Einundzwanzigster Datenschutz- und Informationsfreiheitsbericht

des

Landesbeauftragten für Datenschutz

und Informationsfreiheit

Nordrhein-Westfalen

Ulrich Lepper

für die Zeit vom 1. Januar 2011

bis zum 31. Dezember 2012

21. 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: 21.DIB LDI NRW
ISSN: 0179–2431
Düsseldorf 2013

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

1 Überblick

In meinem letzten Bericht hatte ich Chancen und Risiken des "informationstechnischen Jahrhunderts" angesprochen. Ohne die Risiken überbetonen zu wollen, müssen wir darauf achten, nicht durch Mikrochips, Bytes und eine vernetzte Technik zunehmend fremdbestimmt zu werden. "Alleskönner" wie zum Beispiel Smartphones ermöglichen immer mehr Datenverarbeitungen im Hosentaschenformat. Einerseits erleben wir die ortsungebundene, jederzeitige Verfügbarkeit von Wissen sowie die grenzenlose Erreichbarkeit, andererseits aber auch lückenlose Kontrolle über unseren Aufenthalt, Freundeskreis und unsere Konsumgewohnheiten. Zwar spielt Eigenverantwortung eine große Rolle. Angesichts der in hohem Maße unzureichenden **Transparenz** vieler Datenverarbeitungen steht jedoch unsere Freiheit auf dem Spiel.

Dies gilt insbesondere, wenn es nicht gelingt, alle Anbieter, von denen sich einige offenbar nicht an die Anforderungen des Datenschutzes gebunden fühlen, dazu zu bringen, den Datenschutz einzuhalten. Auch für außereuropäische Anbieter von Sozialen Netzwerken, von Apps, Online-Spielen oder sonstigen Angeboten im Internet müssen **europäische Datenschutzstandards** gelten, soweit Personen in der Europäischen Union betroffen sind. Dazu zählen klar verständliche Informationen, welche Daten für welche Zwecke verarbeitet werden, sowie Auskunfts-, Berichtigungs- und Löschungsansprüche, ebenso das Verbot, biometrische Daten für Gesichtserkennungsverfahren ohne Einwilligung der Betroffenen zu verarbeiten. Aber auch Internetseitenbetreiber, die ihre Seite etwa über Social-Plug-ins, wie den "Gefälltmir"-Button von Facebook, mit einem Sozialen Netzwerk verbinden, tragen eine eigene Verantwortung dafür, dass diejenigen, die solche Seiten aufrufen, über die weitere Verarbeitung ihrer Daten durch dritte Stellen informiert und nicht ohne ihr Wissen von diesen ausgespäht werden. Auf die besondere Verantwortung der öffentlichen Stellen, die solche Seiten vorhalten, habe ich das Land und die Kommunen hingewiesen.

Selbstverpflichtungen der Internetwirtschaft, die der Bundesminister des Innern für Soziale Netzwerke angestoßen hat, dürfen nicht dazu führen, dass geltende Gesetze zur Disposition gestellt werden. Im Gegenteil: Gefragt ist ein Mehr an Datenschutz. Ich muss ganz klar feststellen, dass es trotz vielfältiger Bemühungen im Berichtszeitraum

nicht gelungen ist, mit einigen "Playern" zu konstruktiven Lösungen zu kommen. Ebenso enttäuschend sind die Gespräche auf Bundesebene zur Selbstregulierung; hier sind wir im Berichtszeitraum keinen Schritt vorangekommen. Ich habe den Eindruck, dass angesichts der Reformberatungen zum Europäischen Datenschutz auf Zeit gespielt wird, um in Brüssel eine Herabsetzung nationaler Datenschutzstandards zu erreichen.

Geht es nach Vorstellungen in der Wirtschaft, aber auch in vielen Bereichen der öffentlichen Hand, sollen Daten zukünftig verstärkt in der sogenannten **Cloud** verarbeitet werden. Dies spart eigene Ressourcen und bietet die Möglichkeit, von jedem Ort aus mit unterschiedlichen Endgeräten, ob mit Tablet-PCs, Smartphones oder mit großen Rechnern, auf die ausgelagerten Daten zuzugreifen. Nutzerinnen und Nutzer sind in der Regel allerdings überfordert, wenn es darum geht, Zuverlässigkeit und Sicherheit der Angebote zu beurteilen. Nach wie vor sind die Bedingungen insbesondere beim grenzüberschreitenden Datentransfer völlig unklar. Die Euphorie, die diesem Geschäftsmodell entgegengebracht wird, kann ich nicht teilen. In einer Arbeitsgruppe im Rahmen des vom Bundesminister für Wirtschaft und Technologie gestarteten Projekts "Trusted Cloud" habe ich mitgewirkt und gemeinsam mit Expertinnen und Experten Vorschläge erarbeitet, um Chancen des Cloud Computing nutzen zu können, ohne Einbußen für den Datenschutz und die IT-Sicherheit in Kauf nehmen zu müssen. Diese Vorschläge können allerdings nur ein erster Schritt sein.

