten tatsächlich in der Hand, wer ihre Daten zur Kenntnis nehmen kann und wer nicht.

Insoweit erfüllt die eGK die Sicherheitsanforderungen. Um hier jedoch zu einer umfassenden Bewertung zu gelangen, ist folgende Frage zu stellen: Reicht diese auf die technische Bereitstellung der notwendigen Funktionen gerichtete Betrachtungsweise aus?

Der PIN-Mechanismus ist problematisch. Dies wird auch in einem von der Universität Bayreuth durchgeführten Evaluationsgutachten bestätigt:

"Als problematisch erwies sich zudem die PIN-Eingabe, insbesondere bei älteren und behinderten Patienten. Über 50 % der Ärzte berichteten, dass ihre Patienten oft Probleme mit der PIN-Eingabe hatten, 10 % der Ärzte antworteten sogar, dass dies immer der Fall war." (Universität Bayreuth, Institut für Medizinmanagement und Gesundheitswissenschaften, booz&co: Evaluationsbericht im Rahmen der Testregionen übergreifenden Evaluation der 10.000er Tests bei der Einführung der elektronischen Gesundheitskarte, Seite 7)

Zudem ist zu beachten, dass Menschen (unabhängig von ihrem individuellen Alter) krankheitsbedingt in eine Lage kommen können, in der sie mit dem PIN-Mechanismus plötzlich nicht mehr umgehen können.

Die Bedienung von Patiententerminals erscheint ebenfalls schwierig. Insbesondere die Verwaltung der Zugriffsberechtigungen einer elektronischen Patientenakte via Terminal dürfte Viele überfordern.

- ➡ Durch barrierefreie Lösungen ist sicherzustellen, dass das informationelle Selbstbestimmungsrecht auch faktisch gewährleistet ist.

8.2 Einrichtungsübergreifende elektronische Patientenakten (eEPA) – Grundlegende Anforderungen

Im Rahmen des Projekts "EPA.2015" der Landesregierung NRW, das sich mit arztgeführten eEPA beschäftigt, hat meine Behörde Anforderungen an datenschutzgerechte eEPA-Systeme aufgestellt.

Unternehmen fragen immer wieder, welche Datenschutzanforderungen bei der Entwicklung elektronischer Patientenakten zu berücksichtigen seien, die von verschiedenen medizinischen Einrichtungen verwendet werden sollen. Dabei sind im Wesentlichen drei Themenkomplexe von Bedeutung: Datensicherheit, materiell rechtliche Vorgaben und die Anforderungen aus Sicht der Anwender (siehe nachstehende Abbildung).

<table>
<tr><th colspan="2">Datensicherheit (duale Sicht)</th></tr>
<tr><td>Verlässlichkeit
-Sicherheit des Systems-</td><td>Beherrschbarkeit
-Sicherheit vor dem System-</td></tr>
<tr><td>• Vertraulichkeit
• Integrität
• Verfügbarkeit</td><td>• Zurechenbarkeit
• Nachvollziehbarkeit
• Verbindlichkeit</td></tr>
<tr><th colspan="2">materielles Recht</th></tr>
<tr><td colspan="2">▪ Zugriffsautorisierung (Einwilligung)
▪ inhaltliche u. zeitliche Zugriffsbeschränkung (Erforderlichkeit)
▪ Gewährleistung der Patientenrechte</td></tr>
<tr><th colspan="2">Anwenderanforderungen (Patientin/Patient, Ärztin/Arzt)</th></tr>
<tr><td colspan="2">o Praktikabilität (Nutzerfreundlichkeit, Barrierefreiheit)
o Alltagstauglichkeit (Integrierbarkeit in med. org. Abläufe)</td></tr>
</table>

- **Datensicherheit**

Maßnahmen technischer und organisatorischer Art zur Gewährleistung der Datensicherheit werden auf der Grundlage eines individuell zu erarbeitenden Sicherheitskonzepts ermittelt. Als methodische Vorgehensweise zur Erstellung eines Sicherheitskonzepts sowie zur Etablierung eines Sicherheitsprozesses bieten sich die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Standard 100-1 bis 100-4) an.

Bei der Sicherheitskonzeptionierung ist zu beachten, dass unter Datenschutzaspekten neben den klassischen Sicherheitskriterien der Vertraulichkeit, Integrität und Verfügbarkeit als weitere Kriterien die Zurechenbarkeit (Authentizität), die Nachvollziehbarkeit (Revisionsfähigkeit) und die Verbindlichkeit (Nicht-Abstreitbarkeit) als Aspekte der Systembeherrschbarkeit zu berücksichtigen sind.

Aufgrund der hohen Sensibilität patientenbezogener Daten ist die Gewährleistung der Vertraulichkeit von zentraler Bedeutung (§ 203 Strafgesetzbuch, § 3 Abs. 9 Bundesdatenschutzgesetz, § 9 ärztliche Berufsordnungen, § 97 Strafprozessordnung, BVerfGE 32, 373, 380). Technisch kann diesen Anforderungen nur die Ende-zu-Ende-Verschlüsselung (im Sinne von Arzt-zu-Arzt-Verschlüsselung) mit starken kryptografischen Verfahren gerecht werden.

Das Kriterium der Zurechenbarkeit soll eine eindeutige Zuordnung von Daten zu Personen sowie von Verarbeitungsprozessen zu deren Auslösern sicherstellen.

Die Nachvollziehbarkeit soll gewährleisten, dass im Nachhinein feststellbar ist, wer wann welche Daten einer eEPA in welcher Weise verarbeitet hat. Dadurch ist die gesamte Datenverarbeitung vollständig überprüfbar und transparent.

Die Verbindlichkeit stellt sicher, dass die Datenurheberschaft sowie die Verantwortlichkeit für einen Datenverarbeitungsprozess nicht abgestritten bzw. gegenüber einem Dritten nachgewiesen werden kann.

- **Materiell-rechtliche Anforderungen**

Für die im Projekt "EPA.2015" betrachtete Variante einer elektronischen Patientenakte gibt es keine spezialgesetzliche Regelung. Daraus resultiert, dass ein lesender oder schreibender Zugriff auf eine eEPA

nur zulässig ist, wenn die Patientin oder der Patient jeweils eingewilligt hat (§ 4 Abs. 1 BDSG). Da eine schriftliche Einwilligung in der jeweiligen Behandlungssituation in der Regel nicht angemessen ist, muss ein adäquater Autorisierungsmechanismus gefunden werden. Ein solcher Mechanismus ist so zu gestalten, dass durch ihn die Patientin bzw. der Patient ihre bzw. seine freie Entscheidung zum Ausdruck bringen kann. Dabei ist sicherzustellen, dass ein eEPA-Zugriff nur erfolgen kann, wenn die Patientin oder der Patient diesen Mechanismus "auslöst". Denkbar wäre eine technische Zugriffskontrolle, die einen Zugriff nur zulässt, wenn beispielsweise eine TAN (im Besitz und/oder Wissen der Patientin oder des Patienten) vorgelegt wird.

Auch bei Vorliegen einer Einwilligung dürfen die Informationen einer eEPA grundsätzlich nur im Rahmen des für die Behandlung erforderlichen Umfangs und nur bis zum Abschluss der Behandlung genutzt werden (Erforderlichkeitsprinzip). Diese Anforderung ist in der technischen Umsetzung schwierig, weil letztlich nur die behandelnde Ärztin oder der Arzt entscheiden kann, welche Informationen zur Behandlung benötigt werden und wann die Behandlung abgeschlossen ist. Daraus ist nicht zu schließen, dass ein grundsätzlicher (zeitlich unbeschränkter) Vollzugriff ermöglicht werden kann. Die Erforderlichkeit muss sich vielmehr nach den Besonderheiten der jeweiligen Behandlungssituation richten.

- **Was ist zu tun?**

Eine Lösung zur Umsetzung des Erforderlichkeitsprinzips hängt unmittelbar mit den Anforderungen an eine rechtswirksame Einwilligung zusammen. Eine Einwilligung, die sich pauschal und ohne zeitliche Beschränkung auf die Nutzung des gesamten Akteninhalts bezöge, wäre unzulässig, weil die betroffene Person nicht in der Lage wäre, die Auswirkungen einer solchen Einwilligung auf die Datenverarbeitung zu überschauen. Eine technische Lösung erfordert demnach ein differenziertes Berechtigungskonzept sowie einen Autorisierungsmechanismus mit Verfallszeitpunkt. Außerdem sollte auf einen strukturierten Akteninhalt Wert gelegt werden. Beispielsweise können Informationen, die bei jeder ärztlichen Behandlung benötigt werden (wie Medikamentenliste, Allergien, Unverträglichkeiten, Vorerkrankungen und so weiter) in einem Teilbereich der Akte als Basisdokumentation hinterlegt werden. Eine nach medizinisch-fachlichen Kriterien strukturierte Akte erleichtert die Einrichtung von Berechtigungen.

Ein eEPA-System muss so konzipiert sein, dass die Wahrnehmung der Rechte der Patientinnen und Patienten (Betroffenen) gewährleistet ist. Grundsätzlich obliegt der für die Datenverarbeitung verantwortlichen Stelle, die Betroffenenrechte umzusetzen. In Bezug auf eine eEPA stellt sich aber die Frage, welche Stelle verantwortlich im Sinne des Datenschutzrechts ist. Eine eEPA wird gespeist aus den Informationen der Primärsysteme (Praxisverwaltungssystem, Krankenhausinformationssystem). In Bezug auf diese Systeme sind die jeweiligen Ärztinnen und Ärzte bzw. medizinischen Einrichtungen verantwortliche Stellen. Von den Patientinnen und Patienten kann nicht verlangt werden, dass sie ihre Rechte jeweils punktuell gegenüber einzelnen Ärztinnen und Ärzten oder verschiedenen medizinischen Einrichtungen artikulieren. Zudem muss eine eEPA als eine (neue) Datensammlung behandelt werden, die in ihrer Gesamtheit wie ein Mosaik zu betrachten ist, das zwar aus vielen Steinchen unterschiedlicher Herkunft besteht, aber als Ganzes erst das Bild ergibt. Deshalb muss es für eine eEPA eine verantwortliche Stelle zur Wahrnehmung der Rechte der Betroffenen geben. Diese Stelle könnte eine Ärztin oder eine Arzt sein und von der betroffenen Person bestimmt werden ("Aktenmoderatorin oder -moderator"). Im Rahmen der Aktenmoderation könnten die Rechte der Patientinnen und Patienten verwirklicht oder ggf. erforderliche Schritte eingeleitet werden, wenn die Beteiligung der einstellenden Ärztin oder des Arztes nicht möglich ist.

Insbesondere bei den Rechten der Betroffenen auf Löschung, Berichtigung und Sperrung ihrer Daten wird das Spannungsverhältnis zwischen der informationellen Selbstbestimmung und dem Interesse an einer auf vollständiger Sachgrundlage beruhenden ärztlichen Versorgung offenkundig. Je nachdem, wie die vorgenannten Rechte ausgeübt werden, kann in der eEPA ein unzutreffendes Bild über den Gesundheitszustand mit erheblichen Risiken für die Patientin bzw. den Patienten entstehen. In diesen Fällen erscheint eine verantwortliche ärztliche Beratung durch die "Aktenmoderation" von besonderer Bedeutung.

- **Anforderungen an die Anwendungsfreundlichkeit**

Die Systeme sind für die Patientinnen und Patienten praktikabel und barrierefrei zu gestalten. Hierzu gehört insbesondere der Autorisierungsmechanismus, über den die Einwilligung realisiert wird. Das informationelle Selbstbestimmungsrecht ist nur dann gewährleistet,

wenn dieser Mechanismus uneingeschränkt genutzt werden kann, also beispielweise auch von älteren und behinderten Personen.

Eine elektronische Patientenakte ist so zu konzipieren, dass sie alltagstauglich ist und damit die medizinischen und organisatorischen Abläufe und Gegebenheiten in den medizinischen Einrichtungen adäquat unterstützt. Um diese Ziele zu erreichen, sollte am Anfang eine detaillierte Anforderungs- und Systemanalyse durchgeführt werden, damit die relevanten Anwendungsfälle ermittelt werden können. Beispielhaft seien an dieser Stelle einige Alltagssituationen angeführt, mit denen das heutige Gesundheitssystem umgehen kann und die auch mit Einführung eines eEPA-Systems technisch ermöglicht werden sollten:

- Befunde, Arztbriefe u.ä. werden oft erst erstellt, wenn die Patientin oder der Patient die medizinische Einrichtung schon verlassen hat. Das Einstellen dieser Dokumente in eine eEPA sollte auch dann noch möglich sein.
- Es besteht nicht immer ein physischer Kontakt zwischen Ärztin oder Arzt einerseits und Patientin oder Patient andererseits (z.B. bei einer telefonischen Beratung oder bei der Vor- und Nachbereitung eines Hausbesuchs). Wenn die Ärztin oder der Arzt einen eEPA-Zugriff benötigt, sollte auch für solche Situationen eine Autorisierung möglich sein.
- Patientinnen und Patienten sind nicht immer selbst in einer medizinischen Einrichtung anwesend, sondern werden manchmal von einer Person ihres Vertrauens vertreten. Dieser Person sollte es möglich sein, eEPA-Zugriffe stellvertretend zu autorisieren.
- In Notfällen können sich unvorhergesehene Vertretungssituationen ergeben. Es sollte also eine flexible Lösung (z.B. durch gerade erreichbare Familienangehörige) realisierbar sein.
- In Situationen, in denen die Patientin oder der Patient nicht mitwirkungsfähig ist, die Ärztin oder der Arzt aber eine mutmaßliche Einwilligung unterstellen kann, sollte ein eEPA-Zugriff ebenfalls ermöglicht werden.
- In Krankenhäusern sollte die Autorisierung für eine Gruppe von Ärztinnen und Ärzten möglich sein, nämlich bezogen auf

die Ärztinnen und Ärzte einer Station bzw. Abteilung, die die Patientin oder den Patienten behandeln.

Ein alltagstaugliches System unterstützt technisch das, was rechtlich zulässig und unter fachlichen Aspekten erforderlich ist, und es unterbindet technisch, was nicht zulässig ist.

➡ Die Herausforderung bei der Entwicklung von eEPA-Systemen liegt darin, ausgehend von der informationellen Selbstbestimmung praktikable Lösungen für den Umgang mit sensitiven Gesundheitsdaten in derartigen Systemen zu erzielen. Der für solche Systeme zu fordernde hohe Datensicherheitsstandard steht praxistauglichen Lösungen nicht im Wege.

8.3 KV-SafeNet – Ein sicheres Datennetz für Ärzte?

Etliche Ärztinnen und Ärzte sind an mich herangetreten, da sie befürchten, dass die Daten ihrer Patientinnen und Patienten nicht mehr ausreichend geschützt seien, wenn sie ihre Praxisrechner an das Datennetz KV-SafeNet der Kassenärztlichen Vereinigungen anschließen. Es besteht die Sorge, dass es Schwachstellen in der Konfiguration des KV-SafeNet-Routers gibt und Provider unbemerkt auf das Praxisnetz zugreifen können.

- **Was ist KV-SafeNet?**

KV-SafeNet ist ein Netz für die ärztliche Kommunikation. Es vernetzt Praxissysteme mit den Kassenärztlichen Vereinigungen und ermöglicht ebenso den Datenaustausch mit anderen Praxen und medizinischen Einrichtungen.

- **Wie funktioniert KV-SafeNet?**

Durch den speziell konfigurierten KV-SafeNet-Router wird ein vom Internet getrenntes virtuelles privates Netz (VPN) zwischen Praxis und dem Rechenzentrum der jeweiligen Kassenärztlichen Vereinigung und damit auch zum schnellen Netz (KV-Backbone) aufgebaut, das die Kassenärztlichen Vereinigungen untereinander verbindet. Gleichzeitig blockiert der Router den Zugriff von außen auf die Praxisrechner und die Daten im Praxisnetz. Der KV-SafeNet-Router wird nur von speziell

hierfür von der Kassenärztlichen Bundesvereinigung (KBV) zertifizierten Providern angeboten. Hierdurch soll sichergestellt werden, dass ein hoher Sicherheitsstandard eingehalten wird.

- **Wo liegt das Problem?**

Nach einem Hinweis war ein KV-SafeNet-Router von dem Provider nicht so konfiguriert (offene interne Ports), wie es nach dem hohen Sicherheitsstandard erforderlich ist. Dadurch ergaben sich zumindest theoretisch Angriffspunkte. Darüber hinaus wurde bemängelt, dass die Administration und Wartung des Routers durch die jeweiligen Provider ohne Kenntnis und Möglichkeit zur Einflussnahme durch die Ärztinnen und Ärzte erfolgte. Außerdem war auf einem Router von der Herstellerfirma ein Netzwerkanalysetool vorinstalliert, das prinzipiell geeignet war, den Netzverkehr mitzuschneiden.

- **Was will die KBV zur Lösung des Problems tun?**
  - Zukünftig werden die Ärztinnen und Ärzte den Zeitpunkt für einen Wartungszugriff bestimmen können und außerdem auf Verlangen von den Providern über die Inhalte aller Administrationsarbeiten informiert werden.
  - Nicht benötigte Ports der Router werden geschlossen.
  - Das Verfahren zur Providerzertifizierung wird überarbeitet und die Prüfkriterien werden erweitert.

- **Wie ist KV-SafeNet datenschutzrechtlich zu beurteilen?**

Grundsätzlich ist eine Lösung auf der Grundlage des KV-SafeNet-Routers zu begrüßen, da eine hardwarebasierte Lösung die sicherste Alternative zum Aufbau virtueller privater Netzwerke darstellt. Die potentielle Schwachstelle dieses Konzepts liegt allerdings in seiner technischen und organisatorischen Umsetzung, da die Bereitstellung und Administration der KV-SafeNet-Router privaten Providern überlassen wird. Diese werden zwar von der Kassenärztlichen Bundesvereinigung auf der Grundlage der Rahmenrichtlinie KV-SafeNet zertifiziert. Da sie jedoch den alleinigen Zugriff auf die Router haben, besteht eine nicht zu vernachlässigende Gefährdung durch Missbrauch. Beispielsweise wäre es einem Provider möglich, ein bereits herstellerseitig auf dem Router vorinstalliertes Netzwerk-Analysetool für Mitschnitte des Netzverkehrs zu missbrauchen oder auch verbotenerweise selbst ein sol-

ches Tool für diese Zwecke zu installieren. Wegen des hohen Schutzbedarfs der in Praxisnetzen verarbeiteten Daten sind auch solche Szenarien in eine Risikobetrachtung einzubeziehen.

- **Forderungen aus Sicht des Datenschutzes**

Um die Missbrauchgefahr seitens der Provider einzuschränken, muss eine Lösung entwickelt werden, die sicherstellt, dass

1. jegliche Administrations- und Wartungsaktivitäten durch die Provider revisionssicher protokolliert werden und
2. ein Zugriff auf einen KV-SafeNet-Router nur erfolgen kann, wenn die Ärztin oder der Arzt diesen durch eine aktive Handlung über einen technischen Mechanismus frei schaltet.

➡ Die KV-SafeNet-Lösung hat grundsätzlich das Potential zur Realisierung eines sicheren Netzes für den ärztlichen Datenaustausch. Aufgrund des hohen Schutzbedarfs patientenbezogener Daten ist allerdings noch Nachbesserungsbedarf erkennbar. Welche technischen und organisatorischen Maßnahmen hierzu konkret erforderlich sind, muss auf Grundlage einer von der KBV zu erstellenden detaillierten und umfassenden Risiko- und Bedrohungsanalyse ermittelt werden.

8.4 Hausarztverträge

Bundesweit werden bzw. wurden bereits Verträge zur hausarztzentrierten Versorgung zwischen den gesetzlichen Krankenkassen und den Hausärzteverbänden geschlossen, auf deren Grundlage die Hausärzteverbände als private Anbieter u.a. die Abrechnung der kassenärztlichen Honorare vornehmen sollen. In NRW wurde sowohl von einer Krankenkasse als auch von einer Kassenärztlichen Vereinigung auf datenschutzrechtliche Probleme in den Vertragswerken aufmerksam gemacht und um datenschutzrechtliche Prüfung gebeten.