Der verantwortungsbewusste Umgang mit den eigenen Daten und den Daten anderer ist bei alledem unverzichtbar. Eine moderne Informations- und Kommunikationsgesellschaft ist ohne **Medienkompetenz** nicht vorstellbar. Ich bin mir bewusst, dass die Vermittlung von Medienkompetenz schon bei jungen Menschen eine Mammutaufgabe ist und nicht allein von staatlicher Seite geleistet werden kann. In Nordrhein-Westfalen gibt es zahlreiche Einrichtungen und Initiativen, nicht zuletzt im Schulbereich. Der Landtag hat mit dem Tag der Medienkompetenz ein wichtiges Signal gesetzt. Dort hatte ich Gelegenheit, den Stellenwert des Datenschutzes im Rahmen der Medienkompetenz zu erläutern.

Über meine Homepage, in Newslettern und in den Datenschutzberichten gebe ich Hinweise sowohl zur Anwendung der Datenschutzgesetze als auch zum Selbstdatenschutz. In Bezug auf Aktivitäten der Lan-

desregierung sehe ich meine Aufgabe im Wesentlichen darin, Anregungen, Empfehlungen, Vorschläge oder Mithilfe in sonstiger Form als Angebot zur Verfügung zu stellen, ohne neben oder anstelle der Landesregierung in Bereichen tätig zu sein, in denen diese entweder bereits aktiv oder in erster Linie gefragt ist. Ich begrüße, dass der Landtag mich in diesem Sinne unterstützt.

Die Vermittlung von Datenschutz- und Medienkompetenz ist nur die eine Seite der Medaille. Wichtig ist ebenso die **Sensibilisierung** der Wirtschaft im Umgang mit dem Recht auf informationelle Selbstbestimmung.

Während ich einerseits gegen ein Unternehmen mit einem Bußgeld von 60.000 Euro vorgehen musste, habe ich andererseits aus meinen zahlreichen Gesprächen mit Vertreterinnen und Vertretern aus Wirtschaft und Verbänden deutlich den Wunsch wahrgenommen, durch **Auditierung** mehr Sicherheit für den datenschutzgerechten Umgang mit Daten zu bekommen. Selbstkreierte Audits ohne Rückkoppelung mit den Datenschutzbehörden helfen nicht weiter. Ob mit einem Audit auch ein Mehr an Datenschutz erreicht werden kann, soll die Praxis zeigen. Ein Audit, das verlässlich bestehende Datenschutzanforderungen spezifiziert und als ein aus eigenem Antrieb veranlasstes Vorgehen flächendeckend zu einer Überprüfung von vor Ort ergriffenen Datenschutzmaßnahmen zu führen vermag, wäre in jedem Fall ein Fortschritt für den Datenschutz. Ich habe bereits erste Überlegungen, wie ein Modell aussehen könnte, angestellt. Dem Wunsch des Landtags folgend möchte ich eine Landesdatenschutzkonferenz unter anderem mit Vertreterinnen und Vertretern aus Wirtschaft und Behörden einberufen, um einen breiten Diskussionsprozess einzuleiten.

Für den **öffentlichen Bereich** hat es verschiedene herausragende Diskussionen im Berichtszeitraum gegeben, beispielsweise im Zusammenhang mit dem neuen **Melderecht**. Die lebhafte Diskussion, zu der ich an dieser Stelle nichts mehr hinzuzufügen brauche, ist nunmehr zu einem Abschluss gekommen. Ein **Beschäftigtendatenschutzgesetz** ist bis zum heutigen Tage nicht verabschiedet worden.

Auf zwei Bereiche möchte ich allerdings besonders eingehen: Die schrecklichen Verbrechen rechtsextremistischer Täter haben eine Diskussion ausgelöst, in der auch Datenschutzstandards in Frage gestellt werden. Beinahe reflexartig gehen Vorschläge in die Richtung, den Si-

cherheitsbehörden weitere Datenverarbeitungsbefugnisse einzuräumen. Ein derartiges Vorgehen ist entschieden zurückzuweisen. Zunächst sind die Befugnisse, der Zuschnitt und die Zusammenarbeit der Sicherheitsbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden. Für mich ist besonders wichtig, dass bei einer **Reform im Bereich der Inneren Sicherheit** der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot zwischen Polizei und Nachrichtendiensten, die informationelle Gewaltenteilung im Bundesstaat und eine effektive rechtsstaatliche Kontrolle der Nachrichtendienste gewährleistet werden.