Nach dem Sozialgesetzbuch – Fünftes Buch – (SGB V) haben die gesetzlichen Krankenkassen ihren Versicherten eine besondere hausärztliche Versorgung anzubieten (hausarztzentrierte Versorgung). Kernanliegen dieser Versorgung ist die Stärkung der Hausärztinnen

und -ärzte in ihrer Funktion als zentrale Ansprechperson für ihre Patientinnen und Patienten. Vertragsparteien sind zum einen die gesetzlichen Krankenkassen und zum anderen die Hausärzteverbände. Während bisher nur die kassenärztlichen Vereinigungen als öffentliche Stellen die Kassenarzthonorare abrechnen durften, ist nun die Einbindung privater Abrechnungsdienstleistungsunternehmen wegen einer Neuregelung in § 295 Abs. 1 b SGB V möglich. Dieser erlaubt erstmals explizit, dass private Stellen mit der Verarbeitung und Nutzung der für die Abrechnung erforderlichen personenbezogenen Daten beauftragt werden dürfen. Entscheidend ist, dass diese Datennutzung nur im Wege der Auftragsdatenverarbeitung im Sinne des Sozialgesetzbuches – Zehntes Buch – (SGB X) möglich ist. Für eine Auftragsdatenverarbeitung müssen bestimmte Voraussetzungen erfüllt sein. Insbesondere muss der Auftraggeber – hier: die Hausärztin oder der Hausarzt – zu jedem Zeitpunkt über den wesentlichen Umgang mit den Daten bestimmen können, während der Auftragnehmer – hier: der Hausärzteverband – lediglich Hilfsfunktionen übernimmt. Die mir vorgelegten Verträge erfüllen die Anforderungen der Auftragsdatenverarbeitung nicht. Die einzelnen Hausärztinnen und -ärzte haben weder Kenntnis darüber, welche Daten wie genau verarbeitet werden, noch haben sie die Möglichkeit, konkrete Weisungen bezüglich der Datenverarbeitung zu erteilen. Des Weiteren verpflichten sie sich dazu, etwaige Honorarforderungen zur Führung von Musterprozessen abzutreten, was den Grundsätzen einer Datenverarbeitung im Auftrag ebenfalls widerspricht. Im Januar 2011 hat das Oberverwaltungsgericht Schleswig-Holstein (OVG) eine Verfügung der dortigen Aufsichtsbehörde zu einem vergleichbaren Vertrag im einstweiligen Rechtsschutzverfahren bestätigt. Nach Ansicht des OVG liegen gravierende Verstöße gegen datenschutzrechtliche Vorgaben zum Schutz von Patientendaten vor. Durch die Entscheidung des OVG wurde letztlich auch meine Rechtsauffassung bestätigt.

➡ Die vorgelegten Verträge zur hausarztzentrierten Versorgung unter Beteiligung privater Dienstleistungsunternehmen widersprechen den gesetzlichen Anforderungen an die Auftragsdatenverarbeitung.

8.5 Mammographie-Screening

Während für die Datenübermittlung der Meldebehörden an die Zentralen Stellen in NRW für Zwecke des Mammographie-Screenings eigens eine rechtliche Grundlage in Form einer Verordnung (Verordnung über die Zulassung der regelmäßigen Datenübermittlung von Meldebehörden an die Zentralen Stellen bei den Kassenärztlichen Vereinigungen) geschaffen wurde, mangelt es bei der Weitergabe der persönlichen Daten der betroffenen Frauen von der Zentralen Stelle an die Screening-Einheiten an der erforderlichen Rechtsgrundlage.

Im Rahmen des Angebots des Mammographie-Screenings übermitteln die Meldebehörden den bei den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe angesiedelten sogenannten Zentralen Stellen die Daten (u.a. Name, Geburtsdatum, Anschrift) der 50- bis 70-jährigen Frauen. Die Zentralen Stellen versenden dann die mit einem konkreten Untersuchungstermin versehenen Einladungen an die Frauen. Bereits zu diesem Zeitpunkt übermitteln die Zentralen Stellen die persönlichen Daten der Frauen an die sogenannten Screening-Einheiten, d.h. die jeweiligen die Untersuchung durchführenden Stellen.

Die Vorgehensweise der Zentralen Stellen basiert auf der Krebsfrüherkennungs-Richtlinie, diese stellt allerdings keine Rechtsgrundlage dar, wie sie für eine Datenübermittlung notwendig wäre.

Das Verfahren kann datenschutzkonform so umgestaltet werden, dass analog zur Datenübermittlung von den Melderegistern an die Zentralen Stellen auch für die weitere Übermittlung an die Screening-Einheiten eine rechtliche Grundlage erlassen wird. Alternativ wäre es auch datenschutzkonform und pragmatisch, die Einladungsschreiben derart umzugestalten, dass diese zunächst als Informationsschreiben dienen. Es sollte den betroffenen Frauen, die an einem – freiwilligen – Screening interessiert sind, die Möglichkeit gegeben werden, eigeninitiativ und selbstbestimmend aus der Auswahl der verschiedenen Screening-Einheiten direkt mit einer von diesen einen Termin zu vereinbaren. Dies würde zudem dem Recht auf freie Wahl der Ärztin oder des Arztes entsprechen.

➡ In diesem Sinne habe ich die Angelegenheit gegenüber dem zuständigen Ministerium aufgegriffen.

9 Sport

Erhebung und Verarbeitung von Daten durch die Nationale Anti-Doping-Agentur (NADA)

In Deutschland vollzieht die meiner Aufsicht unterliegende NADA, eine vom Bund finanzierte private Stiftung mit Sitz in Bonn, die internationalen Vorgaben zu Dopingkontrollen auf nationaler Ebene. Die ordnungsgemäße Durchführung der Kontrollen ist Voraussetzung für die Startberechtigung der deutschen Leistungssportlerinnen und -sportler in internationalen Wettbewerben. In diesem Zusammenhang sind auch Datenschutzfragen zu klären.

Die Bundesrepublik Deutschland hat sich international zur Verfolgung des Dopings im Sport verpflichtet. Das Thema Dopingbekämpfung im Sport wird von unterschiedlichen Organisationen auf internationaler und nationaler Ebene verfolgt. Die Welt-Anti-Doping-Agentur (WADA) mit Sitz in Montreal legt weltweit den Rahmen für Maßnahmen gegen Doping im Leistungssport auf der Grundlage des Welt-Anti-Doping-Codes fest.

Zur Durchführung der Dopingkontrollen erhebt die NADA in großem Umfang personenbezogene Daten. Betroffen können in diesem Zusammenhang – neben den Sportlerinnen und Sportlern – auch Dritte sein. Denn bei den Aufenthaltsdaten der Athletinnen und Athleten, die erfasst werden, um die Durchführung unangekündigter Kontrollen zu ermöglichen, werden auch Daten dritter Personen erhoben, bei denen sich die Athletinnen und Athleten aufhalten. Darüber hinaus erhebt und verarbeitet die NADA Gesundheitsdaten der Sportlerinnen und Sportler. Hierbei handelt es sich um die bei Kontrollen erhobenen Werte sowie um Angaben zu eingenommenen Medikamenten, um über medizinische Ausnahmegenehmigungen entscheiden zu können.

Nach dem Bundesdatenschutzgesetz (BDSG) dürfen schutzwürdige Interessen der Betroffenen der Datenverarbeitung nicht entgegenstehen, was nicht nur in Bezug auf Dritte Probleme bereitet. Es geht neben den Aufenthaltsdaten schließlich auch um Gesundheitsdaten. Auch soweit von einer Einwilligung der Athletinnen und Athleten ausgegangen wird, ist zu berücksichtigen, dass diese nicht für Drittbetroffene

gelten kann. Ebenso steht nicht zweifelsfrei fest, ob die für eine Einwilligung geforderte Freiwilligkeit immer gegeben ist.

Mit der NADA besteht Übereinstimmung, dass – unabhängig davon, ob und inwieweit auf eine Rechtsgrundlage oder Einwilligung zurückgegriffen werden kann – eine Datenverarbeitung nur im Rahmen des Erforderlichen stattfinden darf. Insoweit müssen Erforderlichkeit und Angemessenheit jedes einzelnen Datums, das im Einzelnen erhoben wird, dezidiert hinterfragt werden. Möglichkeiten, die Datenverarbeitung auf ein unumgängliches Maß zu beschränken, sind zu erkennen und auszuschöpfen. Dies erfordert zum einen, auf internationaler Ebene zu einer datenschutzgerechteren Ausgestaltung des weltweit geltenden WADA-Codes zu gelangen. Hierbei kann ich den Bund nur darin unterstützen, seine in diese Richtung gehenden Aktivitäten fortzuführen. Zum anderen gilt es weiterhin, auf nationaler Ebene Spielräume für datenschutzfreundlichere Lösungen zu nutzen.

Ich setze die bereits seit längerem geführten Gespräche mit der NADA fort, um gemeinsam mit dieser auf einen datenschutzkonformen Umgang mit den personenbezogenen Daten der Sportlerinnen und Sportler hinzuwirken.

- Der Datenschutz im System der Bekämpfung des Dopings im Sport muss auch weiterhin fortentwickelt und ausgebaut werden. Insbesondere auf internationaler Ebene gilt es, das Anliegen weiter zu verfolgen, dem europäischen Verständnis von Datenschutz Eingang in den internationalen Bereich zu verschaffen.

10 Zensus 2011

Zur Durchführung der registergestützten Volkszählung auf der Grundlage des Zensusgesetzes 2011 sind ergänzende Regelungen im Ausführungsgesetz des Landes Nordrhein-Westfalen getroffen worden.

Die datenschutzrechtlichen Anforderungen für die Durchführung des für 2011 in der Europäischen Union vorgesehenen Zensus wurden im Datenschutz- und Informationsfreiheitsbericht 2009 im Hinblick auf den damaligen Gesetzgebungsstand aufgezeigt (siehe Bericht 2009 unter Ziffer 15.1). Das anschließend verabschiedete Gesetz über den registergestützten Zensus im Jahre 2011 (BGBl. 2009 I S. 1781) legt nunmehr die Erhebungsgrundlagen fest. Die Bevölkerungs-, Gebäude- und Wohnungszählung zum Berichtszeitpunkt (9. Mai 2011) wird im Wesentlichen durch Datenerhebungen aus Registern durchgeführt, deren Aktualisierung bis zu diesem Stichtag erwartet wird.

Durch die Nutzung dieser Informationsquellen können unmittelbare Haushaltsbefragungen, die bisher auf der Grundlage des Mikrozensusgesetzes durchgeführt worden sind, jedoch nicht vollständig ersetzt werden. Die statistischen Ämter der Länder werden zum Berichtszeitpunkt vielmehr ergänzende, aus statistikfachlichen Gründen erforderliche Haushaltsbefragungen auf Stichprobenbasis (Haushaltsstichprobe) durchführen. Der Stichprobenumfang soll 10 Prozent der Bevölkerung nicht überschreiten.

Die Zusammenführung auch sensibler persönlicher Daten aus zahlreichen Verwaltungsregistern soll auf der Grundlage der Datenerhebungsregelungen des Zensusgesetzes 2011 erfolgen. Sie ist nicht von der Einwilligung der Betroffenen abhängig. Soweit die Daten damit Zweck ändernd für den Zensus 2011 genutzt werden, beruht auch dies auf dem gesetzgeberischen Willen, die ursprünglich für einen anderen Zweck erhobenen und gespeicherten Daten für einen registergestützten Zensus zu verwenden. Aus Sicht des Datenschutzes kann eine solche gesetzliche Zweckänderung jedoch nur hingenommen werden, sofern ein Datenrücklauf aus dem Bereich der amtlichen Statistik in den Verwaltungsvollzug nicht erfolgt, die Löschungsverpflichtungen eingehalten werden, das Statistikgeheimnis beachtet wird und die Datensicherheit gewahrt bleibt. Dahingehende Regelungen sind im Zensusgesetz 2011 sowie im Bundesstatistikgesetz vorgesehen.

Mit dem Ausführungsgesetz des Landes Nordrhein-Westfalen zum Zensusgesetz 2011 sind zur Durchführung des registergestützten Zensus ergänzende Bestimmungen, insbesondere zur Einrichtung der örtlichen Erhebungsstellen und ihrer Trennung von anderen Verwaltungsstellen, erlassen worden.

- Bei der Durchführung der registergestützten Volkszählung wird besonders zu beachten sein, dass die statistikdatenschutzrechtlichen Standards, insbesondere der Grundsatz der Abschottung der amtlichen Statistik von Aufgaben des Verwaltungsvollzugs, bei Einrichtung und Betrieb der örtlichen Erhebungsstellen gewahrt bleiben. Die dort eingesetzten Beschäftigten dürfen während ihrer Tätigkeit nicht mit Aufgaben des Verwaltungsvollzugs betraut werden.

11 Wissenschaft und Schule

11.1 E-Learning in Hochschulen – Modernes Lernen zwischen Chance und Risiko

Wer – wenn nicht die Hochschule – sollte Vorreiterin bei der Entwicklung und Etablierung neuer Lehr- und Lernmethoden sein? Folgerichtig haben in den letzten Jahren verschiedenste Systeme und Verfahren des E-Learnings Einzug in die Hochschulen gehalten. Das eröffnet neue, schnellere und einfachere Möglichkeiten des Lehrens und des Lernens, des Austauschs von Materialien und Meinungen, leider aber auch diverse Datenschutzrisiken.

- Studentin Anja ist begeistert: Neuerdings kann sie die Materialien zur Vorbereitung des Seminars von Dozent X unproblematisch über das Internet abrufen. Was sie nicht weiß: X kann nachverfolgen, ob und wann sie von diesem Angebot Gebrauch gemacht hat. Wie begeistert er davon ist, dass sie – wie er aus seinen Stichproben folgert – die Vorbereitung immer häufiger vernachlässigt, sei dahingestellt.
- Benno, der gerade seinen "Master" in der Tasche hat und sich auf Jobsuche begibt, ist empört: Seine politischen Meinungsäußerungen, die er vor fünf Jahren in einem Diskussionsforum, das für die Lehre genutzt wurde, abgegeben hat und inzwischen für Jugendsünden hält, sind immer noch via Internet abrufbar. Wie seine Recherche ergibt, sind keine Löschungsfristen vorgesehen, und es fühlt sich auch niemand verantwortlich.
- Cindy, frisch immatrikuliert, ist verunsichert: Muss sie sich an einem Online-Seminar beteiligen und dabei – wie es die Dozentin Y erwartet – vorab ihr Foto und weitere persönliche Angaben über sich einstellen?

Dies sind nur wenige Beispiele für unzählige Datenschutzfragen rund um das E-Learning im Hochschulbereich. Da ich angesichts der 60 Hochschulen in NRW, die meiner Kontrolle unterliegen, nicht jeder Einzelanfrage zu dieser Thematik nachgehen und nicht jedes E-Learning-System gesondert überprüfen kann, habe ich das Informationspapier "E-Learning an Hochschulen nach den Grundsätzen des Datenschut-

zes" erstellt und mit einer Arbeitsgruppe von interessierten Hochschuldatenschutzbeauftragten abgestimmt. Es ist nunmehr über meine Homepage www.ldi.nrw.de abrufbar und soll dazu beitragen, den Verantwortlichen in den Hochschulen grundlegende Datenschutzhinweise an die Hand zu geben sowie die Kolleginnen und Kollegen vor Ort bei ihrer Arbeit zu unterstützen.

Dem Vernehmen nach werden die Leitungen wie auch die Datenschutzbeauftragten der Hochschulen oftmals gar nicht, nicht rechtzeitig oder nicht umfassend über Planungen, E-Learning-Systeme einzusetzen, unterrichtet. Das muss sich ändern, damit die Datenschutzbeauftragten die erforderlichen Vorabkontrollen durchführen und die Leitungen insgesamt ihrer Verantwortung für den datenschutzgerechten und sicheren Einsatz von E-Learning Rechnung tragen können.

➧ Die unbestrittenen Chancen des E-Learnings können ungetrübt genutzt werden, wenn die Hochschule zugleich flankierende Maßnahmen trifft, um den datenschutzrechtlichen Risiken wirksam vorzubeugen. Verantwortlich hierfür sind die Hochschulleitungen.

11.2 Prüfungsakten – Anspruch auf Auskunft und Kopien

"Einsicht ist der erste Schritt zur Besserung" – und nur wer seine Fehler erkennt, kann daraus lernen. Dies gilt auch für Prüfungsklausuren im Hochschulbereich. Schränkt eine Hochschule das Recht der Studierenden auf Einsichtnahme in ihre Prüfungsakten jedoch soweit ein, dass es letztlich nur noch "auf dem Papier" existiert, ist dies nicht nur prüfungsrechtlich bedenklich, sondern verletzt auch die Datenschutzrechte der Studierenden.

Insbesondere in den Bachelorstudiengängen ist innerhalb eines straffen Zeitplans eine Vielzahl schriftlicher Prüfungsleistungen zu erbringen. Dies stellt nicht nur für die Studierenden, sondern auch für die Hochschulen eine Herausforderung dar, da sie für einen ordnungsgemäßen Prüfungsablauf und die rechtzeitige Korrektur der Prüfungsarbeiten Sorge zu tragen haben. Der für die Hochschulen hiermit verbundene logistische Aufwand ist sicherlich nicht zu unterschätzen,

doch darf dies nicht zu einer Verkürzung der elementaren Datenschutzrechte der Studierenden führen.

Studierende können gemäß § 18 Abs. 1 und 2 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) in Verbindung mit § 8 Abs. 5 Hochschulgesetz des Landes Einsicht in ihre korrigierten Prüfungsarbeiten verlangen. Nach Maßgabe dieser Vorschriften hat die betroffene Person grundsätzlich einen Anspruch auf Einsichtnahme in alle Unterlagen, in denen ihre personenbezogenen Daten gespeichert sind. Auskunft und Einsichtnahme sind gebührenfrei. Das Recht zur Einsichtnahme umfasst auch das Recht zur Ausfertigung bzw. Aushändigung von Kopien, wobei die Kopierkosten als Auslagen zu erstatten sind. Das Einsichtnahmerecht kann durch abweichende Bestimmungen in den einschlägigen Hochschulprüfungsordnungen nicht wirksam ausgeschlossen oder beschränkt werden.

Meine Behörde wurde zum Beispiel auf die Verfahrensweise einer Universität aufmerksam gemacht, deren Prüfungsordnung die Anfertigung von Notizen bei der Einsichtnahme zwar gestattet, Abschriften und Kopien jedoch ausdrücklich verbietet. Zugleich lässt die Universität eine Nachkorrektur nur unter der Voraussetzung zu, dass der Prüfling zuvor in die Prüfungsarbeit Einsicht genommen und sodann unverzüglich eine erneute Bewertungsüberprüfung unter konkreter Benennung etwaiger Bewertungsfehler schriftlich beantragt hat. Die Dauer der Einsichtnahme wird pauschal auf 20 Minuten beschränkt. Auch das zwischenzeitliche Vorhaben der Universität, den Studierenden Kopien ihrer Arbeiten erst auszuhändigen, wenn Klausurbesprechungen mit den jeweiligen Prüferinnen und Prüfern ohne Erfolg verlaufen sind, genügt den datenschutzrechtlichen Anforderungen nicht.

Unter den genannten Umständen wird es den Studierenden unverhältnismäßig erschwert, ihr gesetzlich verankertes Einsichtnahmerecht wahrzunehmen, um so die Bewertung einer sachlich und zeitlich angemessenen Überprüfung unterziehen und Einwände gegen die Bewertung erheben zu können.

Ich habe der Universität daher empfohlen, die einschlägige Prüfungsordnung zu ändern und den Studierenden auf Antrag Kopien ihrer Prüfungsarbeiten zur Verfügung zu stellen.

➡ Studierende haben einen Anspruch auf Einsichtnahme in ihre Prüfungsarbeiten gemäß § 18 Abs. 1 und 2 DSG NRW, der auch die Möglichkeit zum Erhalt von Kopien als besondere Form der Einsichtnahme umfasst.

11.3 Datenverarbeitung durch Schule und Schulträger

In der Schulpraxis scheinen Irrungen und Wirrungen darüber, wer Herr der Schülerdaten ist und die Verantwortung für diese trägt sowie ob, wann und auf welcher Rechtsgrundlage Schülerdaten von der Schule an den Schulträger übermittelt werden dürfen, eher die Regel als die Ausnahme zu sein. Eingaben und Anfragen geben immer wieder Anlass, Licht ins Dunkel zu bringen.

Einige fiktive, aber realistische Beispiele: Die Stadt X fordert die Schulen in ihrer Trägerschaft auf, ihr unverzüglich alle Schülerdaten zu übermitteln, weil diese mittels einer neuen Software zentral durch den Schulträger verarbeitet werden sollen. Die Schulen in Y übermitteln dem Schulträger auf dessen Bitte personenbeziehbare Schülerdaten zur Schulentwicklungsplanung. Schule Z leitet rein vorsorglich bei jedem Schulwechsel Daten an ihren Träger weiter.

Das Schulgesetz NRW (SchulG) weist den Schulen und den Schulträgern zwei verschiedene Aufgabenbereiche zu: Während erstere für die inneren Schulangelegenheiten – insbesondere die Bildung und Erziehung der Schülerinnen und Schüler – zuständig sind, umfasst die Zuständigkeit der letzteren die äußeren Schulangelegenheiten, also z.B. die Bereitstellung und Unterhaltung der Schulanlagen, Gebäude, Einrichtungen und Lehrmittel. Schule und Schulträger sind – wie in § 2 Abs. 2 Satz 3 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) klargestellt wird – datenschutzrechtlich zwei verschiedene Stellen. Herr der Daten in inneren Schulangelegenheiten und damit auch verantwortlich für die Einhaltung der Datenschutzvorschriften ist die Leiterin oder der Leiter der Schule, nicht ihr Träger. In § 120 SchulG und der Verordnung über die zur Verarbeitung zugelassenen Daten von

Schülerinnen, Schülern und Eltern (VO-DV I) finden sich detaillierte Vorschriften zur Verarbeitung von Schülerdaten in und durch Schulen. Sollen von einer Schule personenbezogene Daten an den Schulträger übermittelt werden, bedarf dies einer Rechtsgrundlage. Da der Schulträger in der Regel zu seiner Aufgabenerfüllung keine personenbezogenen Schülerdaten benötigt, ist eine solche Übermittlung nur in Ausnahmefällen zulässig.

An diese Überlegungen anknüpfend lassen sich Lösungen für die beispielhaft aufgeführten Problemfelder finden:

- In X ist keine Rechtsgrundlage für die Übermittlung der Schülerdaten von den Schulen an den Schulträger zu dessen Aufgabenerfüllung ersichtlich. Herr der Daten sind die jeweiligen Schulleiterinnen und -leiter. Diese haben nach § 1 Abs. 3 VO-DV I für die Schule sicherzustellen, dass der Schutz der verarbeiteten Daten gemäß § 10 DSG NRW gewährleistet ist und die Löschungsbestimmungen eingehalten werden; sie sind insgesamt für die Wahrung des Datenschutzes verantwortlich. Der Schulträger hat hierfür nach Maßgabe des SchulG eine am allgemeinen Stand der Technik und Informationstechnologie orientierte Sachausstattung zur Verfügung zu stellen.

  Möglich wäre es indes, dass die Schulen den Schulträger gemäß §§ 2 Abs. 3 VO-DV I, 11 DSG NRW mit der Datenverarbeitung für sie beauftragen, weil es sinnvoll und sicherer sein kann, dessen Infrastruktur zu nutzen. Der Schulträger darf die Daten in diesem Fall nur im Rahmen der Weisungen der Schulen und nur für die Zwecke der jeweiligen Schulen verarbeiten; die Schulleitungen bleiben weiterhin verantwortlich. Das setzt unter anderem eine schriftliche Auftragserteilung mit den erforderlichen Weisungen voraus. In X wäre es also nicht zu beanstanden, wenn der Schulträger eine Datenverarbeitung im Auftrag lediglich anbietet bzw. vorschlägt und die Schulen ihn entsprechend beauftragen und anweisen. Nicht die Träger, sondern die Schulleitungen treffen die Entscheidung und tragen die Verantwortung für die Daten. Selbstverständlich muss dabei ferner allen anderen Anforderungen des Datenschutzes und der Datensicherheit Rechnung getragen werden.

- In Y steht demgegenüber keine Auftragsdatenverarbeitung, sondern tatsächlich eine Datenübermittlung in Rede. Nach § 120 Abs. 5 Satz 1 SchulG darf die Schule dem Schulträger Schülerdaten übermitteln, soweit dies zu seiner Aufgabenerfüllung erforderlich ist. Dem Schulträger ist zwar dahingehend zuzustimmen, dass zu seinen Aufgaben auch die Schulentwicklungsplanung gehört, aber benötigt er zu diesem Zweck personenbeziehbare Schülerdaten? Nach den bisherigen Erkenntnissen ist dies nicht der Fall. Die Schulen in Y dürfen deshalb regelmäßig nur anonymisierte Daten an ihren Träger zum Zweck der Schulentwicklungsplanung weitergeben.
- Die Schule Z steht vor einem Problem, das sich gleichsam allen Schulen in NRW stellen dürfte: Den Schulträgern ist die Aufgabe der Schulpflichtüberwachung nicht zugewiesen, also dürfte eine Datenübermittlung zum Zweck der Erfüllung dieser Aufgabe bereits aus diesem Grund nicht in Betracht kommen. Gleichwohl sieht der Runderlass "Überwachung der Schulpflicht" des Ministeriums für Schule und Weiterbildung NRW – als solcher ohnehin keine Rechtsgrundlage für eine Verarbeitung personenbezogener Daten – eine Datenübermittlung an die Kommune in verschiedenen Fällen noch immer vor, während in der höherrangigen VO-DV I bereits entsprechende Anpassungen vorgenommen wurden. Wenn die abgebenden und aufnehmenden Schulen jeweils ihrer Pflicht nachkommen, die Einhaltung der Schulpflicht bei einem Schulwechsel zu überwachen, entstehen jedenfalls bis zum Abschluss der Sekundarstufe I keine Kontrolllücken. Der Empfehlung, den Erlass aufzuheben oder zu überarbeiten, ist gleichwohl bislang nicht entsprochen worden.

  ➡ Schulen und Schulträger müssen gemeinsam darauf achten, dass sie personenbezogene Schülerdaten nur im Rahmen ihrer jeweiligen Zuständigkeit verarbeiten und dabei die Grenzen des rechtlich Zulässigen nicht überschreiten. Nur so können zugleich unzulässige Datensammlungen auf Vorrat und sogenannte "Datenfriedhöfe" vermieden werden.

11.4 Datenverarbeitung durch externe Unternehmen

Schulen können sich vor Angeboten externer Stellen, Daten für sie zu verarbeiten, kaum retten: Die einen bieten etwa an, E-Mail-Postfächer einzurichten, die zugleich der schulischen Kommunikation dienen sollen, andere wollen gleich die gesamte Datenverarbeitung übernehmen. Aber dürfen sich Schulen zur Datenverarbeitung Dritter bedienen, und wenn ja: Unter welchen Voraussetzungen kann dies geschehen?

Rückmeldungen aus der Praxis zeigen, dass eine solche "Auslagerung" der Datenverarbeitung oftmals erfolgt, ohne dass überhaupt Überlegungen zu den Anforderungen des Datenschutzes und der Datensicherheit angestellt werden. Die diesbezüglichen Angebote sind breit gestreut und erscheinen den Schulen attraktiv, preisgünstig und praktisch. Dass dabei personenbezogene Daten in die Sphäre Dritter gelangen, möglicherweise sogar ins Ausland transferiert werden, wird offenbar häufig gar nicht als Problem wahrgenommen oder schlichtweg ignoriert.

Grundsätzlich darf nur die Schule die Daten der Schülerinnen, Schüler, Eltern und Lehrkräfte, die sie zur Erfüllung ihrer Aufgaben erhoben hat, verarbeiten. Verantwortlich für die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit ist, wie zuvor unter Ziffer 11.3 dargelegt, die Schulleiterin oder der Schulleiter. Selbst der Schulträger darf diese Daten nur im Wege der Datenverarbeitung im Auftrag für die Schule verarbeiten, wenn diese ihn schriftlich beauftragt und angewiesen hat.

Nach den schulrechtlichen Vorschriften ist die Schule berechtigt, unter Beachtung der Voraussetzungen des § 11 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) "die Datensicherheit gewährleistende und zuverlässige Institutionen" mit der Verarbeitung ihrer Daten zu beauftragen. Über die angesprochene Auftragsdatenverarbeitung durch den Schulträger hinaus gibt es ein unübersehbares Spektrum von Angeboten öffentlicher und nicht-öffentlicher Stellen. Dabei werden nicht selten die Voraussetzungen und Grenzen einer zulässigen Datenverarbeitung im Auftrag verkannt: Es werden keine schriftlichen Verträge mit strikten Weisungen geschlossen. Bei den Schulen liegen keine detaillierten Kenntnisse über die weitere Verarbeitung der Daten im Rahmen des Angebots vor, geschweige denn, dass ein Sicherheitskon-

zept erstellt und eine Vorabkontrolle durchgeführt wurden. Außerdem dürfte keineswegs sichergestellt sein, dass es sich bei allen Anbietern tatsächlich "um die Datensicherheit gewährleistende und zuverlässige Institutionen" handelt, und es ist ferner fraglich, ob die Daten stets "auf ADV-Arbeitsplätzen" verarbeitet werden, "die für Verwaltungszwecke eingerichtet" sind, wie es andere Schulvorschriften verlangen.

Zu den angesprochenen Problemen kommen unter Umständen noch weitere Unwägbarkeiten hinzu, wenn internationale Unternehmen ihre Dienste anbieten. So lässt sich etwa den Datenschutzhinweisen eines amerikanischen Anbieters entnehmen, dass Daten weltweit gespeichert werden können. Die Standorte der Server werden nicht preisgegeben, d.h. eine Speicherung beispielsweise in den USA kann nicht ausgeschlossen werden. Soweit es im Zusammenhang mit der Nutzung der Dienstleistung auch zu Übermittlungen etwa in die USA kommen sollte, hätte die Schulleitung meine Stellungnahme gemäß § 17 Abs. 1 Satz 3 DSG NRW einzuholen. Dazu liegt es allerdings in ihrer Verantwortung, die Zulässigkeit einer etwaigen Übermittlung zu klären. Da manche Dienstleistungsunternehmen am Markt überdies im Rahmen des sogenannten Cloud Computing auf Rechnerkapazitäten rund um den Globus zugreifen (siehe hierzu unter Ziffer 15.2), kann es ggf. zu Übermittlungen an weitere ausländische Stellen kommen. Auch dies müsste die Schulleitung vorab klären (was ihr kaum möglich sein dürfte), um für die betroffenen Staaten eine Beurteilung nach § 17 Abs. 1 DSG NRW einzuholen.

Insgesamt stoßen die vielfältigen Angebote auf großes Interesse bei den Schulen in Nordrhein-Westfalen. Die schulrechtlichen Vorschriften reichen für sich allein nicht aus, um die Wahrung der Datenschutzbelange der betroffenen Schülerinnen, Schüler, Eltern und Lehrkräfte zu gewährleisten. Die Schulleitungen bedürfen bei ihrer Prüfung und Entscheidung über eine etwaige Nutzung externer Dienste vielmehr konkreter Hilfestellung und Unterstützung.

➡ Die Angelegenheit habe ich inzwischen gegenüber dem Ministerium für Schule und Weiterbildung NRW mit der Anregung aufgegriffen, die Entscheidung der Schulen durch geeignete Maßnahmen vorzubereiten und/oder zu begleiten.

11.5 Befragung von jugendlichen Schülerinnen und Schülern durch Jugendämter zur Lebenssituation und zum Freizeitverhalten

Gemeinden eines Kreises hatten jugendliche Schülerinnen und Schüler über deren Lebenssituation und Freizeitverhalten befragt und hierbei teils sensibelste Daten erhoben.

Gemeinden eines Kreises in NRW – mit Ausnahme einer Kommune – hatten eine kreisweite Befragung bei Schülerinnen und Schülern der Klassen 7 bis 10 aller Schulformen angestoßen. Die Befragung hatte das Ziel, die Lebenssituation und das Freizeitverhalten von Jugendlichen besser kennen zu lernen. Sie sollte den Jugendämtern eine bessere Einschätzung ermöglichen, wie gut vorhandene Freizeitmaßnahmen und außerschulische Bildungsangebote von Jugendlichen angenommen werden, ob sie in ausreichendem Maße bereitgestellt werden und welche Angebote fehlen.

Über die Schulen wurde an die Jugendlichen hierfür ein 20-seitiges Formular mit 74 Fragen verteilt. Zwar enthielt das Formular den Hinweis, dass die Befragung anonym und die Teilnahme freiwillig sei. Soweit die Jugendlichen teilnähmen, sollten sie allerdings den Fragebogen dann auch vollständig ausfüllen. Und der hatte es in sich.

Durch die Befragung wurden zahlreiche, teils sensibelste Bereiche detailliert erfasst. Durch den Umfang der gesammelten Daten und über die Kombinationsmöglichkeit der Angaben war die zugesicherte Anonymität jedoch nicht zuverlässig gewährleistet.

Bedenklich war, dass der Fragebogen auch sogenannte Selbstbezichtigungsfragen enthielt, wie etwa nach eigenem Drogenkonsum, dem Mitführen einer Waffe, oder Fragen zu Gewalt, Mobbing und sexueller Belästigung. Die Datenerhebung war wegen der Möglichkeit einer personellen Zuordnung und der Gefahr einer sozialen Abstempelung unzulässig.

➡ Der LDI-Empfehlung, die Fragebögen ersatzlos zu vernichten, sind die Kommunen gefolgt.

12 Kommunales

12.1 Ratsvorlagen und Ratsinformationssysteme

Die Einhaltung des Datenschutzes bei der Bekanntgabe personenbezogener Daten in Rats- und Ausschusssitzungen sowie in Ratsinformationssystemen ist immer noch ein Problem.

Bereits in meinen Berichten 2003 unter Ziffer 12.1 und 2007 unter Ziffer 11.4 habe ich darüber informiert, dass personenbezogene Daten durch Kommunen im Rat nur offenbart werden dürfen, soweit entgegenstehende schützenswerte Interessen Einzelner oder Belange des öffentlichen Wohls nicht überwiegen. Grundsätzlich ist hierbei eine Abwägung zwischen dem Anspruch der betroffenen Person auf Schutz ihrer Daten und dem Prinzip der Öffentlichkeit von Rats- und Ausschusssitzungen vorzunehmen. Darüber hinaus ist der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit zu beachten. An die Erforderlichkeit der Bekanntgabe ist ein strenger Maßstab zu stellen. Er setzt eine Prüfung in jedem konkreten Einzelfall voraus, ob den Rats- und Ausschussmitgliedern auch ohne Offenbarung der Daten eine ausreichende Grundlage für eine sachgerechte Entscheidung zur Verfügung steht. Hierauf hat auch die Landesregierung Nordrhein-Westfalen bei der Beantwortung einer Kleinen Anfrage (LT-Drs. 14/1593) hingewiesen.

In Ratsinformationssystemen im Internet, mit denen zahlreiche Kommunen ihre Bürgerschaft informieren, ist die Bekanntgabe personenbezogener Daten – hierzu gehört auch bereits die Adresse – gemäß § 4 Datenschutzgesetz Nordrhein-Westfalen nur zulässig, wenn die oder der Betroffene vorher eingewilligt hat. Eine Rechtsgrundlage, die eine Bekanntgabe ohne vorherige Einwilligung erlaubt, existiert nicht.

Die Zahl der bei mir eingehenden Eingaben spricht leider dafür, dass viele Kommunen diese datenschutzrechtlichen Vorgaben noch nicht einhalten.

- Eine adäquate Sitzungsvorbereitung der gewählten Ratsmitglieder wie auch die umfassende Information der Öffentlichkeit kann und muss auch unter Beachtung des Datenschutzes durch die Kommunen gewährleistet werden.

12.2 Neuer Personalausweis – Kleine Karte für mündige Bürgerinnen und Bürger

Der am 1. November 2010 eingeführte neue Personalausweis (nPA) nimmt Bürgerinnen und Bürger auf eine völlig neue Art und Weise in die Pflicht. Neben einer auch digitalen Speicherung der Grunddaten werden nun – teilweise auf Wunsch – ähnlich wie beim Pass biometrische Daten gespeichert. Zudem können auf Wunsch Funktionen eingerichtet werden, die eine Teilnahme am elektronischen Rechts- und Geschäftsverkehr ermöglichen. Damit ist der elektronische Personalausweis weit mehr als ein Ausweispapier.

Mit dem elektronischen Personalausweis werden drei neue Funktionsbereiche eingeführt:

1. Die zusätzliche Speicherung biometrischer Merkmale wie im elektronischen Reisepass: Als elektronische Funktionen werden die bisher schon optisch vom Dokument ablesbaren Daten nun in einem kontaktlos auslesbaren Ausweis-Chip abgelegt. Das Gesichtsbild wird in jedem Fall auslesbar gespeichert. Freiwillig können Bürgerinnen und Bürger zwei Fingerabdrücke speichern lassen.

2. Auf Wunsch wird eine elektronische Identifikation/Authentifizierung durch Speicherung und Nutzung der bereits bisher auf dem Personalausweis aufgedruckten Daten aktiviert. Damit können sich die Ausweisinhaberinnen und -inhaber auch online ausweisen. Dies funktioniert sowohl gegenüber Behörden im sogenannten E-Government als auch gegenüber privatwirtschaftlich tätigen Dienstleistungsunternehmen, beispielsweise beim Online-Shopping (z.B. Flugtickets).

3. Die Ausweise sind für die Aufnahme qualifizierter elektronischer Signaturen, welche bisher nur mittels gesonderter Karten genutzt werden konnten, vorbereitet.

Die Einführung des nPA in der Praxis begleite ich aufmerksam unter Technik- und insbesondere unter Sicherheitsaspekten. Dazu gehört auch die Anwendungsfreundlichkeit in der Praxis. Die Möglichkeit, den nPA im Rahmen elektronischer Geschäftsprozesse zu nutzen, ist zu begrüßen. Damit wird die Funktion, die dem Personalausweis bisher

schon im realen Rechtsverkehr faktisch zugedacht war, nunmehr auch auf den Online-Rechtsverkehr ausgeweitet. Im Jahr 2010 war ich in der vom Bund initiierten "Ad-hoc-Arbeitsgruppe Berechtigungszertifikate" vertreten. Diese Zertifikate erteilt das Bundesverwaltungsamt (BVA) den Dienstleistungsunternehmen nach einem System von Leitlinien, welches in der Arbeitsgruppe von Datenschutzbeauftragten des Bundes und der Länder mit dem BVA entwickelt wurde. Hier werden die Online-Geschäftsprozesse der Unternehmen im Verhältnis zu den dafür erforderlichen Daten aus dem nPA abgebildet. Dazu gehören u.a. Prozesse wie "Alters- und Wohnortverifikation", "Verträge" oder "Selbstauskunft". Bereits im Berechtigungszertifikat wird die Freigabe zum Auslesen bestimmter Daten festgelegt. Hieran ist das Unternehmen bei seiner Online-Praxis gebunden. So kann zum Beispiel der Zugang zu nicht jugendfreien Seiten zukünftig schon zu Beginn des Kontaktes zur Kundin oder zum Kunden über eine Altersverifikation aus dem nPA gesteuert werden. Für das jeweilige Rechtsgeschäft nicht erforderliche Daten werden nicht abgerufen.

Auch eine Kommune aus NRW hat in Abstimmung mit mir beim BVA zwei Berechtigungszertifikate für das Auslesen von Daten im Bereich der städtischen Online-Angebote beantragt. Zur Vorbereitung der allgemeinen Einführung des nPA wurde zudem bundesweit seit Anfang 2010 ein sogenannter Feldtest durchgeführt. Hieran nahmen auch Kommunen aus NRW teil.