Die Aggressivität von gewaltbereiten Tätern sowie die Sorge vor terroristisch motivierten Anschlägen haben Forderungen nach einer Ausweitung der Videoüberwachung im öffentlichen Raum laut werden lassen. Einer flächendeckenden **Videoüberwachung**, die nicht nach Gefahrenschwerpunkten und der Eignung solcher Maßnahmen unterscheidet, ist allerdings eine klare Absage zu erteilen. Unsere Werteordnung setzt voraus, dass wir uns frei und ungezwungen bewegen können. Zu dieser Freiheit gehört, nicht ungewollt zum Gegenstand einer wie auch immer gearteten Überwachung zu werden - egal, durch wen. Abstrakte Gefährdungen können nicht Anlass für eine dann noch gleichsam flächendeckende Vorratsdatenspeicherung in Deutschland sein. Videoüberwachung wird oft als Allheilmittel gesehen, kann aber die Erwartungen, die Sicherheit für die Bürgerinnen und Bürger zu erhöhen, vielfach nicht erfüllen. Sie muss auf das unumgänglich Notwendige begrenzt bleiben. In ganz besonderem Maße gilt dies für über die einfache Videoüberwachung hinausgehende Verfahren, bei denen auf der Grundlage typisiert programmierter Verhaltensschemata bereits von der Norm abweichende Bewegungsabläufe und Verhaltensmuster als Verdachtsfall erkannt werden. Mit Hilfe von Erkennungssoftware und weiteren verfügbaren Daten können ins Visier geratene Bürgerinnen und Bürger "durchleuchtet" werden. Mir ist nicht bekannt, ob diese Verfahren im Einsatz sind; die EU lässt hierzu aber bereits forschen.

Zugriffe des Staates auf private Rechner mit der Zielrichtung, dort Nachrichten- und Gesprächsinhalteinhalte, die dem Schutz des Telekommunikationsgeheimnisses unterliegen, im Rahmen der

sogenannten **Quellen-Telekommunikationsüberwachung** zu erfassen, sind mit erheblichen Gefahren für die Freiheit verbunden und dürfen, wie das Bundesverfassungsgericht entschieden hat, nur unter ganz engen Voraussetzungen, z.B. bei besonders schwerwiegenden Straftaten, in Betracht gezogen werden. Bereits mit Blick auf die kaum eingrenzbaren technischen Möglichkeiten zur Ausforschung von Rechnern müssen Überwachungen wenigstens so gestaltet werden, dass sie nicht lediglich von unabhängigen Stellen angeordnet werden, sondern auch die rechtmäßige Durchführung mittels wirksamer verfahrensbegleitender Kontrollen durch unabhängige Stellen sichergestellt ist.

Erleichtert bin ich, dass sich Schulverwaltungen, nicht nur in Nordrhein-Westfalen, von der Idee verabschiedet haben, in der Schule für schulinterne Zwecke hergestellte Druckwerke mit Hilfe von sogenannten **"Schultrojanern"** automatisiert mit dem Ziel abgleichen zu lassen, ob Urheberrechte Dritter verletzt sind. Bei allem Verständnis für die Wahrung des Rechts am geistigen Eigentum lehne ich derartige Verdachtsschöpfungsmaßnahmen ab und kann sie mir im Übrigen in einem pädagogischen Kontext kaum vorstellen. Bereits Stichworte wären in einem solchen Verfahren geeignet, einen ersten Verdacht auszulösen. Außerdem vermag ich eine Rechtsgrundlage für einen solchen Abgleich nicht zu erkennen.

Von zentraler Bedeutung für den Datenschutz sind die Vorschläge der EU-Kommission zur Reform des **Europäischen Datenschutzrechts** vom 25. Januar 2012. Sie enthalten weitreichende Änderungen für den Datenschutz in Europa. Unmittelbar betroffen ist der Datenschutz auch in Nordrhein-Westfalen. Die geplanten Regelungen betreffen nicht nur das allgemeine Datenschutzrecht, sondern je nach Ausgestaltung alle Fachgesetze, die datenschutzrechtliche Spezialregelungen enthalten. In der praktischen Anwendung berühren sie letztlich alle Bereiche, in denen personenbezogene Daten verarbeitet werden, sowohl die Datenverarbeitung von Unternehmen als auch jene von Behörden.

Insbesondere das Internet kennt keine Grenzen. Daher ist es wichtig, verbindliche Regeln für den Umgang mit personenbezogenen Daten zu entwickeln, die in Deutschland genauso gelten wie in Italien, Spanien oder Irland. Aber auch bei einer Datenverarbeitung außerhalb Europas mit Auswirkungen auf Bürgerinnen und Bürger in der Europäischen Union muss das Recht einer jeden Person auf informationelle Selbstbestimmung über ihre Daten Beachtung finden. Diesen Ansatz und eine

Reihe anderer Vorschläge begrüße ich und setze mich dafür ein, sie weiter zu verfolgen. Die Vorschläge bedürfen jedoch insgesamt einer gründlichen Überarbeitung. Ein hohes Datenschutzniveau sowie eine funktionierende Kontrolle durch die Datenschutzbehörden in den Mitgliedstaaten, die die Unabhängigkeit der Datenschutzbeauftragten wahrt, sind für mich dabei unverzichtbar. Zu den Chancen und Risiken der Brüsseler Reformüberlegungen habe ich den Landtag und die Landesregierung in schriftlichen Stellungnahmen unterrichtet. Ich begrüße, dass der Landtag das Thema aufgegriffen hat und eine transparente, sachliche und präzise Kommunikation im Reformprozess fordert. So wie von der Kommission vorgeschlagen, kann eine europäische Lösung jedenfalls nicht aussehen.

Im Jahr 2012 konnten wir auf zehn Jahre Informationsfreiheitsgesetz in Nordrhein-Westfalen zurückblicken. **Informationsfreiheit** rückt zunehmend in das Bewusstsein der Öffentlichkeit. Die öffentlichen Stellen haben im Laufe der Jahre Erfahrungen sammeln können; der Anspruch der Bürgerinnen und Bürger auf freien Zugang zu den bei den öffentlichen Stellen vorhandenen Informationen findet zunehmend Beachtung. Allerdings gibt es nach wie vor eine Reihe von Fällen, in denen den Bürgerinnen und Bürgern erst mit meiner Hilfe Zugang zu den nachgefragten Informationen gewährt wird.

Die mit der Landtagsinitiative "**Open Government** Strategie für Nordrhein-Westfalen vorantreiben" eingeleitete Diskussion zu mehr Transparenz öffentlichen Handelns kann ich aus Sicht der Informationsfreiheit nur begrüßen. Unter dem Begriff "Open Data" geht es darum, bereits von Amts wegen Informationen bereitzustellen, ohne dass es eines Antrages bedarf. Es ist nunmehr an der Zeit, die Informationsfreiheit auf der Grundlage der gewonnenen Erfahrungen weiterzuentwickeln.

Mit dem Gesetz über die **Unabhängigkeit** des Landesbeauftragten für Datenschutz und Informationsfreiheit vom 5. Juli 2011 hat der Landtag die Entscheidung des Europäischen Gerichtshofs (EuGH) vom 9. März 2010 zur vollständigen Unabhängigkeit der Datenschutzaufsicht, also auch im Hinblick auf die Kontrolle im nicht-öffentlichen Bereich, umgesetzt. Während nach dem Datenschutzgesetz Nordrhein-Westfalen die Datenschutzkontrolle im öffentlichen Bereich schon immer unabhängig war, standen dem Ministerium für Inneres und Kommunales NRW in Bezug auf den nicht-öffentlichen Bereich noch Weisungsbefug-

nisse zu. Diese Befugnisse hat der Gesetzgeber aufgehoben und zugleich die bislang vorhandene organisationsrechtliche Angliederung an das Ministerium aufgegeben. Die völlige Unabhängigkeit wird organisatorisch durch die Einordnung meiner Behörde als "verselbständigte Landesbehörde eigener Art" unterstrichen. Zugleich ist mir die Eigenschaft einer obersten Dienstbehörde und damit die gesamte Personalverantwortung für die Beschäftigten meiner Behörde übertragen worden. Haushaltstechnisch wird meine Behörde nicht mehr im Einzelplan des Ministeriums für Inneres und Kommunales NRW, sondern im Haushalt des Landtags mit einem eigenen Kapitel geführt.

Anfängliche Befürchtungen, dass durch die Einrichtung einer Landesbehörde "sui generis" die Beschäftigten meiner Behörde den Kontakt zur Landesverwaltung verlieren und in ihrer Personalentwicklung eingeschränkt werden, haben sich erfreulicherweise nicht erfüllt. Auf der Grundlage einer zwischen dem Innenminister und mir im April 2012 abgeschlossenen Kooperationsvereinbarung sind der wechselseitige Personalaustausch mit der Landesverwaltung, die Personalgewinnung und die Personalentwicklung gewährleistet. Darüber hinaus leistet das Ministerium bei einzelnen Fragen der Personalverwaltung und in organisationstechnischer Hinsicht wertvolle Unterstützung; in haushaltstechnischen Fragen werde ich von der Landtagsverwaltung unterstützt.