Es wird weiterhin aufmerksam zu beobachten sein, wie die Bürgerinnen und Bürger mit dem neuen technischen Möglichkeiten umgehen. Die Vereinigung mehrerer Funktionen auf einer Karte erhöht trotz technischer Sicherung das Missbrauchrisiko bei Verlust der Karte.

➡ Ich werde die Einführung des nPa in der Praxis weiter begleiten. Auf der Grundlage der dabei noch zu gewinnenden Erkenntnisse wird eine abschließende datenschutzrechtliche Bewertung erst möglich sein.

12.3 Kommunales Forderungsmanagement nicht außer Haus!

Wirtschaftlich verantwortungsbewusstes Handeln von Kommunen setzt auch voraus, dass sie ihre rückständigen Forderun-

gen effizient einziehen. Falls es an der hierfür erforderlichen Verwaltungsorganisation, qualifiziertem Personal oder Fachwissen mangelt, wird eine Optimierung des Forderungsmanagements zuweilen durch Beauftragung privater Unternehmen angestrebt.

So ließ eine Kommune in ihrem Auftrag Mahngespräche mit säumigen Bürgerinnen und Bürgern durch ein Treuhandunternehmen durchführen. Bei den zugrunde liegenden Schulden handelte es sich um kommunale Steuerforderungen.

Nach den mit den betroffenen Steuerpflichtigen zu führenden Mahngesprächen sollte das Unternehmen die Kommune über die hinsichtlich der Schulden getroffenen Vereinbarungen unterrichten. Ein Forderungseinzug sollte hingegen nicht erfolgen. Die Einwilligung der Steuerpflichtigen in die Bekanntgabe ihrer Daten an das Unternehmen lag nicht vor.

Die Vorgehensweise der Stadt warf mehrere rechtliche Probleme auf:

- Die Mahnung ist auch in Form eines Mahngesprächs als regelmäßig einer Vollstreckungshandlung vorhergehende Maßnahme der Verwaltungsvollstreckung zuzuordnen und stellt damit eine hoheitliche Aufgabe dar. Sie ist kein Bestandteil der Finanzbuchhaltung der Kommune, die ganz oder zum Teil von einer Stelle außerhalb der Gemeindeverwaltung besorgt werden kann (§ 94 Gemeindeordnung für das Land Nordrhein-Westfalen), so dass die Inanspruchnahme einer Stelle außerhalb der Gemeindeverwaltung nicht in Betracht kam. Eine dafür erforderliche vollstreckungsrechtliche Befugnis für die Übertragung des Mahnwesens auf ein Inkassounternehmen bestand somit nicht.
- Eine Datenverarbeitung im Auftrag konnte ebenso nicht angenommen werden, da bei der Kommune die uneingeschränkte Verantwortlichkeit für die Datenverarbeitung und -nutzung nicht verblieben war.
- In der unzulässigen Verarbeitung und Nutzung der kommunalen Steuerdaten durch das Inkassounternehmen lag zudem eine Verletzung des Steuergeheimnisses (§ 30 Abgabenordnung).
- Schließlich wurde das Inkassounternehmen in unzulässiger Weise durch die Bekanntgabe der Daten in die Lage versetzt, unter Ver-

wendung der Daten der Steuerpflichtigen seine eigenen Datenbestände ergänzen zu können.

Nach entsprechender Beratung durch meine Behörde sowie nach Rücksprache mit der Kommunalaufsicht hat die Kommune ihre Zusammenarbeit mit dem Unternehmen im Bereich des Mahnwesens eingestellt.

➡ Das Verwaltungsvollstreckungsgesetz NRW erlaubt keine Privatisierung des kommunalen Forderungsmanagements.

13 Polizei und Justiz

13.1 Gesetz zur Vorratsdatenspeicherung gekippt – Kommt nun Quick-Freeze?

Die von der Europäischen Richtlinie 2006/24/EG geforderte sechsmonatige, anlasslose Speicherung von Telekommunikationsverbindungsdaten ist aus datenschutzrechtlicher Sicht ein Dammbruch, gegen den das Bundesverfassungsgericht mit seiner Entscheidung vom 2. März 2010 einen – vorläufigen – Schutzwall errichtet hat. Nun tobt der Streit zwischen Befürwortern und Gegnern der sogenannten Vorratsdatenspeicherung weiter, während sich die EU Gedanken über eine Überarbeitung der Richtlinie macht.

Selten prallen Datenschutzvorstellungen und Sicherheitsdenken so unversöhnlich aufeinander wie beim Thema Vorratsdatenspeicherung, der verdachtslosen Speicherung aller Telefon- und Internetverbindungsdaten für Zwecke der Kriminalitätsbekämpfung, die hierzulande für sechs Monate erfolgen sollte. Die massenhaften Verfassungsbeschwerden gegen die Umsetzung der europäischen Vorgaben zeigen, dass der Einschnitt in die persönliche Freiheit durch die Vorratsdatenspeicherung bei einer großen Bevölkerungsgruppe einen Nerv getroffen hat: das Bedürfnis nach Schutz der Privatsphäre.

Im Rahmen der durch diese Protestbewegung veranlassten verfassungsrechtlichen Prüfung der Umsetzungsgesetze haben die Datenschutzbeauftragten der Länder eine gemeinsame Stellungnahme gegenüber dem Bundesverfassungsgericht abgegeben. Sie haben darin betont, dass sie die Vorratsdatenspeicherung für verfassungswidrig halten, weil sie das Fernmeldegeheimnis, also das Grundrecht auf von staatlichen Stellen unbeobachtete Telekommunikation, in seinem Wesensgehalt verletzt, jedenfalls aber unverhältnismäßig und damit unzulässig in dieses Grundrecht eingreift.

Dieser Ansicht ist das Bundesverfassungsgericht zwar nicht in allen Punkten gefolgt. Es hat aber in seiner Entscheidung vom 2. März 2010 hervorgehoben, dass

- die Vorratsdatenspeicherung einen schwerwiegenden Grundrechtseingriff darstelle,

- es zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehöre, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst werden darf,
- eine Vorratsdatenspeicherung nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht komme,
- eine derartige anlasslose Datensammlung nur verfassungsgemäß sein könne, wenn sie Ausnahmecharakter habe, und
- an eine verhältnismäßige gesetzgeberische Ausgestaltung höchste organisatorische und sicherheitstechnische Anforderungen zu stellen seien.

Das Bundesverfassungsgericht hat die Vorratsdatenspeicherung damit also nicht generell für verfassungswidrig erklärt. Es hat aber nicht nur sehr hohe Anforderungen an eine verfassungsgemäße Ausgestaltung gestellt, sondern die bisherige gesetzliche Regelung mit sofortiger Wirkung für nichtig erklärt.

Die Datenschutzbeauftragten des Bundes und der Länder haben das Urteil im Ergebnis begrüßt und in einer gemeinsamen Entschließung vom 17./18. März 2010 (Abdruck im Anhang) ihr grundsätzliches Nein zur Vorratsdatenspeicherung wiederholt. Vor dem Hintergrund, dass die EU selbst eine umfassende Evaluierung der Richtlinie in Angriff genommen hat, haben sie die Bundesregierung ferner aufgefordert, sich für eine Aufhebung der Europäischen Richtlinie einzusetzen.

Da angesichts der Evaluierung der Richtlinie zu erwarten ist, dass sich die europäischen Vorgaben ändern könnten, hat sich eine politische Debatte darüber entwickelt, ob und wann die noch gültige Richtlinie umzusetzen ist. Im Zuge dieser Diskussion wurden Vorschläge eingebracht, wie Datenschutz und Sicherheitsbedürfnisse zu vereinbaren sein könnten: etwa durch ein sogenanntes Quick-Freeze -Verfahren, bei dem lediglich die ohnehin von den Telekommunikationsunternehmen gespeicherten Daten bei Bedarf sofort "eingefroren" und nach genauer Prüfung den Strafverfolgungs - oder Sicherheitsbehörden zur Verfügung gestellt werden könnten. Zum Teil wird auch eine Kombination dieser Lösung mit einer kurzzeitigen Vorratsdatenspeicherung vorgeschlagen.

In der Diskussion um "Vorratsdatenspeicherung", "Quick-Freeze" oder "Quick-Freeze Plus" (= "Vorratsdatenspeicherung light") muss die

Frage geklärt werden, welche Daten zu welchem Zweck benötigt werden. Die Geeignetheit und Erforderlichkeit der Datenspeicherung sind Grundlage der Diskussion über die datenschutzrechtliche Zulässigkeit dieser Maßnahme.

- Die Verfassungsbeschwerden gegen die Vorratsdatenspeicherung haben dazu geführt, dass eine schwerwiegende Beeinträchtigung der persönlichen Freiheit für alle Bürgerinnen und Bürger zumindest vorläufig unterbleibt und Zeit gewonnen ist, um neu zu überdenken, welche Maßnahmen zur Strafverfolgung wie auch zum Schutz der Bürgerinnen und Bürger wirklich notwendig und mit einem freiheitlichen Gemeinwesen noch vereinbar sind.

13.2 Neues Bundeskriminalamtgesetz (BKAG)

Ende 2008 wurde das BKAG grundlegend geändert. Datenschutzrechtlich relevant sind insbesondere die "zur Abwehr von Gefahren des internationalen Terrorismus" neu eingefügten Rechtsgrundlagen für staatliche Maßnahmen, welche in die informationelle Selbstbestimmung eingreifen.

Das neue BKAG läutet nicht nur eine Veränderung der Sicherheitsarchitektur in Deutschland ein, sondern schafft auch die Möglichkeit, weitreichend in die Grundrechte der Bürgerinnen und Bürger einzugreifen. Erstmals werden dem BKA umfassende polizeiliche Befugnisse zur Abwehr des internationalen Terrorismus eingeräumt. Da in unserem föderalen Rechtsstaat die Abwehr von Gefahren auch im Bereich des internationalen Terrorismus Sache der Länder ist, kommt es durch die neue Zuständigkeit zu parallelen Strukturen. Schon dies führt dazu, dass mehrfach personenbezogene Daten zum gleichen Zweck erhoben werden.

Das Gesetz ermöglicht der Bundespolizei, im Vorfeld von Gefahren Ermittlungen zu tätigen. Dies führt zu einer Ausweitung polizeilicher Datenverarbeitung. Der Bundespolizei werden zum Zwecke der Gefahrenabwehr neue Befugnisse eingeräumt, insbesondere verdeckte Eingriffe in informationstechnische Systeme (Online-Durchsuchung, Quellen-Telekommunikationsüberwachung), die das Bundesverfas-

sungsgericht in nur sehr engen verfassungsrechtlichen Grenzen für zulässig hält.

Es bestehen Zweifel, ob insbesondere die zuvor genannten Befugnisse den verfassungsrechtlichen Anforderungen entsprechen. Abgesehen von sich hier oder an anderer Stelle des Gesetzes stellenden Fragen zur Bestimmtheit, zur Ausgestaltung des Schutzes des Kernbereichs und zu Verfahrensgestaltungen, die zur Sicherung der Rechte von Betroffenen erforderlichen sind, eignen sich derartige Befugnisse kaum als Mittel der polizeilichen Gefahrenabwehr. Solche Maßnahmen setzen voraus, dass bereits Anhaltspunkte für eine Gefahr vorliegen. Sind keine Anhaltspunkte gegeben, wird die Erforderlichkeit derart weitreichender Befugnisse für Zwecke der polizeilichen Gefahrenabwehr eher zu verneinen sein. Darüber hinaus kann – jedenfalls in Bezug auf aus einer Online-Durchsuchung erlangte Daten – die Validität der Daten für Zwecke der polizeilichen Gefahrenabwehr, die schließlich im Ergebnis auf konkrete Gefahren beendende Eingriffe ausgerichtet sein soll, nicht ohne weitere Informationen rechtssicher unterstellt werden. Die Bedenken gelten um so mehr, als das Erfordernis, dem BKA diese Befugnisse einzuräumen, u.a. mit dem Argument begründet wird, das BKA müsse in Fällen von Terrorgefahr für den – als begrenzt einzuschätzenden – Zeitraum, in denen die zuständige Landespolizei noch nicht feststehe, einstweilen handeln können.

Schon vor diesem Hintergrund kann ich nur davon abraten, Befugnisse vorzusehen, die zu nahezu unbegrenzbaren Eingriffen in die Privatsphäre der Bürgerinnen und Bürger berechtigen.

Dem Bundesverfassungsgericht liegen mehrere Verfassungsbeschwerden vor.

➡ Die weitere Entwicklung werde ich aufmerksam verfolgen. In jedem Fall muss die im Gesetz vorgesehene Evaluierung kritisch begleitet werden, auch im Hinblick auf die Zuständigkeit der Länder.

13.3 Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW) geändert – Kernbereichsschutz ausdrücklich verankert

Die mit dem Gesetz zur Änderung des PolG NRW vom 9. Februar 2010 vorgenommenen Änderungen sind vergleichsweise moderat ausgefallen. Während zunächst noch zu befürchten war, dass die massiv ausgebauten präventiven Befugnisse des Bundeskriminalamts (siehe hierzu unter Ziffer 13.2) auch Eingang in das PolG NRW finden würden, beschränkt sich das Änderungsgesetz vorrangig auf die Fortschreibung von bereits Vorhandenem.

Gerade im Hinblick darauf, dass das Polizeirecht Regelungen zur Gefahrenabwehr und nicht zur repressiven Strafverfolgung enthält, birgt die Vorverlagerung von Handlungsbefugnissen immer eine erhöhte Gefahr grundrechtsbeeinträchtigenden Handelns. Umso begrüßenswerter ist es, dass der Gesetzgeber die Rechtsprechung des Bundesverfassungsgerichts zum Schutz des Kernbereichs der privaten Lebensgestaltung nunmehr durch eine allgemeine Kernbereichsschutzregelung in § 16 PolG NRW umzusetzen versucht. Diese Regelung stellt klar, dass die Erhebung personenbezogener Daten, die dem Kernbereich zuzurechnen sind, unzulässig ist.

Das in Zweifelsfällen vorgesehene Verfahren zur Feststellung der Kernbereichsbetroffenheit bedarf allerdings in der Praxis insofern einer Präzisierung, als § 16 Abs. 3 PolG NRW nunmehr auch eine Einbindung der oder des behördlichen Datenschutzbeauftragten in den Prüfungsprozess vorsieht. § 32a Abs. 2 Satz 3 Datenschutzgesetz NRW fordert für behördliche Datenschutzbeauftragte jedoch, dass diese während ihrer Tätigkeit nicht mit Aufgaben betraut werden, deren Wahrnehmung zu Interessenkollisionen führen könnte. Mit dieser Regelung soll vermieden werden, dass sich Datenschutzbeauftragte selbst kontrollieren müssen. Datenschutzbeauftragte dürfen deshalb nicht in größerem Umfang selbst Daten verarbeiten oder für Entscheidungen über Datenverarbeitungen verantwortlich sein. Mit der Aufgabenzuweisung, im Bereich des Kernbereichsschutzes tätig zu werden, laufen behördliche Datenschutzbeauftragte aber Gefahr, nicht lediglich mit der Kontrolle von Entscheidungen betraut, sondern in die Entscheidungsfindung selbst einbezogen zu werden. Hierzu enthalten die

zwischenzeitlich erlassenen Verwaltungsvorschriften allerdings klarstellende Anmerkungen, was zu begrüßen ist.

➡ Die Umsetzung der nunmehr getroffenen und grundsätzlich zu begrüßenden gesetzlichen Kernbereichsschutzregelungen werde ich in der Praxis aufmerksam verfolgen.

13.4 Land regelt den Justizvollzug – Zentrale Haftdatei soll errichtet werden

Im Zuge der Föderalismusreform aus dem Jahr 2006 ging die Gesetzgebungskompetenz für den Justizvollzug auf die Länder über. Bei den bisher hierzu getroffenen landesgesetzlichen Regelungen wäre mehr Datenschutz möglich gewesen.

Die Länder mussten zunächst die überfällige gesetzliche Regelung des Jugendstrafvollzugs innerhalb der vom Bundesverfassungsgericht gesetzten Übergangsfrist schaffen. Es folgten die Gesetze zum Vollzug der Untersuchungshaft. Eine Neuregelung des Erwachsenenstrafvollzugs steht in den meisten Ländern, auch in NRW, noch aus.

Seit März 2010 gilt hierzulande das Gesetz zur Regelung des Vollzugs der Untersuchungshaft, zuvor waren bereits im Januar 2008 das Gesetz zur Regelung des Vollzugs der Jugendstrafe und im November 2009 das Gesetz zur Verbesserung der Sicherheit in den Justizvollzugsanstalten (JVollzSG NRW) in Kraft getreten.

Die umfassenden datenschutzrechtlichen Stellungnahmen meiner Behörde haben in den Gesetzgebungsverfahren nur in wenigen Einzelpunkten Berücksichtigung gefunden. Aufgrund der bisherigen Erfahrungen bei der Anwendung des Strafvollzugsgesetzes des Bundes hatte meine Behörde insbesondere vorgeschlagen,

- die bisher schwach ausgestalteten und von den Vollzugsbehörden oft sehr restriktiv ausgelegten Auskunfts- und Akteneinsichtsrechte der Gefangenen im Hinblick auf die über sie selbst gespeicherten Informationen zu verbessern,
- die demgegenüber sehr großzügigen Regelungen der Überlassung von Gefangenenakten an öffentliche Stellen außerhalb des Vollzugs und insbesondere an Forschende einzuschränken und für die

Forschung mit Gefangenendaten die Regelung aus dem nordrhein-westfälischen Datenschutzgesetz zu übernehmen und

- das Vertrauensverhältnis zwischen den Gefangenen und dem medizinischen Dienst zu stärken, indem Durchbrechungen der Schweigepflicht nicht mehr für jede Aufgabe der Vollzugsbehörde, sondern nur unter engen Voraussetzungen erlaubt werden.

Leider wurde die Chance nicht genutzt, die gesetzliche Ausgangslage diesbezüglich zu verbessern. Stattdessen wurden weitgehend die bisherigen bundesgesetzlichen Regelungen des Erwachsenenstrafvollzugs auf den Jugendstrafvollzug und den Untersuchungshaftvollzug übertragen.

Neu geschaffen wurde jedoch eine Rechtsgrundlage für Videoüberwachung in den Justizvollzugsanstalten. Grundsätzlich ist zu begrüßen, dass eine so verbreitete und in die Persönlichkeitsrechte eingreifende Maßnahme nunmehr auf eine gesetzliche Grundlage gestellt wurde. Auch sind im Verlaufe des Gesetzgebungsverfahrens datenschutzrechtliche Verbesserungen erzielt worden, zum Beispiel wurden die Voraussetzungen für die Speicherung der Videoaufnahmen ausdrücklich geregelt und Bildaufzeichnungen von Hafträumen dabei ausgeschlossen. Dennoch bleiben einige Kritikpunkte bestehen: Vor allem erscheint die Videobeobachtung von Hafträumen, auch wenn sie nur im besonderen Einzelfall angeordnet werden kann, weiter grundsätzlich problematisch. Es ist unklar, wie hierbei die Gewährleistung einer Intimsphäre der Gefangenen mit den vollzuglichen Bedürfnissen, einschließlich des Schutzes der Gefangenen selbst, vereinbart werden kann. Zumindest sollte eine ausdrückliche Information der Betroffenen vor Beginn der Maßnahme gesetzlich verpflichtend vorgesehen werden.

Ein besonderer Problempunkt ist weiterhin die geplante Errichtung einer Zentralen Haftdatei, in der Gefangenendaten für die Vollzugsbehörden des Landes zentral gespeichert und dem Zugriff weiterer öffentlicher Stellen ausgesetzt werden sollen.

Die Notwendigkeit für eine solche Zentraldatei ist aus meiner Sicht bisher nicht hinreichend dargelegt worden. Auch die Zwecke, denen sie dienen soll, sind nicht gesetzlich definiert worden. Dies ist bedenklich, da Datenerhebung und Datenverarbeitung immer nur aufgabenbezogen erfolgen dürfen und ihre Erforderlichkeit nur im Hinblick auf

den konkret verfolgten Zweck beurteilt werden kann. So wäre etwa das Ziel, die Zugriffsmöglichkeit der Aufsichtsbehörde auf die von ihr im Einzelfall benötigten Gefangenendaten zu verbessern, für sich genommen nicht zu beanstanden.

Darüber hinaus fehlt die notwendige Definition des Speicherumfangs. Die gesetzliche Formulierung, die im Vollzug erhobenen Daten "können für die Vollzugsbehörden im Geltungsbereich dieses Gesetzes in einer Zentralen Datei gespeichert werden", ist wegen ihrer Unbestimmtheit verfassungsrechtlich bedenklich. Eine umfassende zentrale Speicherung aller im Vollzug erhobenen Gefangenendaten erscheint unverhältnismäßig. Statt der Exekutive die Auswahl der zentral benötigten Daten zu überlassen, müssten die für die Zwecke der Datei erforderlichen Datensätze vielmehr in der gesetzlichen Eingriffsermächtigung selbst so genau wie möglich umgrenzt, am besten – ähnlich wie in anderen Gesetzen wie z.B. dem Meldegesetz oder wie in der Regelung des länderübergreifenden staatsanwaltschaftlichen Verfahrensregisters – abschließend aufgezählt werden.

➡ Im Zuge eines Gesetzgebungsverfahrens zur Neuregelung des Erwachsenenstrafvollzugs sollte über die datenschutzrechtlichen Kernprobleme auch der bisherigen Vollzugsgesetze neu nachgedacht werden. Dringender Nachbesserungsbedarf besteht ferner im Hinblick auf die rechtliche Verankerung und Ausgestaltung der geplanten zentralen Haftdatei. Darüber bin ich mit dem Justizministerium im Gespräch.

13.5 Zuverlässigkeitsüberprüfungen bei der FIFA-Frauen-Fußball-WM 2011

Bei der FIFA-Frauen-Fußball-WM, die im Sommer 2011 in Deutschland stattfinden wird, sind wieder Zuverlässigkeitsüberprüfungen bei den vor Ort eingesetzten Beschäftigten geplant. Die Polizei in NRW hat im Hinblick auf die Durchführung des Akkreditierungsverfahrens die Federführung übernommen.

Die datenschutzrechtlichen Bedenken, die schon in Hinblick auf andere Großereignisse geäußert wurden (siehe Bericht 2007 unter Ziffer 6.1 und dort im Anhang die Entschließung der 74. Datenschutzkonferenz

vom 25./26. Oktober 2007), bestehen nach wie vor. Es zeigt sich darüber hinaus, dass sich konzertierte Sicherheitsüberprüfungen bei Großereignissen immer mehr vom Ausnahme- zum Regelfall entwickeln.

Von den Zuverlässigkeitsüberprüfungen sind vor allem Personen betroffen, die bei Ordner- und Sicherheitsdiensten beschäftigt sind und in oder vor Stadien und Trainingsstätten eingesetzt werden. Weiterhin werden Personen, die sich in besonders sicherheitssensiblen Bereichen, z.B. in VIP-Bereichen, aufhalten, auf ihre Zuverlässigkeit überprüft.

Das Tätigwerden der Polizei- und Verfassungsschutzbehörden erfolgt allein auf der Grundlage der Einwilligung der betroffenen Arbeitnehmerinnen und Arbeitnehmer. Da die Beschäftigten jedoch bei einer Weigerung, sich der Überprüfung zu unterziehen, voraussichtlich arbeitsrechtliche Konsequenzen zu befürchten haben, ist die Freiwilligkeit der abzugebenden Einwilligungserklärungen und damit deren Wirksamkeit zu bezweifeln. Von einer solchen Freiwilligkeit könnte allenfalls dann ausgegangen werden, wenn den Betroffenen die Möglichkeit offenstünde, im Falle ihrer Weigerung in anderen nicht sicherheitsrelevanten Bereichen eingesetzt zu werden, und wenn sie keine arbeitsrechtlichen Konsequenzen zu befürchten hätten.

- Sollte beabsichtigt sein, Polizei und Verfassungsschutz verstärkt in Zuverlässigkeitsüberprüfungen bei Großereignissen einzubinden, ist eine entsprechende Rechtsgrundlage zu schaffen. Diese muss dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit genügen und insbesondere die Erforderlichkeit von Sicherheitsüberprüfungen im Verhältnis zu einem tatsächlich möglichen Sicherheitsgewinn im Blick haben. Dabei sind den Betroffenen auch Verfahrensrechte einzuräumen.

13.6 Inbetriebnahme von polizeilichen Videofahrrädern gestoppt

Mit Helmkamera Jagd auf Verkehrssünderinnen und -sünder auf dem Fahrrad machen – dies war das Anliegen von zwei Po-

lizeibehörden, in deren Innenstädten sich Unfälle mit Fahrradbeteiligung häuften. Es fehlte für dieses Vorhaben aber die notwendige Rechtsgrundlage.

Für die Erfassung potentieller Verkehrssünder sollten polizeiliche Fahrradstreifen die Möglichkeit haben, durch Aktivierung einer Helmkamera Videoaufzeichnungen von Verstößen gegen die Straßenverkehrsordnung zu fertigen. Durch gezielte Ansprache und Konfrontation mit den Aufzeichnungen sollte bei den Betroffenen das Problembewusstsein geweckt werden.

Gegen dieses grundsätzlich nachvollziehbare Anliegen bestanden jedoch deshalb datenschutzrechtliche Bedenken, weil die als mögliche Grundlagen genannten Vorschriften der Strafprozessordnung (StPO) den Eingriff nicht tragen:

Meine Behörde wies die betreffenden Polizeibehörden zum einen darauf hin, dass die generelle Eingriffsbefugnis des Ordnungswidrigkeitengesetzes in Verbindung mit der StPO zwar für Ermittlungen jeder Art gilt. Die Anwendung spezieller gesetzlicher Ermittlungsmaßnahmen der StPO zur Fertigung von Bildaufzeichnungen geht jedoch vor. Daher kann nicht auf die allgemeinen Regelungen zurückgegriffen werden.

Die Anwendung der spezielleren StPO-Regelungen zu Bildaufnahmen scheidet aber auch aus. Nach diesen Vorschriften können auch ohne Wissen der Betroffenen außerhalb von Wohnungen Bildaufnahmen hergestellt werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthalts der Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert sind. Die Fahrradstreifenbeamtinnen und -beamten können jedoch den Sachverhalt bezeugen und stehen damit zur Aufklärung als Zeuginnen und Zeugen des Sachverhalts zur Verfügung. Werden die betreffenden Radfahrerinnen und -fahrer angehalten und ihre Personalien festgestellt, werden die Aufzeichnungen nicht benötigt. Das Problem der fehlenden Identitätsfeststellungsmöglichkeit bei flüchtenden Radfahrerinnen und -fahrern wird durch die Aufzeichnung nicht gelöst, denn mit Kfz-Kennzeichen vergleichbare Fahrradkennzeichen gibt es nicht, so dass Ermittlungen aussichtslos sind. Schließlich ist auch die Feststellung eines hinreichenden Anfangsverdachts problematisch. Es besteht insofern die Besorgnis einer "prophylaktischen" Inbetriebnahme der

Kamera in Fällen einer bloßen Vermutung, dass sich demnächst ein verkehrsrechtlicher Verstoß ereignen könnte.

➡ Die Polizei hat den Einsatz von Videofahrrädern nicht weiter verfolgt.

13.7 Lichtbilderstellung in Gefangenensammelstellen

Zwei Petenten, die während eines polizeilichen Einsatzes in eine Gefangenensammelstelle gebracht worden waren, beanstandeten, dass dort von ihnen Lichtbilder gefertigt worden waren, obwohl sie ihre Identität durch Vorlage ihrer Personalausweise nachweisen wollten. Als Grund für diese Vorgehensweise wurde seitens der Polizei auf die Notwendigkeit einer Identitätsfeststellung während laufender Maßnahmen verwiesen. Die Beteiligung an einer Straftat wurde beiden Personen nicht vorgeworfen.

Die betreffende Polizeibehörde hat in ihrer Stellungnahme eingeräumt, dass in einem solchen Fall, in dem die Betroffenen die Identifizierung selbst ermöglichen und keiner Straftat verdächtig sind, weder die Voraussetzungen für eine Identitätsfeststellung noch für eine erkennungsdienstliche Behandlung vorliegen. Sie verweist jedoch auf die polizeirechtliche Generalklausel des § 8 Abs. 1 Polizeigesetz des Landes Nordrhein-Westfalen als Befugnisnorm. Demgegenüber hat meine Behörde die Auffassung vertreten, dass das polizeiliche Handeln schon allein deswegen nicht auf die Generalklausel gestützt werden kann, weil es spezialgesetzliche Regelungen zur Erstellung von Lichtbildern gibt. Sind diese nicht einschlägig, scheidet eine Anwendung der allgemeinen Regelung aus, weil andernfalls die Voraussetzungen der spezialgesetzlichen Grundlagen umgangen werden. Darüber hinaus liegt in diesen Fällen auch keine konkrete Gefahr vor. Die Personalien der betroffenen Personen werden bereits zu Beginn der Ingewahrsamnahme automatisiert erfasst. Alle notwendigen Informationen zu den Betroffenen sind bekannt. Weshalb es in einer solchen Konstellation überhaupt einer Lichtbildfertigung bedarf, ist nicht einsichtig. Sofern es um die Verfolgung von Straftaten der in Gewahrsam Genommenen geht, existieren andere Rechtsgrundlagen für eine Lichtbilderstellung. Rein organisatorische Schwierigkeiten der Beamtinnen und Beamten vor Ort rechtfertigen

den Grundrechtseingriff durch Fertigung von Lichtbildern jedenfalls nicht. Auch das Innenministerium NRW blieb in seiner Stellungnahme jedoch bei der Auffassung, dass eine Anwendbarkeit der Generalklausel für die Lichtbildfertigung in Gefahrensammelstellen in Betracht komme.

➡ Diese Einsatzpraxis ist nicht rechtskonform. Das Ministerium für Inneres und Kommunales sollte seine Praxis ändern.

13.8 Schuldner im Netz – Bundesweiter Online-Zugriff auf Daten von Schuldnerinnen und Schuldnern mit Zahlungsschwierigkeiten ab dem Jahr 2013

Bereits bisher gibt es bei den Vollstreckungsgerichten Schuldnerverzeichnisse, in die unter bestimmten Voraussetzungen auch private Dritte Einsicht erhalten können. Ab dem Jahr 2013 sollen die Schuldnerverzeichnisse über ein Internetportal zur Verfügung gestellt werden. Die Einsichtnahme soll wesentlich erleichtert werden.

Das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vom 29. Juli 2009 hat zum wesentlichen Ziel, die Stellung von Gläubigerinnen und Gläubigern im Zwangsvollstreckungsverfahren zu stärken. Hierzu gehört unter anderem die Schaffung eines bundesweiten, automatisiert geführten Schuldnerverzeichnisses, durch das die Daten zahlungsunfähiger oder -unwilliger Schuldnerinnen und Schuldner über das Internet abrufbar werden.

Zur Verwirklichung dieses Projektes hat sich die Bund-Länder-Arbeitsgruppe "Vollstreckungsportal" gebildet. Das Land NRW, das bereits Erfahrung mit einem landesweiten elektronischen Schuldnerverzeichnis besitzt, hat die Federführung für die Umsetzung übernommen. Zurzeit wird ein Verordnungsentwurf des Bundes zur Regelung der Einzelheiten des Verfahrens erwartet. Im Austausch mit den in NRW an dem Vorhaben Beteiligten habe ich Gelegenheit, seine Ausgestaltung kritisch zu begleiten. Dabei konnten bisher verschiedene Datenschutzprobleme, aber auch einzelne datenschutzrechtliche Verbesserungen ausgemacht werden:

Soweit vorgeschlagen wird, neben dem elektronischen Personalausweis auch Kreditkartendaten zur Identifizierung bei der Abfrage im Internet zuzulassen, habe ich grundsätzliche Bedenken. Erstens besteht dabei die Gefahr eines Missbrauchs von fremden Kreditkartendaten, zweitens halte ich es für problematisch, wenn staatliche Stellen zur Identifizierung abfrageberechtigter Personen auf andere Mittel als den dafür vorgesehenen Personalausweis zurückgreifen.

Problematisch ist auch, wie bei einer Anfrage über das Internet das Vorliegen der Voraussetzungen für die Auskunftserteilung geprüft werden soll. Die Einsichtnahme in das Schuldnerverzeichnis ist schließlich nicht zu jedem beliebigen Zweck gestattet. Vielmehr sind im Gesetz die zulässigen Verwendungszwecke abschließend aufgeführt: neben der Zwangsvollstreckung etwa die Abwendung wirtschaftlicher Nachteile, wenn beispielsweise ein Rechtsgeschäft mit der Schuldnerin oder dem Schuldner abgeschlossen werden soll. Fraglich ist, wie diese gesetzlich legitimierten Interessen im Internet so "dargelegt" werden können, dass ihnen noch eine beschränkende Funktion zukommt. Das bloße Anklicken dargebotener Auswahlmöglichkeiten dürfte kaum den Voraussetzungen des Begriffs "Darlegen" entsprechen und würde aus meiner Sicht diese beschränkende Funktion nicht besitzen. Hierbei würde eine Stelle fehlen, die die Erklärung entgegennimmt und die, wie im bisherigen Verfahren, eine Plausibilitätskontrolle vornehmen und sich etwa Unterlagen vorlegen lassen könnte.

Einen gewissen Ausgleich bildet die Protokollierung der Zugriffe, die eine nachträgliche Kontrolle ermöglicht. Ferner soll bei der elektronischen Version die Einsichtnahmemöglichkeit der Schuldnerinnen und Schuldner in den sie betreffenden Datensatz einschließlich der erfolgten Abfragen verbessert werden. Hierfür sollen die Betroffenen mit der Benachrichtigung über ihre Eintragung eine PIN erhalten, die ihnen den unmittelbaren Zugriff über das Internet zu jeder Zeit ermöglicht. Damit wird auch eine nachträgliche Kontrolle der Zugriffe durch die Betroffenen selbst wesentlich erleichtert. Dies stellt einen nicht zu unterschätzenden Vorteil gegenüber dem gegenwärtigen Verfahren dar.

- Ein Zugang zum Schuldnerverzeichnis über das Internet erfordert besondere Lösungen, die die Datenschutzrechte der Betroffenen wahren.

14 Finanzen

Akteneinsichtsrecht nach der Abgabenordnung – Warten auf eine gesetzliche Neuregelung

Wer einen Zugang zu Informationen über seine Steuerdaten wünscht, muss immer noch damit rechnen, dass das Finanzamt einen entsprechenden Antrag mit dem Hinweis ablehnen wird, die Abgabenordnung (AO) enthalte hierzu keine Rechtsgrundlage und es müsse ein "berechtigtes Interesse" an der Akteneinsicht geltend gemacht werden.

Das Bundesministerium der Finanzen (BMF) hat mit einer Verwaltungsanweisung vom 17. Dezember 2008 an die obersten Finanzbehörden der Länder seine Auffassung bekräftigt, die Erteilung von Auskünften über Daten, die zu einer Person über Besteuerungsverfahren gespeichert sind, verlange die Darlegung eines "berechtigten Interesses" und das Fehlen von Gründen für eine Auskunftsverweigerung.

Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch muss auch im Besteuerungsverfahren Anwendung finden. Die Datenschutzbeauftragten des Bundes und der Länder haben daher gefordert, dass das BMF die Verwaltungsanweisung aufhebt, und im Übrigen der Auskunftsanspruch durch eine Regelung in der AO klargestellt wird. Im Sommer 2010 hat das BMF nunmehr einen Diskussionsentwurf zur Schaffung einer gesetzlichen Regelung zum Auskunftsanspruch (§ 32 AO -E-) vorgelegt. Hiergegen bestehen aus datenschutzrechtlichen Gründen erhebliche Bedenken:

So hält das BMF zwar nicht mehr am Begriff eines "berechtigten Interesses" fest, fordert allerdings nach wie vor für das Auskunftsersuchen eine begründete Darlegung. Diese Verpflichtung schränkt das Recht auf informationelle Selbstbestimmung immer noch ein. Dieses gewährt den Auskunftsanspruch vorbehaltlos.

Auch sollen pauschal all diejenigen Daten, die von Steuerpflichtigen selbst oder mit ihrem Wissen an die Finanzverwaltung übermittelt wurden, vom sachlichen Anwendungsbereich des Auskunftsanspruchs ausgenommen sein.

Hinsichtlich solcher Daten, die ohne Mitwirkung und Wissen der Betroffenen gespeichert wurden, ist eine regelmäßige Auskunftssperre bis zum Abschluss der Ermittlungen der Finanzbehörden vorgesehen.

➡ Die geplanten gesetzlichen Regelungen sind danach in mehrfacher Hinsicht nachbesserungsbedürftig. Die Landesregierung sollte sich für ein datenschutzkonformes Auskunftsrecht einsetzen. Bis zu einer normenklaren Auskunftsregelung in der Abgabenordnung müssen die Finanzbehörden Auskünfte an Steuerpflichtige nach der durch das Bundesverfassungsgericht vorgezeichneten Rechtslage erteilen (siehe Entschließung der Datenschutzkonferenz vom 26./27. März 2010 im Anhang).

15 Technik und Medien

15.1 Internet – Analyse des Surfverhaltens

Die Analyse des Surfverhaltens im Internet darf nicht personenbezogen erfolgen. Nur pseudonyme Nutzungsprofile sind zulässig. Einige Analyseverfahren beachten diese Rechtsvorgabe nicht.

Eine Reichweitenmessung im Internet ermöglicht der Betreiberin oder dem Betreiber einer Webseite die Analyse der Webseiten-Besuche durch statistisch aufbereitete Auswertungsergebnisse. Durch Analysetools lässt sich erfassen, wie Besucherinnen und Besucher auf die Webseite gekommen sind, an welcher Stelle sie die Webseite verlassen und wie lange sie sich auf der Webseite aufgehalten haben. Zudem kann Aufschluss darüber gegeben werden, aus welchen Ländern und Regionen die Besucherinnen und Besucher stammen. Durch die Auswertung der so gewonnenen Informationen soll es den Seitenbetreiberinnen und -betreibern ermöglicht werden, sich auf die Besucherinnen und Besucher und ihre Gewohnheiten einzustellen. Zur Reichweitenmessung verwendete Analysetools nutzen oft die Spuren, die die Internetnutzung im Netz hinterlässt. Diese bestehen in erster Linie aus den gesetzten Cookies, der IP-Adresse und dem "digitalen Fingerabdruck" des Browsers der Webseiten-Besucherinnen und -Besucher. Problematisch sind Analysetools, die vollständige IP-Adressen als personenbezogene Daten erfassen.

Diese Auffassung wird auch in einem Beschluss der obersten Aufsichtsbehörden für den Datenschutz des Bundes und der Länder vom 26./27. November 2009 bestätigt (siehe Abdruck im Anhang). In dem Beschluss wurde darauf hingewiesen, dass die Vorschriften des Telemediengesetzes (TMG) und des Bundesdatenschutzgesetzes zu beachten sind und danach Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden dürfen. Zudem wurden die weiteren Anforderungen verdeutlicht, die nach dem TMG erforderlich sind, und es wurde klargestellt, dass die IP-Adresse kein Pseudonym im Sinne des Telemediengesetzes ist.

- ➡ Insgesamt ist die Anwendung von Analysetools unzulässig, wenn in diesem Zusammenhang ohne vorherige Einwilligung der Betroffenen personenbezogene

Daten erhoben werden, die diese identifizieren können. Auf einer Vielzahl von Internetseiten werden nicht nur Informationen abgerufen, sondern auch Zusatzdienste angeboten, die die Bekanntgabe weiterer personenbezogener oder personenbeziehbarer Daten erfordern. Die Summe dieser Informationen eignet sich besonders für die Erstellung personalisierter Nutzungsprofile.

➡ Soweit möglich, empfiehlt sich daher, beim Surfen im Internet das Setzen von Cookies und das Laden von Scripten zu unterbinden. Dies kann durch diverse Einstellungsmöglichkeiten der unterschiedlichsten Browsertypen von jeder Internetnutzerin und jedem Internetnutzer selbst vorgenommen werden. Ausführliche Hinweise zur Einstellung von Browsern können auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik unter "www.bsi-fuer-buerger.de" abgerufen werden.