Aus organisatorischer Sicht ist noch von Bedeutung, dass das Gebäude Kavalleriestraße 2 - 4, in dem meine Behörde untergebracht ist, ab dem Jahr 2013 aufgrund einer Entscheidung des Bau- und Liegenschaftsbetriebs NRW nicht mehr von diesem angemietet ist, sondern unmittelbar von der Eigentümerin. Die Verhandlungen mit der Eigentümerin und Anbietern von Alternativimmobilien sowie die Ausarbeitung eines neuen Mietvertrages, die in Eigenregie geführt wurden, waren sehr aufwändig und haben in nicht unerheblichem Maße Personalkapazitäten gebunden.

An dieser Stelle möchte ich dem Landtag von Nordrhein-Westfalen für die im Haushaltsjahr 2011 bewilligten neuen Stellen ausdrücklich danken. Sie tragen deutlich zur Unterstützung in wichtigen Bereichen, unter anderem in den Bereichen Medienkompetenz und Task Force, bei.

Nach der Entscheidung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzkontrolle haben auch die anderen Länder in

Deutschland die Datenschutzaufsicht neu geregelt. Hieran anknüpfend und mit Blick auf Synergieeffekte haben der **Düsseldorfer Kreis** und die Konferenz der Datenschutzbeauftragten beschlossen, beide Gremien zusammenzuführen. Ziel des Düsseldorfer Kreises als in der föderalen Aufsichtsstruktur etabliertes "Markenzeichen" bleibt die bundesweit einheitliche Auslegung des geltenden Rechts im nicht-öffentlichen Bereich in wesentlichen Fragen, um zu einem für die Bürgerinnen und Bürger und für die Wirtschaft verlässlichen, bundesweit einheitlichen Datenschutzniveau zu gelangen. In diesem Rahmen ist der Düsseldorfer Kreis nach wie vor Ansprechpartner für Wirtschaft und Verbände, führt Verhandlungen und fördert den Meinungsaustausch, nunmehr als Arbeitskreis der Datenschutzkonferenz. Der Vorsitz liegt in Nordrhein-Westfalen.

Datenschutz und Informationsfreiheit stehen weiterhin vor großen Herausforderungen. Dass ich mich dabei auf kompetente und engagierte Mitarbeiterinnen und Mitarbeiter stützen kann, gibt mir die Gewissheit, die vor uns liegenden Aufgaben bewältigen zu können.

Ulrich Lepper Düsseldorf, im Frühjahr 2013

2 Entwicklungen

Neuorganisation

Die Unabhängigkeit spiegelt sich auch im innerbehördlichen Aufgabenspektrum wider. Hinzugekommen sind unter anderem die Aufgabenbereiche Personal, Personalvertretung, Gleichstellung und Haushalt. In meiner Behörde sind außerdem innerorganisatorische Vorkehrungen getroffen worden, um in größerem Maße mit gebündelten Kräften Kontrollmaßnahmen durchführen zu können. Zu diesem Zweck werden insbesondere referatsübergreifende Kontrollaktivitäten in einer Stabsstelle "Task Force" koordiniert. Ebenso ist der Bereich "Medienkompetenz" als Stabsfunktion in einem besonders eingerichteten Referatsbereich ausgewiesen. Ich verspreche mir hiervon weitere Impulse für den Selbstdatenschutz. Zugleich ist das Technikreferat von Verwaltungsaufgaben entlastet worden, um sich, auch in Zusammenarbeit mit Wissenschaft und Forschung, komplizierten Fragestellungen in der täglichen Arbeit sowie auch neuen technischen Entwicklungen intensiver zuwenden zu können.

Beratung/Stellungnahmen

Beratung als ein Standbein zur Unterstützung der Eigenverantwortung der Daten verarbeitenden Stellen entwickelt sich immer mehr zu einem bedeutenden Schwerpunkt. Unternehmen oder Behörden, aber auch Personalvertretungen, Betriebsräte oder Gewerkschaften wenden sich wegen vielschichtiger Fragestellungen an meine Behörde. Auch aus Anlass von Eingaben und Beschwerden, die unverändert den größten Teil der Bearbeitungskapazitäten meiner Behörde in Anspruch nehmen, kommt es im weiteren Verlauf der Bearbeitung häufig zu Empfehlungen ebenso mit beratendem Charakter. Schließlich nimmt meine Behörde zu Entwürfen insbesondere von Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften gegenüber den Ressorts der Landesregierung Stellung. Meine Behörde wirkt zudem beratend in verschiedenen interministeriellen Arbeitsgruppen auch mit Bundesbeteiligung mit. In der überwiegenden Zahl, dies ist erfreulich, konnten die Ausführungen überzeugen; Anregungen und Empfehlungen wurden aufgegriffen oder berücksichtigt.

Kontakt mit Datenschutzbeauftragten

Besprechungen mit Datenschutzbeauftragten über aktuelle Fragen sind ein weiteres Standbein zur Unterstützung der Eigenverantwortung. Regelmäßig gibt es Treffen z.B. mit den Datenschutzbeauftragten der Hochschulen oder mit Datenschutzbeauftragten von Konzernunternehmen. Ich bemühe mich darum, in stärkerem Maße als bisher zu regelmäßigen Besprechungen auch in anderen Bereichen mit Datenschutzbeauftragten zu kommen. Zu diesem Zweck habe ich beispielsweise erstmalig die Datenschutzbeauftragten sämtlicher Kommunalbehörden im Lande zu einer Auftaktveranstaltung nach Düsseldorf geladen. Die Erfahrungen sind positiv. Daher sind Folgetreffen auf regionaler Ebene vorgesehen.

2.1 Informationen meiner Behörde im Internet und durch Newsletter

Ein breites Informationsangebot hilft Bürgerinnen und Bürgern dabei, ihre Rechte zu kennen und geltend zu machen. Diese Informationen unterstützen Unternehmen und Verwaltungen dabei, ihre Verantwortung wahrzunehmen. Das Angebot meiner Behörde wird immer mehr genutzt.

Im Jahr 2011 haben sich die Nutzungszahlen des Internetangebots www.ldi.nrw.de im Vergleich zu 2010 verdreifacht. Auch der von mir eingeführte Newsletter zu Datenschutz und Informationsfreiheit in Nordrhein-Westfalen findet Zuspruch.

Die eigene Verantwortung können Unternehmen und Verwaltungen, aber auch Bürgerinnen und Bürger am besten wahrnehmen, wenn sie gut informiert sind. Das gilt ebenso vor einer Entscheidung über eine Datenverarbeitung wie auch dann, wenn bereits Probleme aufgetreten sind.

Ich freue mich, dass meine Informationen und meine Beratung oft nachgefragt werden – sei es im persönlichen Kontakt im Einzelfall oder bei Veranstaltungen - und lege großen Wert auf ein gutes Internetangebot.

➡ Nur gut informierte Bürgerinnen und Bürger können bewusst über den Schutz ihrer Daten entscheiden.

Auch Unternehmen und Verwaltungen sind auf gute Informationen angewiesen, um ihrer Datenschutzverantwortung gerecht zu werden. Ich trage deshalb weiterhin mit einem breiten Informationsangebot dazu bei.

2.2 Medienkompetenz und Datenschutzkompetenz

Datenschutz ist ein wichtiger Baustein, der bei Medienbildung und Medienkompetenz nicht fehlen darf. Datenschutz bedeutet dabei nicht nur Datensicherheit, sondern ist in einem sehr viel weiteren Sinn zu verstehen.

Wer über Medienkompetenz und Medienbildung spricht, kommt nicht darum herum, zunächst zu klären, wie die Begriffe zu verstehen sind. In der Literatur finden sich viele verschiedene Ansätze und Differenzierungen. Aus meiner Sicht stellt sich Medienkompetenz wie folgt dar (siehe auch mein Dossier im Medienkompetenz-Netzwerk NRW unter www.mekonet.de):

Spätestens seitdem es nicht mehr nur darum geht, Medien mit ihren vielfältigen Anwendungsmöglichkeiten zu verstehen und zu nutzen, sondern auch darum, Medienbeiträge selbst zu erzeugen und Teil eines Mediums – beispielsweise eines Sozialen Netzwerks – zu sein, muss auch die Perspektive des Datenschutzes vertreten sein. Datenschutz bedeutet dabei nicht nur, bestimmte technische Kompetenzen im Bereich der Datensicherheit abzudecken. Das Thema erfordert vielmehr ein umfassendes Verständnis, das Wertebildung sowie gesellschaftliche, politische und wirtschaftliche Betrachtungen mit einschließt. Ziel ist der bewusste und fähige Umgang mit eigenen Grundrechten und den Rechten anderer.

Datenschutzkompetenz muss ein selbstverständlicher Bestandteil der Medienbildung sein. Die Vermittlung ist eine gesamtgesellschaftliche Aufgabe und muss möglichst früh beginnen. Die im Folgenden dargestellte Verknüpfung von Medienkompetenz und Datenschutzkompetenz kann die Einbindung der Datenschutzperspektive in Bildungskonzepte, die schon bestehen oder noch entwickelt werden, erleichtern.