15.2 Cloud Computing – Datenschutz in der Wolke?

Der Begriff "Cloud Computing" ist in aller Munde. Ob es sich nur um eine vorübergehende Erscheinung handelt oder um eine IT-Revolution, vergleichbar mit der Erfindung des Personalcomputers oder des Internets, wird die Zukunft zeigen. Noch ist nicht absehbar, in welche Richtung sich Cloud Computing entwickeln wird. Aufgrund der Komplexität und der noch weitgehenden Unbestimmtheit dieser Form der Datenverarbeitung nur einige Hinweise:

- **Was ist Cloud Computing?**

Es gibt keine einheitliche oder gar standardisierte Definition. Grundsätzlich erlaubt Cloud Computing die Bereitstellung von IT-Infrastruktur, Plattformen und Anwendungen aller Art in Form von Diensten, die über das Web "on demand" bedarfsgerecht und flexibel zur Verfügung gestellt und nach ihrer tatsächlichen Nutzung abgerechnet werden.

Bildlich gesprochen bietet Cloud Computing die Möglichkeit, IT-Dienstleistungen wie Strom aus der Steckdose zu beziehen. Man be-

nötigt keine eigene IT-Infrastruktur (keinen eigenen Stromgenerator) mehr, sondern bezieht die benötigten IT-Dienste (Strom) von einem Cloud-Anbieter (Stromversorgungsunternehmen).

Letztlich ist Cloud Computing in den verschiedensten Formen und Ausprägungen denkbar.

- **Materiell-rechtliche Aspekte:**

Für die Verarbeitung personenbezogener Daten in der Cloud, wenn sie nicht auf den eigenen Systemen der für die Datenverarbeitung verantwortlichen Stelle durchgeführt wird, müssen die Anforderungen einer Datenverarbeitung im Auftrag (§ 11 Bundesdatenschutzgesetz, § 11 Datenschutzgesetz Nordrhein-Westfalen) erfüllt sein. Außerhalb des europäischen Wirtschaftsraumes (EWR) muss zusätzlich eine Rechtsgrundlage für die Datenübermittlung an den Auftragnehmer vorliegen. Der Auftraggeber einer Auftragsdatenverarbeitung bleibt verantwortliche Stelle und ist für die Einhaltung der Vorschriften des Datenschutzes verantwortlich. Er ist und bleibt damit Herr des Verfahrens. Unternehmen, die Cloud-Dienste anbieten, erfüllen als Auftragnehmer nur reine Hilfs- und Unterstützungsfunktionen nach den Vorgaben der verantwortlichen Stelle, ohne eigenen Spielraum.

Hier liegt aber das Problem. Eine rechtskonforme Ausgestaltung einer Auftragsdatenverarbeitung und deren Umsetzung in der Praxis können sich als schwierig erweisen, weil die Anforderungen der Auftragsdatenverarbeitung im Grundsatz einen Widerspruch zur Philosophie des Cloud Computing darstellen. Um in dem oben angeführten Bild zu bleiben, ist für die Nutzerinnen und Nutzer von Cloud-Diensten alles hinter der Steckdose "in der Wolke". Sie wissen nicht, wie und wo die Datenverarbeitung in der Cloud abläuft und haben auch keinen oder nur beschränkten Einfluss darauf. Der Auftraggeber ist aber verpflichtet, einen Auftragsverarbeiter auszuwählen, der hinsichtlich der technischen und organisatorischen Sicherungsmaßnahmen eine hinreichende Gewähr bietet. Als für die Datenverarbeitung verantwortliche Stelle hat er sich von der Einhaltung der Maßnahmen zu überzeugen. Kommerzielle Angebote von Cloud-Diensten stammen allerdings zumeist von international agierenden Unternehmen, die mehrere grenzüberschreitend verteilte Rechenzentren betreiben. Daten und Anwendungen können redundant (als Kopien) auf mehrere Standorte verteilt und von einem Rechenzentrum auf ein anderes verschoben werden. Die

Ortsgebundenheit der Datenverarbeitung ist in der Cloud nicht mehr gegeben. Dem Auftraggeber ist die Ausübung seiner Kontrollpflichten und -rechte in vielen Fällen dadurch faktisch nicht möglich.

- **Aspekte der Datensicherheit:**

Auch beim Cloud Computing sind natürlich die Vertraulichkeit, Integrität und Verfügbarkeit sowie die Authentizität und Revisionssicherheit zu gewährleisten.

Die Sicherstellung der Vertraulichkeit ist von großer Bedeutung, weil die verantwortliche Stelle ihre Daten aus der Hand gibt. Sollen sensible personenbezogene Daten, insbesondere Daten, die einem Berufs- oder Amtsgeheimnis unterliegen, in der Cloud verarbeitet werden, ist die Datenverschlüsselung unabdingbar.

Durch Virtualisierung, Ressourcenteilung und einen hohen Verteilungs- und Redundanzgrad in Cloud-Umgebungen besteht die Gefahr, dass eine Vermengung von Daten, Diensten und deren Kundenzuordnung eintritt. Dadurch würde die Authentizität bedroht, die eine eindeutige Zuordnung von Daten, Prozessen und den auslösenden Nutzerinnen und Nutzern voraussetzt.

Die verantwortliche Stelle ist außerdem verpflichtet, im Nachhinein nachweisen zu können, wer welche Daten auf welche Weise verarbeitet hat. Da sie aber selbst keinen direkten Einfluss und Zugriff auf Protokollierungen hat, ist sie darauf angewiesen, dass das Unternehmen, das den Cloud-Dienst anbietet, für sie die Nachvollziehbarkeit (Revisionssicherheit) gewährleistet. Ob die Cloud-Unternehmen dies können und inwieweit die von ihnen zur Verfügung gestellten Protokollierungen als hinreichend verbindlich angesehen werden können, ist fraglich.

Einige beispielhafte Gründe, die zur Vorsicht Anlass geben:

- Es kann durchaus vorkommen, dass ein Cloud-Anbieter durch die Virtualisierung von Serverfarmen nicht weiß, auf welchem Server in welchem Land eine ganz bestimmte Datei einer Kundin oder eines Kunden liegt.
- Bisher sind alle Cloud Computing Modelle firmenspezifisch (proprietär). Damit besteht die Gefahr der Abhängigkeit von einem Unternehmen.

- Wenn ein Anbieter, aus welchen Gründen auch immer, sein Dienstangebot nicht mehr aufrechterhalten kann, ist die für die Datenverarbeitung verantwortliche Stelle möglicherweise nicht mehr in der Lage, die Datenverarbeitung selbst wieder zu übernehmen.
- Kundinnen und Kunden müssen zwangsläufig dem Cloud-Unternehmen vertrauen, weil sie keinen Einfluss auf dessen Personal haben. Insbesondere durch die Virtualisierungstechnologie ist es leicht, Daten, Anwendungen und ganze virtuelle Maschinen zu kopieren.
- Kontrollen durch die Aufsichtsbehörden für den Datenschutz werden sich in der Praxis schwierig gestalten oder sogar unmöglich werden.
- Beim grenzüberschreitenden Cloud Computing ist nicht gewährleistet, dass in allen Staaten, in denen die Datenverarbeitung stattfinden kann, ein angemessenes Datenschutzniveau besteht.
- In einer Cloud droht die Verantwortung für die konkrete Verarbeitung und für eventuelle Persönlichkeitsrechtsverletzungen hinter den grenzüberschreitenden Wolken zu verschwinden.
- Ist ein Unternehmensnetzwerk noch durch entsprechende Sicherheitsmaßnahmen gegenüber Angriffen von außen zu schützen, kann in der Cloud der Angreifer sich auf demselben Datenverarbeitungssystem befinden wie das potentielle Opfer, denn auch er kann als Kunde Cloud-Dienste anmieten.
- Insgesamt ist mit neuen Angriffsmöglichkeiten zu rechnen, die heute noch nicht absehbar sind. Ihnen wird mit noch zu entwickelnden Sicherungs- und Abschottungsmechanismen begegnet werden müssen.
- Eine Cloud – als Gesamtkonstrukt gesehen – bietet zentrale Angriffsmöglichkeiten mit ungeahnten Folgen, ähnlich dem Ausfall eines großen Stromversorgers.

➡ Datenschutz und Datensicherheit sind beim Cloud Computing in besonderer Weise zu beachten. Alle Beteiligten sind aufgerufen, gemeinsame Anstrengungen zu unternehmen, um dies sicherzustellen. Hier sind

sowohl neue technische Konzepte als auch flankierend neue gesetzliche Regelungen erforderlich.

15.3 Online-Spiele – Die Fundgrube zum Datensammeln

Neben Adresshandel, Gewinnspielen und Nutzungsanalysen bei Webseitenbesuchen gibt es leider eine weitere umfangreiche Möglichkeit, Daten über Nutzerinnen und Nutzer des Internets zu erheben und auszuwerten. Offline- und insbesondere Online-Spiele sind häufig die Grundlage für einen regen Informationsaustausch zwischen Spielerin oder Spieler und dem Unternehmen, das das Spiel hergestellt hat oder die Plattform betreibt.

Selbst bei Offline-Spielen, die in jedem Kaufhaus oder Elektrogeschäft angeboten werden, ist häufig die Registrierung beim Herstellungsunternehmen notwendig, um das gekaufte Spiel starten zu können. Im Rahmen der Registrierung sollen dann Daten wie beispielsweise Name, Anschrift, Alter, E-Mail-Adresse und Telefonnummer erhoben werden. Auch wenn bei der nun folgenden Datenerhebung auf den Zweck der Erhebung hingewiesen oder gar eine Einwilligungserklärung zur Datenerhebung und Nutzung eingefordert wird, ist es für die Käuferin oder der Käufer zu diesem Zeitpunkt oft zu spät. Das Geld für die Anschaffung des Offline-Spiels ist bereits entrichtet. Käuferinnen und Käufer sollten schon vor dem Kauf darauf hingewiesen werden, dass das Spielen nur unter bestimmten Voraussetzungen möglich ist.

Bei Online-Spielen geht die Datenerhebung dann noch um ein Vielfaches weiter. Hier werden häufig neben den Registrierungsdaten auch noch ein Pseudonym und ein Passwort erstellt, um den Zugang zum Spiel zu gewährleisten. Bei kostenpflichtigen Spielen kommen Bankverbindungsdaten hinzu. Problematisch ist, dass manche Angebote auch noch weit über das eigentliche Spielen hinaus gehen. Ähnlich wie bei sozialen Netzwerken werden Zusatzdienste wie Freundeslisten, Adressbücher, Nachrichtenübermittlung oder die Erstellung eines weitreichenden Profils angeboten, worin Angaben wie Größe, Augenfarbe, Hobbys und Ähnliches gemacht werden können. Nicht zu vergessen sind solche Daten, die der Internetbrowser der Nutzerinnen und Nutzer standardmäßig übermittelt. Hierzu gehören beispielsweise die IP-Adresse, das genutzte Betriebssystem, der Browsertyp, Datum

und Uhrzeit sowie die zuvor besuchte Internetadresse. Schon mit diesen Daten und Informationen können sehr gut Profile erstellt und für Werbezwecke genutzt werden.

Um zu gewinnen, setzen Spielerinnen und Spieler auch unfaire Mittel ein. Mit Hilfe sogenannter Cheatprogramme können Spielsituationen künstlich geschaffen oder sogar Spielstände manipuliert werden. Diese Tatsache wiederum hat Unternehmen motiviert, eine Software zu entwickeln, mittels derer solche betrügerischen Einsatzmittel aufgedeckt werden können. Die Folge dabei ist, dass die ehrlichen Spielerinnen und Spielereiner Spionage auf ihrem Rechner zustimmen müssen, um zu den jeweiligen Spielen zugelassen zu werden. Diese Tools, die eigentlich einen Betrug im Spiel verhindern sollen, können Systemprozesse auslesen und Informationen hieraus an das Unternehmen übertragen, das die Plattform betreibt. Dies geschieht häufig, ohne dass die Spielerinnen und Spieler sich dessen bewusst sind. Formgerechte Einwilligungen, wie sie das Gesetz vorschreibt, liegen in der Regel nicht vor. Vielmehr beschränken sich die Unternehmen darauf, lediglich diesbezügliche Hinweise in den Teilnahme- bzw. Nutzungsbedingungen oder in den Allgemeinen Geschäftsbedingungen zu geben. Dies ersetzt jedoch nicht eine erforderliche Einwilligung. Problematisch ist zudem, dass auf den Datenschutz gerichtete Regelungen häufig geändert werden und somit für die Spielerinnen und Spieler überraschend sind oder dass diese aufgrund ihres Alters nicht die erforderliche Einsichtsfähigkeit besitzen, um die Gefahren beurteilen zu können.

Die Regelungen und Bedingungen mancher großer Spieleplattformen sind für Benutzerinnen und Benutzer völlig unübersichtlich. Erschwerend kommt hinzu, dass sie in Teilen in fremder Sprache verfasst werden, so dass selbst durchschnittliche volljährige Nutzerinnen und Nutzer kaum in der Lage ist, die dort beschrieben komplexen Datenverabeitungsprozesse zu verstehen.

- Auch wenn die größten Spieleplattformen im Ausland betrieben werden und nicht meiner Aufsicht unterliegen, konnte festgestellt werden, dass Daten oft ohne Rechtsgrundlage verarbeitet werden, anonyme Nutzung nicht ermöglicht wird und viele Vorgänge für die Spielerinnen und Spieler intransparent sind. Aufgrund der Masse der Angebote droht zudem die Gefahr, selbst den Überblick über die Verwendung und Nut-

zung der eigenen personenbezogenen Daten zu verlieren. Ich empfehle deshalb, sich vor dem Kauf oder vor einer Registrierung umfassend über die datenschutzrechtlichen Regelungen zu informieren. Dies gilt insbesondere, wenn es um die Nutzung von Spielen durch Kinder und Jugendliche geht.

15.4 Neuordnung der Rundfunkfinanzierung – 15. Rundfunkänderungsstaatsvertrag

Durch den 15. Rundfunkänderungsstaatsvertrag soll eine grundlegende Neuordnung der Finanzierung des öffentlich-rechtlichen Rundfunks vollzogen werden. Anstelle der bisherigen gerätebezogenen Abgabe soll ab 2013 ein wohnungs- bzw. betriebsbezogener Pauschalbeitrag treten. Ziel des Systemwechsels ist eine Vereinfachung des Verfahrens zur Beitragserhebung. Dabei ist zu befürchten, dass die Chance verpasst wird, die Befugnisse beim Beitragseinzug datenschutzrechtlich zu begrenzen und die Grundsätze der Direkterhebung, der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Stattdessen sieht der Staatsvertragsentwurf massive Eingriffe in das informationelle Selbstbestimmungsrecht großer Teile der Bevölkerung vor. Die bestehenden Datenerhebungsbefugnisse der Landesrundfunkanstalten und der von ihr beauftragten Gebühreneinzugszentrale (GEZ) werden beibehalten und sogar durch eine Vielzahl zusätzlicher Befugnisse noch erweitert.

Der Staatsvertragsentwurf sieht unter anderem die einmalige pauschale Übermittlung der Daten aller volljährigen Personen durch die Meldebehörden über einen Zeitraum von zwei Jahren vor. Dies verwundert im Hinblick darauf, dass die GEZ ohnehin schon regelmäßig – etwa bei Ein- und Auszug der Beitragsschuldnerinnen und -schuldner – eine nicht unerhebliche Anzahl Meldedaten erhält.

Hinzu kommt, dass es weiterhin gestattet sein wird, Daten ohne Kenntnis der Betroffenen bei privaten Quellen, zum Beispiel bei Adresshandelsunternehmen und Auskunfteien, zu erheben. Da die Rundfunkanstalten bzw. die GEZ keine Möglichkeit haben, die Qualität der so gewonnenen Daten zu überprüfen, besteht ein enormes Risiko, mit nicht mehr aktuellen oder aus anderen Gründen falschen Daten zu

arbeiten. Dies hat sich schon in der Vergangenheit als problematisch erwiesen. So wurden etwa Haustiere oder Minderjährige mit Gebührenbescheiden konfrontiert.

Nicht akzeptabel ist auch, dass Beitragsschuldnerinnen und -schuldner die Aufgabe einer Wohnung nicht nur anzeigen, sondern auch begründen sollen. Es ist für die Beitragserhebung aber ohne jede Bedeutung, aus welchen persönlichen Gründen eine Wohnung aufgegeben wird. Für den Abmeldevorgang reicht die Mitteilung aus, dass die Wohnung verlassen wird.

Nicht hinnehmbar ist im Übrigen die von der GEZ verfolgte Praxis bei der Beitragsbefreiung aus sozialen Gründen. Die GEZ scannt ihre gesamte Eingangspost, also auch vollständige und nicht geschwärzte Sozialbescheide, weil eine teilweise Erfassung der Bescheide angeblich nicht möglich sein soll. Dies hat zur Folge, dass auch sensible Gesundheits- bzw. Sozialdaten gespeichert werden, obwohl sie für die Entscheidung zur Beitragsbefreiung nicht erforderlich sind.

Dem Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder wurde zwar bezüglich der beabsichtigten Regelungen frühzeitig Gelegenheit zur Stellungnahme gegeben. Jedoch sind die von meinen Kolleginnen und Kollegen und von mir geäußerten datenschutzrechtlichen Bedenken überwiegend nicht ausgeräumt worden (siehe Entschließung der Datenschutzkonferenz vom 11. Oktober 2010 im Anhang).

➡ Der Staatsvertragsentwurf muss nachgebessert werden. Das weitere Verfahren werde ich kritisch begleiten.

16 Informationsfreiheit

16.1 Sind Kooperationsverträge zwischen Hochschulen und der Industrie offenzulegen?

In Zeiten knapper finanzieller Ressourcen sind viele Universitäten bestrebt, Drittmittel einzuwerben. Eine Ausgestaltung solcher Verbindungen stellen Kooperationsvereinbarungen zwischen Wirtschaft und Hochschulen dar.

Meine Behörde hatte zu prüfen, ob ein zwischen einer Hochschule und einem Pharmaunternehmen geschlossener Kooperationsvertrag offenzulegen ist. Die Universität beruft sich zur Ablehnung des Antrages auf die Regelung des § 2 Abs. 3 Informationsfreiheitsgesetz Nordrhein-Westfalen, nach der Hochschulen diesem Gesetz nur unterworfen sind, soweit sie nicht im Bereich von Forschung, Lehre, Leistungsbeurteilung und Prüfungen tätig werden. Nach Ansicht der Universität unterfällt der Kooperationsvertrag dem Begriff der Forschung ; das Pharmaunternehmen macht geltend, dass der Vertrag ein Betriebs- und Geschäftsgeheimnis des Unternehmens darstelle. Nach Prüfung der Kooperationsvereinbarung ist meine Behörde zu dem Ergebnis gelangt, dass das dort Geregelte weder Forschung oder Wissenschaft betrifft noch die Vereinbarung insgesamt ein Betriebs- oder Geschäftsgeheimnis des Pharmaunternehmens darstellt. Ob ggf. einzelne Regelungen ein Betriebs- oder Geschäftsgeheimnis beinhalten könnten, konnte aufgrund des diesbezüglich nicht substantiierten Vortrags nicht festgestellt werden.

Trotz der Empfehlung, den Kooperationsvertrag offenzulegen, lehnt es die Universität weiterhin generell ab, den Informationszugang zu gewähren. Die Entscheidung, ob der Antragsteller nun den Klageweg beschreiten will, bleibt ihm vorbehalten.

- Verträge der öffentlichen Hand gehören so weitgehend wie möglich in die Öffentlichkeit, damit die Bürgerinnen und Bürger sich über die Verwendung öffentlicher Gelder und darüber informieren können, ob und in wieweit Vereinbarungen Auswirkungen auf den Aufgabenvollzug der öffentlichen Hand haben.

16.2 Vorreiter NRW: Die Neuregelung im WDR-Gesetz stärkt das Informationszugangsrecht

Der Landtag stellt klar: Das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) findet auf den WDR Anwendung, es sei denn, es sind journalistisch-redaktionelle Informationen betroffen.