Medienkompetenz und Datenschutzkompetenz haben ein breites Schnittfeld, vor allem im Bereich der Informations- und Kommunikati-

onstechnik. Deshalb lässt sich Medienkompetenz auch aus der Perspektive des Datenschutzes gut beschreiben. Basis dafür ist eine einfache Aufteilung der Medienkompetenz in drei Dimensionen, die jeweils mit Zielen beziehungsweise Kompetenzen aus der Datenschutzperspektive verknüpft werden:

- Technisch-funktional (nutzungsbezogen)
- Kognitiv-interpretatorisch (verständnisbezogen)
- Kognitiv-kritisch (wertungs-/urteilsbezogen).

Bei allen Dimensionen sind Mediennutzerinnen und -nutzer zugleich als Rezipierende und als Produzierende angesprochen.

1. Technisch-funktionale Dimension

   Bei der nutzungsbezogenen Betrachtungsweise stellen sich die folgenden Fragen:

   - Was passiert mit meinen Daten?
   - Wie kann ich einen Missbrauch meiner Daten verhindern?
   - Wie gehe ich mit Daten anderer um?

   Ausgedrückt in Zielen und Kompetenzen bedeutet das:

   - Es ist bekannt, wer welche personenbezogenen Daten bei welcher Gelegenheit verarbeitet oder verarbeiten kann. Beispiele: Browser, Suchmaschinen, Soziale Netzwerke, Games oder Smartphones.
   - Es ist bekannt, welche Sicherheitsmaßnahmen zum Selbstschutz genutzt werden können. Beispiele: Datensparsamkeit, Einstellungsmöglichkeiten in Sozialen Netzwerken oder bei Smartphones.
   - Es ist bekannt, welche Handlungsweisen datenschutzfreundlich sind. Dieses Ziel betrifft vor allem den Umgang mit den Daten anderer bei der Teilnahme an Sozialen Netzwerken und bei der eigenen Medienproduktion. Beispiel: Nutzung der personenbezogenen Daten anderer – wie Fotos, auf denen andere abgebildet sind – grundsätzlich nur mit deren Einwilligung.

2. Kognitiv-interpretatorische Dimension

   Die verständnisbezogene Perspektive lässt sich etwa mit den folgenden Fragen erfassen:

   - Was ist Datenschutz (informationelles Selbstbestimmungsrecht)?
   - Warum ist Datenschutz wichtig?
   - Was macht personenbezogene Daten wertvoll?
   - Wer interessiert sich warum für personenbezogene Daten?

   Für Ziele und Kompetenzen bedeutet das:

   - Die gesellschaftliche und die individuelle Funktion des Grundrechts "informationelle Selbstbestimmung" sind bekannt.
   - Die rechtlichen Grundlagen für den Datenschutz sind bekannt. Beispiele: Grundgesetz, Landesverfassung, Datenschutzgesetz des Landes, Bundesdatenschutzgesetz.
   - Politische Gestaltungen und wirtschaftliche Interessen, die sich auf den Datenschutz auswirken können, sind bekannt. Beispiele: Werbung, kostenlose Nutzung von Angeboten gegen Überlassung der eigenen Daten; Vorratsdatenspeicherung oder Videoüberwachung als Instrumente der inneren Sicherheit.

3. Kognitiv-kritische Dimension

   Beim wertungs-/urteilsbezogenen Ansatz steht die folgende Frage im Mittelpunkt:

   - Welche Daten will ich/muss ich schützen?

     Die Frage stellt sich für die eigenen Daten und für die Daten anderer. Die Antwort wird nach bestimmten Rollen und Situationen zu differenzieren sein.

Für Ziele und Kompetenzen heißt das:

- Der subjektive Wert der (eigenen und fremden) Daten ist – bezogen auf Rollen und Situationen – reflektiert und bewusst.
- Der subjektive Schutzbedarf ist – bezogen auf Rollen und Situationen – reflektiert und bewusst.

Inhaltlich sollten dabei Wertmaßstäbe nicht vorgegeben werden (Welche Daten muss oder soll ich schützen?). Das informationelle Selbstbestimmungsrecht ist ein Freiheitsgrundrecht. Darin enthalten ist auch die Freiheit, das eigene Recht bewusst nicht wahrzunehmen (Welche Daten will ich schützen?). Für die Bildung von eigenen Wertmaßstäben sollten Orientierungspunkte und mögliche Konsequenzen von Entscheidungen auf der Basis von ausreichenden Informationen aufgezeigt werden. Ziel sind bewusste und reflektierte Entscheidungen.

➡ Ich setze mich dafür ein, dass Datenschutzkompetenz ein selbstverständlicher Bestandteil der Medienbildung wird.