Während sich der WDR immer noch weigert, Unterlagen über Aufträge herauszugeben, die an private Unternehmen vergeben wurden (siehe Bericht 2009 unter Ziffer 17.3 zur Klage eines Informationssuchenden gegen den WDR), wurde durch den Landtag NRW zwischenzeitlich eine Neufassung des WDR-Gesetzes verabschiedet. Der Gesetzgeber hat in § 55a ausdrücklich klargestellt, dass der WDR grundsätzlich dem IFG NRW unterfällt, was der WDR unter Verweis auf die grundgesetzlich verbürgte Rundfunk- und Pressefreiheit stets bestritten hatte. Nach der Gesetzesbegründung sollen von der Informationspflicht lediglich diejenigen Informationen ausgeschlossen werden, die dem Kernbereich der journalistisch-redaktionellen Arbeit und dem verfassungsrechtlich geschützten Bereich der Programmgestaltung zuzuordnen sind. Es bleibt abzuwarten, wie sich die neue Rechtslage auf den Ausgang des oben genannten Klageverfahrens gegen den WDR auswirkt, das mittlerweile beim Oberverwaltungsgericht Nordrhein-Westfalen anhängig ist.

➡ Mit dieser informationszugangsfreundlichen Gesetzeslage hat NRW eine klare Vorreiterrolle im Bundesgebiet eingenommen.

16.3 Informationsverweigerung trotz eindeutiger Rechtslage und Beanstandung

Eine Stadt gewährt einem Antragsteller keine Einsicht in ein Gutachten zu einem umstrittenen Stadtbahnbauprojekt. Die Verweigerung der Stadt wurde bereits in einem ähnlich gelagerten Fall durch das Oberverwaltungsgericht Nordrhein-Westfalen als rechtswidrig beurteilt.

Ein Antragsteller hatte bei einer Stadt Einsicht in ein extern erstelltes Gutachten zu einem geplanten Stadtbahnbauprojekt beantragt. Bei

dieser sogenannten "Standardisierten Bewertung" handelt es sich um die Begutachtung des volkswirtschaftlichen Nutzens des Verkehrsprojektes.

Die Stadt trug zur Ablehnung vor, das Gutachten stelle das wesentliche Instrument für die Willensbildung zwischen ihr und den weiteren Zuwendungsgebern dar. Dieser Willensbildungsprozess sei noch nicht abgeschlossen. Die dem Gutachten zugrunde liegenden Parameter müssten zwischen den Zuwendungsgebern erst noch beraten werden. Meine Behörde ließ sich daraufhin das Gutachten von der Stadt zur informationsfreiheitlichen Bewertung übersenden und stellte fest, dass es in sich abgeschlossen und nicht mehr im Entstehungsprozess befindlich ist. Sollten dem Gutachten tatsächlich zukünftig andere Parameter zu Grunde gelegt werden müssen, dürfte ein gänzlich neues, zumindest aber weiteres Gutachten erstellt werden müssen. Darüber hinaus bildet das Gutachten selbst keinen Willensbildungsprozess ab. Dies wäre aber die Voraussetzung dafür, dass der Verweigerungsgrund des § 7 Abs. 2 lit. a) Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) greift. Das Oberverwaltungsgericht Nordrhein-Westfalen (Urteil vom 9. November 2006 – 8 A 1679/04 –) hatte zu diesem Verweigerungsgrund bereits entschieden, dass zwischen den Grundlagen und Ergebnissen der Willensbildung auf der einen Seite und dem eigentlichen Prozess der Willensbildung auf der anderen Seite zu unterscheiden sei. Der genannte Verweigerungsgrund greife deshalb nur für Anordnungen, Äußerungen und Hinweise, die die Willensbildung steuern sollen. Geschützt sind somit allein Unterlagen, die den Prozess der Willensbildung inhaltlich unmittelbar wiedergeben, nicht aber die dem Willensbildungsprozess zugrunde liegenden Sachinformationen.

Im Rahmen des Gutachtens wurde allein die Förderfähigkeit des Stadtbahnprojektes überprüft. Es dient der Verwaltung somit möglicherweise als Grundlage zur weiteren Willensbildung, bildet jedoch selbst keinen Willensbildungsprozess ab und unterfällt daher nicht dem genannten Verweigerungsgrund.

- Trotz entsprechender Beanstandung und Unterrichtung der Aufsichtsbehörde legte die Stadt das Gutachten bis heute nicht offen und verstößt damit fortgesetzt gegen die Regelungen des IFG NRW.

16.4 Informationszugang im Schulbereich

Eltern, aber auch die Beschäftigten der Schulbehörden sind im Umgang mit den Regelungen des Informationsfreiheitsgesetzes Nordrhein-Westfalen (IFG NRW) im Schulbereich noch immer unsicher.

Ergebnisse von Vergleichsarbeiten, zentralen Prüfungen oder des Zentralabiturs sowie die Auskunft, wie viel Geld in den letzten Jahren in die Sanierung der Schultoiletten investiert wurde – die Bandbreite an Themen für einen Antrag nach dem IFG NRW im Schulbereich scheint unerschöpflich. Hier nun einige immer wieder auftretende Problemfelder:

- **An welche Stelle ist der IFG-Antrag zu richten?**

Gemäß § 5 Abs. 1 Satz 4 IFG NRW sind Anträge zu amtlichen Informationen der Verwaltungstätigkeit von Schulen in inneren Schulangelegenheiten an die Schulaufsicht, in äußeren Schulangelegenheiten an den Schulträger zu richten (zur Unterscheidung zwischen äußeren und inneren Schulangelegenheiten siehe unter Ziffer 11.3).

Die oben aufgeführten Anfragen zu den Ergebnissen von Vergleichsarbeiten, zentralen Prüfungen oder des Zentralabiturs betreffen innere Schulangelegenheiten und sind somit an die jeweilige Schulaufsichtsbehörde zu richten. Für die Anfrage nach dem Investitionsvolumen in die Schultoiletten als äußere Schulangelegenheit ist dagegen der Schulträger zuständig.

Die jeweilige Schulaufsichtsbehörde bzw. der Schulträger – nicht etwa die jeweilige Schulleitung – ist für die inhaltliche Prüfung des Anspruchs auf Information zuständig. Sollte sich für eine Anfrage im Übrigen weder die Schulaufsicht noch der Schulträger zuständig fühlen – was auch schon vorgekommen ist –, so ist die weitere Bearbeitung des Antrags von diesen beiden Behörden untereinander abzustimmen. Einer erneuten Antragstellung bei der jeweils anderen Behörde bedarf es nicht.

- **Warum gibt es diese Regelung?**

Die Regelung soll es den Schulen ersparen, die auf sie möglicherweise zukommenden Anfragen selbst bewältigen zu müssen. Die

Zuständigkeit für die Bearbeitung von Informationszugangsanfragen wurde deshalb auf die Schulaufsichtsbehörden übertragen.

- **Was ist, wenn die begehrte Information bei der Schulaufsicht oder dem Schulträger nicht vorhanden ist?**

Diese Konstellation kommt bei Anfragen an die Schulaufsicht häufig vor. Obwohl der Zugangsanspruch grundsätzlich auf diejenigen Informationen beschränkt ist, die (bereits) bei der öffentlichen Stelle vorhanden sind, ist die Schulaufsichtsbehörde in diesem Fall verpflichtet, sich die begehrte Information von der Schule zu beschaffen.

- **Woran könnte der Informationszugangsantrag scheitern?**

Auch hier kommen grundsätzlich die im IFG NRW geregelten Verweigerungsgründe in Betracht. Die Hauptproblematik von Anfragen im Schulbereich liegt im zu gewährleistenden Schutz personenbezogener Daten. Kann sich aus einer Anfrage, ggf. auch mit entsprechendem Zusatzwissen, ein Personenbezug zu einzelnen Schülerinnen und Schülern herstellen lassen, so würde es sich um personenbezogene Daten handeln, die in der Regel nur mit entsprechender Einwilligung der Betroffenen zugänglich gemacht werden dürfen. Sind hingegen Lehrerdaten betroffen, ist der Schutz personenbezogener Daten abgeschwächt. Die Lehrkräfte müssen es als Amtsträger ggf. hinnehmen, dass bestimmte personenbezogene Angaben im Zusammenhang mit ihrer dienstlichen Tätigkeit offenzulegen sind (siehe auch unter Ziffer 16.7).

➡ Die Bearbeitung von Anträgen nach dem IFG NRW im Schulbereich macht noch immer erhebliche Probleme. Dem sollte mit dem Erlass von Anwendungshinweisen zum IFG NRW durch das zuständige Schulministerium entgegengewirkt werden.

16.5 Wichtiger Etappensieg in Sachen Cross-Border-Leasingverträge

Eine Stadt ist zur Vorlage von Unterlagen zu einem Cross-Border-Leasingvertrag verpflichtet. Das Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW) hat festgestellt, dass eine

diesbezügliche Sperrerklärung der obersten Aufsichtsbehörde rechtswidrig ist.

In einem Gerichtsverfahren klagt ein Antragsteller auf Akteneinsicht in einen US-Cross-Border-Leasingvertrag, mit welchem eine Stadt ihre Abwasseranlagen langfristig an ein US-Unternehmen vermietet und für einen kürzeren Zeitraum zurückgemietet hat, verbunden mit entsprechenden Entgeltvereinbarungen und einem Barwertvorteil für die Kommune (siehe Bericht 2005 unter Ziffer 23.3.4). Nachdem das Verwaltungsgericht die Stadt zur Vorlage der streitigen Unterlagen aufgefordert hatte, sprach die oberste Aufsichtsbehörde, hier das Innenministerium NRW, einen sogenannten Sperrvermerk aus.

Nach einer Regelung in der Verwaltungsgerichtsordnung kann die oberste Aufsichtsbehörde einem Gericht gegenüber die Vorlage von Urkunden oder Akten verweigern, wenn das Bekanntwerden des Inhalts dieser Urkunden oder Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen. In einem solchen Fall entscheidet dann das OVG NRW. Hier hatte daher das OVG NRW in einem Zwischenverfahren über die Aktenvorlagepflicht der beklagten Stadt zu entscheiden.

Nach Auffassung des OVG NRW hat das Innenministerium NRW sein Ermessen vorliegend nicht richtig ausgeübt. Das Innenministerium hatte sich im Wesentlichen darauf berufen, dass eine vertragliche Vertraulichkeitsvereinbarung und Betriebs- oder Geschäftsgeheimnisse des US-Unternehmens einer Vorlage entgegenstünden. Das OVG NRW hat nun nochmals klargestellt, dass vertragliche Vertraulichkeitsabreden keine Verweigerung einer Aktenvorlage rechtfertigten. Allein die Formulierung einer Vertraulichkeitserklärung vermöge einen Schutz vor einer Informationsübermittlung an andere Personen nicht zu begründen. Eine solche Vereinbarung könne nicht losgelöst von dem eigentlichen materiellen Inhalt des Vertragswerks, in dem sie enthalten sei, betrachtet werden, sodass ihr eine eigenständige Erheblichkeit unabhängig von den sonstigen Vertragsregelungen nicht zuerkannt werden könne. Daran ändere auch eine befürchtete Schadensersatzforderung nichts.

Ebenfalls liege kein Betriebs- oder Geschäftsgeheimnis des US-Unternehmens vor, da kein berechtigtes Interesse an der Nichtverbreitung

der Information bestehe. Die Laufzeiten von Cross-Border-Leasingverträgen von etwa 25 bis 99 Jahren schlössen aus, dass mögliche Konkurrenten einen wirtschaftlichen Nutzen aus der Kenntnis der begehrten Information ziehen könnten. Selbst wenn jedoch ein Betriebs- oder Geschäftsgeheimnis angenommen würde, würde die Abwägungsklausel des § 8 Satz 3 Informationsfreiheitsgesetz Nordrhein-Westfalen ebenfalls zu einer Offenlegung führen. Nach dieser – im Übrigen vielfach übersehenen – Regelung stehen Betriebs- oder Geschäftsgeheimnisse einem Informationszugang nicht entgegen, wenn die Allgemeinheit ein überwiegendes Interesse an der Gewährung des Informationszugangs hat und der eintretende Schaden nur geringfügig wäre. Gegenstand des Vertrags sind hier die Abwasseranlagen einer Stadt. Für die Entsorgung von Abwasser besteht nach dem Landeswassergesetz eine Beseitigungspflicht der Gemeinden. Da bei dieser Aufgabe öffentliche Gelder eingesetzt werden, besteht nach Ansicht des OVG NRW ein erhebliches öffentliches Informationsinteresse, dass die Gelder sach- und interessengerecht sowie nach anerkannten finanz- und kommunalpolitischen Grundsätzen eingesetzt werden. Einen Vorrang des Schutzes von Geschäftsgeheimnissen gebe es daher nicht. Mit dieser Argumentation bestätigt das OVG NRW die bereits im Bericht 2005 unter Ziffer 23.3.4 vertretene Rechtsauffassung. Es bleibt nun abzuwarten, wie das Gericht in der Hauptsache die vorzulegenden Akten bewertet. Die Rechtsauffassung des OVG NRW im Zwischenverfahren dürfte allerdings ein wichtiger Fingerzeig sein.

➡ Auch hier gilt, dass Verträge der öffentlichen Hand so weitgehend wie möglich öffentlich zugänglich sein sollen (siehe Ziffer 16.1.).

16.6 Das leidige Thema der Gebührenberechnung

Die Gebühren, die für einen Informationszugang erhoben werden können, sind auf maximal 1.000 Euro begrenzt. Behörden werden in zunehmender Weise kreativ, um diese Gebührenobergrenze zu unterlaufen.

Ein Antragsteller erbat von einer Gemeinde Auskunft zu deren Kalkulation der Abwassergebühren. Nachdem der Antragsteller seinen Antrag auf sechs einzelne Fragen konkretisiert hatte, stellte die Gemeinde zwar in Aussicht, diese Fragen zu beantworten, wies zugleich

aber darauf hin, dass hohe Gebühren anfallen würden. Allein die erste Frage werde aufgrund des nötigen Arbeitsaufwandes Gebühren in Höhe von 1.000 Euro auslösen. Für die folgenden Fragen würden jeweils weitere Gebühren fällig werden. Darüber hinaus sollte der Antragsteller die Gebühren im Voraus entrichten.

Das Vorgehen der Behörde ist mit dem Grundsatz des Informationsfreiheitsgesetzes Nordrhein-Westfalen, dass Gebührenerhebungen nicht abschreckend wirken dürfen, nicht vereinbar. Wird ein Antrag auf Informationszugang zu einem Thema gestellt und durch verschiedene Fragen zu diesem Thema konkretisiert, handelt es sich um einen einzigen Informationszugangsantrag. Für diesen Antrag darf nur einmal eine Gebühr erhoben werden. Gebührenvorauszahlungen sind wegen ihres grundsätzlich abschreckenden Charakters ohnehin nicht zulässig. Der Antragsteller hat sowohl zur Frage der Art und Weise der Informationsgewährung als auch zur Frage der Rechtmäßigkeit der Gebührenvorauszahlung Klagen erhoben, deren Urteile für die Zukunft Klarheit schaffen könnten.

➡ Gebühren dürfen den freien Informationszugang nicht behindern.

16.7 Veröffentlichungspflichten sind oft noch nicht erfüllt

Zahlreiche öffentliche Stellen haben die durch das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) geschaffene Verpflichtung, Geschäftsverteilungspläne, Organigramme und Aktenpläne nach Maßgabe dieses Gesetzes zu veröffentlichen, auch nach neun Jahren IFG NRW nicht umgesetzt.

Nach § 12 IFG NRW sind die öffentlichen Stellen dazu verpflichtet, ihre Geschäftsverteilungspläne, Organigramme und Aktenpläne nach Maßgabe dieses Gesetzes allgemein zugänglich zu machen. Soweit möglich hat die Veröffentlichung in elektronischer Form zu erfolgen. Die Vorschrift schreibt eine aktive Informationspolitik für die öffentlichen Stellen fest. Den Bürgerinnen und Bürgern soll ein Überblick ermöglicht werden, welche Informationen es bei welchen öffentlichen Stellen gibt; nur dann können Antragstellerinnen und Antragsteller ihre Rechte effektiv ausüben (siehe Bericht 2003 unter Ziffer 22.6 und

Ziffer 11.1). So werden anhand der genannten Übersichten Aufbau, Kommunikationsbeziehungen, Weisungsbefugnisse, Zuständigkeiten und Aufgabenwahrnehmung innerhalb einer öffentlichen Stelle erkennbar. Der zunehmende Einsatz von Informationstechnik bei den öffentlichen Stellen ist auch im Rahmen der Veröffentlichungspflichten zu nutzen, etwa durch Veröffentlichungen im Internet.

Es soll jedoch nicht nur der behördliche Aufbau transparent werden, sondern die Bürgerinnen und Bürger sollen auch wissen, wer ihre zuständigen Ansprechpersonen sind und wie sie diese dienstlich erreichen können. Welche Daten der Beschäftigten veröffentlicht werden, bestimmt § 12 IFG NRW zwar nicht selbst, doch soll die Veröffentlichung nach Maßgabe des Gesetzes, also des IFG NRW, erfolgen. § 9 Abs. 3 IFG NRW regelt, welche personenbezogenen Daten von Beschäftigten des öffentlichen Dienstes grundsätzlich zu offenbaren sind, ohne dass es hierzu einer Einwilligung der Betroffenen bedarf: Namen, Titel, akademischer Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und Rufnummer. Eine Ausnahme zu diesem Grundsatz sieht das IFG NRW allein für die seltenen Fälle vor, in denen einer Offenbarung der vorgenannten Daten schutzwürdige Belange der betroffenen Person entgegenstehen. Ich empfehle daher, vor einer Veröffentlichung der personenbezogenen Daten die Beschäftigten entsprechend zu informieren und ihnen Gelegenheit zu geben, Anhaltspunkte für entgegenstehende besondere schutzwürdige Belange vorzutragen. Die Verantwortung für die Veröffentlichung trägt die Behördenleitung.

Auch nach neun Jahren IFG NRW ist es vielfach entweder gar nicht oder nur durch aufwendige Recherche auf den Internetseiten der öffentlichen Stellen möglich, die Organisationspläne zu entdecken. Sind diese gefunden, sind die Zuständigkeiten oft so grob dargestellt (z.B. nur bis zur Referatsleitungsebene), dass die zuständige Bearbeiterin oder der zuständige Bearbeiter für eine bestimmte Sachfrage weiterhin nicht zu erkennen ist. Diese Art der Darstellung entspricht nicht dem Sinn und Zweck der Veröffentlichungspflichten des IFG NRW.

➡ Die Verpflichtung der öffentlichen Stellen, ihre Geschäftsverteilungspläne, Organigramme und Aktenpläne nach Maßgabe des IFG NRW zu veröffentlichen, wurde vielfach nicht oder nur unzureichend umgesetzt. Die Behörden sind daher aufgerufen, ihren Pflichten nunmehr nachzukommen.

Anhang

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Entschließung vom 18. Februar 2009

◆ Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!

Das Bundeskabinett hat am 14. Januar 2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (BR-Drs. 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),

2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und

3. die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor (zu erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Abs. 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstellen, dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist.

Sowohl die Betreiber der "Netze des Bundes" als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.

77. Datenschutzkonferenz am 26./27. März 2009

◆ Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.
- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u.a. zur Frage

der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)

- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z.B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.
- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z.B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.
- Der Einsatz von Überwachungssystemen, wie z.B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.
- Es bedarf der Festlegung der Rechte der Beschäftigten, z.B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.
- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.
- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.
- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

◆ Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei "Gewalttäter Sport"

bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

◆ Defizite beim Datenschutz jetzt beseitigen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

- Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.
- Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.
- Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

◆ Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die

Auskunftserteilung von einem "berechtigten Interesse" abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden es Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

Entschließung vom 16. April 2009

◆ Datenschutz beim vorgesehenen Bürgerportal unzureichend

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drs. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.
- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des

Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3.4.2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge

Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

78. Datenschutzkonferenz am 8./9. Oktober 2009

◆ Krankenhausinformationssysteme datenschutzgerecht gestalten!

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

◆ Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des

Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem "Europa der Bürger". Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z.B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.
- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.
- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.
- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden. Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST – im weiteren Verfahren einzusetzen.

◆ Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z.B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;
- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;
- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;
- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;
- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;
- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z.B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;
- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;
- die Videoüberwachung in Staat und Gesellschaft einzuschränken;
- den Schutz der Meldedaten zu verbessern;
- ein praktikables Datenschutzaudit zu schaffen;
- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

◆ "Reality-TV" – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

"Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige "Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger "Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen "Reality"-Reportagen Abstand zu nehmen.

◆ Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

◆ Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten

betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

79. Datenschutzkonferenz am 17./18. März 2010

◆ Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die

denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

◆ Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene "Evaluierung" des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

- die mit der zu evaluierenden Norm intendierten Ziele,

- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z.B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),
- die Leistung, Wirkung sowie der Erfolg und die Effizienz,
- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

◆ Körperscanner – viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z.B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche

Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

◆ Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen "besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt". Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

◆ Ein modernes Datenschutzrecht für das 21. Jahrhundert Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft

etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt

werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

◆ Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Entschließung vom 22. Juni 2010

◆ Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz "Qualität vor übereilten Regelungen" gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.
- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur "Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten" würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer

ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.

- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.
- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.
- Die im Gesetzentwurf an mehreren Stellen vorgesehene "Einwilligung" der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Entschließung vom 24. Juni 2010

◆ Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z.B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen

Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- **Vorherige Information der Arbeitnehmer**

  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- **Keine Speicherung auf Vorrat**

  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- **Verhindern des unzulässigen Datenabrufs**

  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- **Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept**

  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

Entschließung vom 11. Oktober 2010

◆ Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,
- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und
- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

80. Datenschutzkonferenz am 3./4. November 2010

◆ Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

◆ Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z.B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotential bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der

Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

◆ Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)

Sitzung vom 23./24. April 2009

◆ Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert. Letztere stellen auch darüber hinaus gehende Listen z.B. mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind.

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Abs. 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden. Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss, sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dürfen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG vorliegt.

In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg hin.

◆ Telemarketing bei NGOs

Auch die sogenannten NGOs (non governmental organization), also nichtstaatliche Organisationen die gemeinnützig oder auch als Interessenverbände tätig sind, haben in den letzten Jahren zunehmend damit begonnen, Telefonmarketing zu betreiben. Beworben werden insbesondere Personen, die schon einmal für die jeweilige NGO gespendet haben. Wenn der

Spender seine Telefonnummer in den früheren Kontakten nicht angegeben hat, wird dieses Datum mit Hilfe des Telefonbuches oder einer Telefon-CD ermittelt.

Die Aufsichtsbehörden erklären, dass auch NGOs ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu diesem Zweck ist ohne Einwilligung rechtswidrig.

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 13. Juli 2009

◆ Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sog. eBorders-Projekts die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge erfolgt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Abs. 1 Satz 1 Nr. 2

BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt.

Die Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt. Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. Oktober 2009

◆ Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.
2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:
    - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;
    - sonstige Daten über negatives Zahlungsverhalten, bei denen
        - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat
        - die Erledigung nicht länger als ein Jahr zurückliegt und – eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2. erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

Hintergrund:

Nach § 29 Absatz 2 Nr. 1a Bundesdatenschutzgesetz ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder –unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressenten erteilen dürfen. Vorzuziehen – so der damalige Beschluss – seien branchenspezi- fische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber so genannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer .2 genannten Katalog hinausgehen.

Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

Sitzung vom 26./27. November 2009

◆ Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen

können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofil genutzt werden kann.

Der beabsichtigten "Prangerwirkung" mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen "für die, die es angeht", publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

◆ Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.
- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der

Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

◆ Gesetzesänderung bei der Datenverwendung für Werbezwecke

Vom 1. September 2009 an gelten nach § 28 Abs. 3 BDSG neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden.

Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

Sitzung vom 28/29. April 2010

◆ Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. "sicheren Hafens" (Safe Harbor).[1] Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. [1]

[1] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte USUnternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Die FTC veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen USamerikanischer Unternehmen durch die Kontrollbehörden in Europa und den [2]USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifzierungungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, wann die Safe Habor-Zertifizierung des Importeurs erfolgte. Eine mehr als sieben Jahre zurückliegende Safe Habor-Zertifizierung ist nicht mehr gültig. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard- Vertragsklauseln oder bindenden Unternehmensrichtlinien zur

[2] Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

Sitzung vom 24./25. November 2010

◆ Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

◆ Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die

Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.

- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.

- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von Internetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.

- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzem sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

◆ Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden

verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB. Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4 f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein - unabhängig von der Branche und der Größe der verantwortlichen Stelle
    - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und
    - umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,
    - Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.
2. Branchenspezifisch - abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten
    - Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
    - Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
    - betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
    - Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und

- Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse **bereits zum Zeitpunkt der Bestellung** zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne lnteressenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.

2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG).Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 - 2 Jahren empfohlen.

3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.
2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Abs. 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.
3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.
4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.
5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

◆ Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste ("ePrivacy Directive") in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit "cookies" neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im

geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine "alte" Vorschrift zukünftig in "neuer", zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von "cookies" in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von "cookies" erstellt, die im "cookie" gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der "ePrivacy Directive" erfordert daher eine gesetzliche Anpassung des TMG.

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

◆ Keine weitere Einschränkung der Transparenz bei Finanzaufsichtsbehörden (26. Januar 2009)

Der Bundesrat hat im Zuge seiner Beratung des Zahlungsdiensteumsetzungsgesetzes (BT-Drs. 16/11613) vorgeschlagen, das Informationsfreiheitsgesetz des Bundes noch weiter einzuschränken: Ausgerechnet gegenüber Bundesbehörden der Finanz-, Wert-papier- und Versicherungsaufsicht soll es künftig kein Recht auf Informationszugang mehr geben. Die Entscheidung liegt jetzt beim Deutschen Bundestag.

Die Informationsfreiheitsbeauftragten in Deutschland lehnen die Schaffung einer solchen pauschalen Ausnahme entschieden ab. Es kann nicht sein, dass gerade bei den Aufsichtsbehörden, deren Tätigkeit durch die aktuelle Finanz- und Bankenkrise in die öffentliche Kritik geraten ist, die Transparenz noch weiter eingeschränkt wird. Das Vertrauen der Öffentlichkeit in die staatlichen Kontrollinstanzen sollte durch mehr Offenheit wiederhergestellt und nicht durch Einschränkung der Informationsfreiheit noch weiter erschüttert werden.

Informationen, die in diesem Bereich tatsächlich geheimhaltungsbedürftig sind, werden bereits heute durch das Informationsfreiheitsgesetz ausreichend geschützt. So müssen solche Informationen nicht offen gelegt werden, deren Bekanntwerden im jeweiligen Einzelfall nachteilige Auswirkungen auf die Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden haben kann; ohnehin sind Be-triebs- und Geschäftsgeheimnisse sowie personenbezogene Daten geschützt. Damit besteht schon gegenwärtig im Bereich der Finanzaufsicht nur eine begrenzte Transparenz. Auch die Gerichte entwickeln hier differenzierte und sachgerechte Kriterien für die Anwendung der gesetzlichen Geheimhaltungsgründe. Diese von der Rechtsprechung eingeleitete Gesetzesauslegung nun durch eine Gesetzesänderung korrigieren zu wollen und den Zugang zu Informationen der Finanzaufsichtsbehörden gänzlich auszuschließen, widerspricht Sinn und Zweck des Informationsfreiheitsgesetzes und den berechtigten Auskunftsinteressen der Bürgerinnen und Bürger. Durch die vorgeschlagene Gesetzesänderung würde sogar der Zugang zu Informationen über solche Unternehmen ausgeschlossen, die kontinuierlich gegen schwerwiegende Straftatbestände verstoßen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an den Deutschen Bundestag, eine solche Einschränkung des Informationsfreiheitsgesetzes nicht zu beschließen.

◆ Informationszugang für Bürgerinnen und Bürger verbessern! (24. Juni 2009)

Die Anwendung der Informationsfreiheitsgesetze in Bund und Ländern hat bewiesen: Der freie Zugang von Bürgerinnen und Bürgern zu Informationen öffentlicher Stellen ist auch in Deutschland fester Bestandteil der Demokratie. Seit 1998 haben nun schon elf Länder und der Bund ein allgemeines

Informationsfreiheitsgesetz erlassen. Umweltinformationsgesetze und das Verbraucherinformationsgesetz ergänzen und erweitern den freien Zugang zu Informationen in spezifischen Bereichen.

In einer Vielzahl von Fällen haben die Bürgerinnen und Bürger Zugang zu amtlichen Informationen erhalten. Die Erfahrungen zeigen aber auch, dass sie immer wieder auf unnötige Hindernisse stoßen, wenn sie ihre Informationsrechte geltend machen wollen. So ist es für alle Beteiligten, auch für die Behörden, immer wieder schwer zu bestimmen, welches Informationszugangsrecht gilt. Zudem mindern teilweise ausufernde Ablehnungsgründe die Erfolgsaussichten von Zugangsanträgen.

Die Informationsfreiheitsbeauftragten halten es deshalb zugunsten einer größeren Transparenz des Verwaltungshandelns für geboten,

- einen unkomplizierten und umfassenden Zugang zu amtlichen Informationen zu ermöglichen,
- Ausnahmen vom Informationszugang auf das unabdingbar notwendige Maß zu beschränken,
- den Informationszugang grundsätzlich kostenfrei zu gewähren,
- die Verfahren zur Rechtsdurchsetzung des Informationsanspruchs zu beschleunigen,
- Veröffentlichungspflichten als zweite Säule des Informationszugangs im Sinne einer aktiven Informationspolitik zu stärken.

Die Konferenz der Informationsfreiheitsbeauftragten Deutschlands sieht darüber hinaus die Notwendigkeit, die Bewertung des Informationsfreiheitsgesetzes des Bundes auf unabhängiger wissenschaftlicher Grundlage anzugehen.

◆ Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern (24. Juni 2009)

Beschäftigte, die Missstände und Rechtsverstöße in Behörden oder Unternehmen aufdecken (Whistleblower), sorgen dort für mehr Transparenz. Beispiele wie die Aufdeckung der sog. Gammelfleischskandale, der heimlichen Überwachung von Mitarbeiterinnen und Mitarbeitern, der Ausspähung von Telefonverbindungsdaten und der übermäßigen Erfassung von Gesundheitsdaten belegen das. Nur weil Beschäftigte betriebsinterne Vorgänge offenbarten, gelangten die Rechtsverstöße überhaupt ans Licht.

Das öffentliche Interesse an der Offenlegung von Missständen muss mit den zivil- und arbeitsrechtlichen Loyalitätspflichten der Beschäftigten gegenüber den Arbeitgeberinnen und Arbeitgebern in einen angemessenen Ausgleich gebracht werden. Transparenz kann nur erreicht und gefördert werden, wenn die Hinweisgeberinnen und Hinweisgeber keine Repressalien durch Arbeitgeberinnen und Arbeitgeber und die Kollegenschaft befürchten müssen.

Die Konferenz der Informationsfreiheitsbeauftragten fordert den Deutschen Bundestag auf, für mehr Informationsfreiheit einzutreten, indem endlich der Schutz von Whistleblowern gesetzlich festgeschrieben wird. Beschäftigte sollen keine arbeitsrechtlichen Konsequenzen befürchten müssen, nur weil sie

Rechtsverstöße im Arbeitsumfeld anzeigen. Die Konferenz bedauert, dass ein erster Schritt hierzu, nämlich mit einem neuen § 612a BGB den Informantenschutz für Beschäftigte durch ein Anzeigerecht zu regeln, nicht weiterverfolgt wurde.

Der Gesetzgeber ist auch gehalten, den Transparenzgedanken und die datenschutzrechtlichen Belange der meldenden sowie der gemeldeten Person in ein ausgewogenes Verhältnis zu bringen. Hierfür hält die Konferenz folgende Erwägungen für maßgeblich:

- Zur Wahrung der schutzwürdigen Belange der Beteiligten sind verbindliche Verfahrensregeln in Behörden und Unternehmen unerlässlich.
- Whistleblowern muss die vertrauliche Behandlung des Hinweises zugesagt werden können.
- Auch die Rechte der belasteten Person, z.B. auf Benachrichtigung, Auskunft über sowie Berichtigung und Löschung von Daten, müssen berücksichtigt werden.
- Zum Schutz der Vertraulichkeit können Beschwerden an unabhängige ggf. externe Stellen (Ombudsleute) geschickt werden, die sie nur anonymisiert weitergeben dürfen.

◆ **Regelungen zum Informationszugang der Bürgerinnen und Bürger vereinheitlichen! (16. Dezember 2009)**

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder begrüßt die Ankündigung in der Koalitionsvereinbarung der neuen Bundesregierung, die Ansprüche der Verbraucherinnen und Verbraucher auf Information in einem einheitlichen Gesetz zur Regelung der Informationsansprüche der Bürgerinnen und Bürger zusammenzufassen.

Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine Vielzahl von Einzelvorschriften verteilt: Sie finden sich insbesondere im Informationsfreiheitsgesetz, im Umweltinformationsgesetz und im Verbraucherinformationsgesetz. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Rechte der Bürgerinnen und Bürger und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei.

Bei der anstehenden Überarbeitung sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird. Die vielfältigen gesetzlichen Ausnahmetatbestände, wegen derer ein Informationszugang verweigert werden kann, gehören auf den Prüfstand.

◆ **Informationsfreiheit bei öffentlich-rechtlichen Rundfunkanstalten (24. Juni 2010)**

Die Informationsfreiheit erfasst grundsätzlich alle Formen und Bereiche öffentlich-rechtlichen Handelns. Ihr Ziel ist es, Verwaltungsvorgänge transparenter zu gestalten und den Menschen die politische Mitgestaltung zu erleichtern. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland weist deshalb darauf hin, dass das Recht auf Informationszugang auch gegenüber den öffentlich-rechtlichen Rundfunkanstalten als Trägern mittelbarer Staatsverwaltung gilt, sofern nicht deren grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit berührt ist.

Die Rundfunkfreiheit garantiert den Schutz vor staatlicher Kontrolle und Beeinflussung. Eine Öffnung aller Sendeanstalten außerhalb dieses geschützten Kernbereichs für die Informationsbelange der Bürgerinnen und Bürger gefährdet diese Freiheit nicht. Offenheit und Transparenz sind keine Bedrohungen, sondern schaffen Vertrauen in der Bevölkerung. Die Geltung der Informationsfreiheitsgesetze wird die Rundfunkanstalten daher in ihrem demokratischen Auftrag und Selbstverständnis nachhaltig stärken.

Die derzeitige Rechtslage ist aufgrund unterschiedlicher Landesgesetze uneinheitlich. Während in einigen Bundesländern die Anwendbarkeit des Informationsfreiheitsgesetzes ausdrücklich festgeschrieben oder ausgeschlossen ist, ergibt sie sich in anderen Bundesländern nur aus allgemeinen Regeln. Einige Sendeanstalten der ARD sind zudem in Ländern ansässig, in denen noch immer kein Informationsfreiheitsgesetz gilt.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb die Schaffung ausdrücklicher Rechtsvorschriften, sofern nicht schon vorhanden, nach denen die jeweiligen Informationsfreiheitsgesetze auch auf die öffentlich-rechtlichen Rundfunkanstalten außerhalb der grundrechtlich garantierten Rundfunkfreiheit anzuwenden sind.

◆ Open Data: Mehr statt weniger Transparenz! (13. Dezember 2010)

Die WikiLeaks-Debatte zeigt beispielhaft sowohl ein wachsendes Bedürfnis der internationalen Öffentlichkeit nach verbesserter Information und mehr Transparenz staatlichen Handelns als auch nach einem wirksamen rechtsstaatlichen Rahmen für den Zugang zu öffentlichen Informationen. Auch in Deutschland muss die Transparenz des politischen Handelns einen deutlich höheren Stellenwert bekommen, indem die rechtlichen und tatsächlichen Möglichkeiten zum Zugang zu staatlichen Informationen verbessert werden.

Die Informationsfreiheitsbeauftragten haben bereits vor vier Jahren die Verwaltungen aufgefordert, Informationen nicht erst auf Anfrage zu gewähren, sondern auch aus eigener Initiative im Internet zu veröffentlichen. Den Bürgerinnen und Bürgern soll damit der Zugang erleichtert und gleichzeitig der Aufwand für die öffentlichen Stellen mit der Bearbeitung von individuellen Anträgen auf Informationszugang reduziert werden.

Inzwischen ist einiges geschehen: Immer mehr Informationen, zum Beispiel über die Umwelt, Gerichtsentscheidungen, Parlamentsdokumente, amtliche Statistiken oder Vorlagen kommu-naler Vertretungen, sind im Internet frei zugänglich. Aber immer noch fehlt ein Wegweiser durch die meist dezentral veröffentlichten Informationen ebenso wie ein einheitlicher techni-scher Standard, der die Weiterverwendung der Informationen erleichtern würde.

Beispiele aus dem In- und Ausland zeigen bereits heute, dass es möglich ist, eine Vielzahl von Informationen übersichtlich und über eine einheitliche Plattform zur Verfügung zu stellen. So kann Transparenz gleichermaßen einen Beitrag zur Stärkung der Demokratie und auch zur effizienten Aufgabenwahrnehmung der Verwaltung leisten.

- **Verträge zwischen Staat und Unternehmen offen legen! (13. Dezember 2010)**

Öffentliche Stellen des Bundes, der Länder und der Kommunen bedienen sich bei der Wahrnehmung ihrer Aufgaben vielfach privater Unternehmen: von großen Firmen, die öffentliche Infrastrukturprojekte verwirklichen, bis hin zu kleinen Betrieben, die für eine Gemeinde das Dorffest arrangieren. Dabei nimmt der Umfang des Outsourcing ständig zu und umfasst auch zentrale Felder der staatlichen Daseinsvorsorge. Die wesentlichen Inhalte und Konditionen werden dabei vertraglich fixiert.

Das Interesse der Öffentlichkeit an den Inhalten solcher Verträge ist groß, die Bereitschaft der Vertragspartner, sie offen zu legen, meist gering. Bisweilen wird privaten Geschäftspartnern sogar die Vertraulichkeit der Vertragsbestimmungen ausdrücklich zugesichert, um deren Offenbarung zu vermeiden.

Von besonderem öffentlichem Interesse sind aussagekräftige Informationen über öffentliche Gelder, die für bestimmte Leistungen bezahlt wurden, ob die Leistungen mit den zuvor ausgeschriebenen Anforderungen übereinstimmen und in welcher Höhe Steuermittel dafür aufgewendet werden. Diese Angaben dienen der Haushaltstransparenz und der Verhinderung von Korruption. Transparenz bei derartigen Verträgen ist auch deshalb besonders wichtig, weil hier nicht selten langfristige Weichenstellungen getroffen werden, die auch Parlamente späterer Legislaturperioden nicht mehr ändern können. Angaben hierüber dürfen der politischen Diskussion nicht vorenthalten werden.

Die Informationsfreiheitsbeauftragten fordern deshalb, die Verträge zwischen Staat und Unternehmen grundsätzlich offen zu legen. Die pauschale Zurückweisung von auf solche Verträge gerichteten Auskunftsbegehren unter Hinweis auf Vertraulichkeitsabreden und Betriebs- und Geschäftsgeheimnisse ist nicht länger hinnehmbar. Die Konferenz hält es deshalb für zwingend geboten, den Zugang zu entsprechenden Verträgen in den Informationsfreiheitsgesetzen sicherzustellen, wie dies jüngst im Berliner Informationsfreiheitsgesetz (GVBl. Berlin 2010, Seite 358) geschehen ist.

Hinweise auf Informationsmaterial

Neben dem aktuellen Datenschutz- und Informationsfreiheitsbericht 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 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:

- "GPS, Internet und Video – Datenschutz am Arbeitsplatz" (2009)
- "Privatsphäre mit System – Datenschutz in einer vernetzten Welt" (2010)

Eine vollständige Übersicht und ein Online-Bestellformular finden Sie auf unserer Homepage unter www.ldi.nrw.de.

Sie erreichen uns auch:

- per Post: Landesbeauftragter für Datenschutz
  und Informationsfreiheit NRW
  Kavalleriestr. 2-4
  40213 Düsseldorf

- per E-Mail: poststelle@ldi.nrw.de
- per Telefon: 0221/ 38424-0