2.3 Vermittlung von Medienkompetenz

Meine Behörde wirkt an der Vermittlung von Datenschutzkompetenz im Rahmen der Medienkompetenz mit.

Meiner Behörde ist im Datenschutzgesetz Nordrhein-Westfalen die Aufgabe zugewiesen, "die Bürger sowie die Öffentlichkeit" zu Fragen des Datenschutzes zu informieren, nicht nur mit diesem Bericht, sondern auch "auf andere Weise". Information ist eine wichtige Voraussetzung dafür, bewusst mit dem eigenen Recht auf informationelle Selbstbestimmung und mit den Rechten anderer umzugehen – wie zuvor ausgeführt, ein Bestandteil von Datenschutzkompetenz im Rahmen von Medienkompetenz.

In erster Linie ist daran zu denken, die Schule im Rahmen ihrer Bemühungen um Medienkompetenz zu unterstützen. Eine flächendeckende Vor-Ort-Betreuung aller rund 6.500 Schulen in Nordrhein-Westfalen ist von meiner Behörde personell allerdings nicht zu leisten. Hier könnte die Schulung von Multiplikatorinnen und Multiplikatoren ein zukünftiges Betätigungsfeld sein. Meine Behörde wäre im Übrigen

überfordert, wenn sie neben oder anstelle der Landesregierung in Bereichen tätig sein sollte, in denen insbesondere die Landesregierung entweder bereits aktiv oder gefragt ist.

Deshalb konzentriere ich mich bei der Vermittlung von Medienkompetenz auf die folgenden Komponenten:

- Kooperation mit anderen Stellen: In diesem Rahmen stelle ich Multiplikatorinnen und Multiplikatoren Beiträge zur Datenschutzkompetenz zur Verfügung.
- Informationen zu Datenschutzkompetenz auf meinen Internetseiten: Beiträge zur Datenschutzkompetenz stehen zum unmittelbaren Abruf bereit.

Ich setze auf Kooperationen mit anderen Stellen, die sich mit Medienbildung befassen, um den Datenschutzaspekt mit den anderen Dimensionen der Medienkompetenz zu verknüpfen und Synergieeffekte zu nutzen. Dazu stehe ich in Kontakt mit dem Ministerium für Schule und Weiterbildung NRW, um Beiträge für die Medienbildung in den Schulen zu leisten. Daneben bestehen gute Kontakte zu vielen weiteren Einrichtungen in NRW, die sich mit Medienbildung befassen, darunter die Landesanstalt für Medien und das Grimme Institut.

Beispiele für Projekte mit Kooperationspartnern:

- Datenschutz-Modul im Medienkompetenz-Quiz beim Medienkompetenz-Netzwerk NRW des Grimme Instituts (www.mekonet.de).
- Unterstützung der Medienberatung im Geschäftsbereich des Schulministeriums (z.B. beim Projekt Logineo: Webbasierte Benutzeroberfläche mit direktem Zugang zu allen im Schulbereich benötigten digitalen Medien).
- Mit den Datenschutzbeauftragten des Bundes und der anderen Länder arbeite ich in einem Arbeitskreis zu Datenschutz und Bildung zusammen. Beispiel: Unterrichtsmaterialien für ein Zusatzmodul zum Medienkompetenz-Unterricht: "Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web" (Herausgeber: KlickSafe, www.klicksafe.de, getragen unter anderem von der Landesanstalt für Medien NRW).

➡ Ich begrüße, dass der Landtag die Entwicklung von Medienkompetenz unter Einbindung des Datenschutzes als einen wichtigen Baustein zur Verwirklichung des Grundrechts auf informationelle Selbstbestimmung ansieht und die Landesregierung gebeten hat, Beratungsangebote meiner Behörde bei datenschutzrelevanten Aspekten des Themas Medienkompetenz in Anspruch zu nehmen (siehe Landtags-Drucksache 16/1469). Die Öffentlichkeit und gerade auch Kinder und Jugendliche müssen dazu auf verschiedenen Wegen angesprochen und informiert werden. Ich bringe weiterhin Beiträge zur Datenschutzkompetenz in Kooperationen ein und entwickle das eigene Angebot weiter.

2.4 Stärkere Aufsicht

Wie in meinem letzten Bericht ausgeführt, gehören zu einem wirksamen Datenschutz schlagkräftige Kontrollen. Schon aus Anlass einer Vielzahl von Beschwerden, Eingaben und Hinweisen nimmt meine Behörde umfangreiche Kontrollen vor und kann Datenschutzmängel abstellen. Im Berichtszeitraum sind nunmehr auch Kontrollen von Amts wegen verstärkt durchgeführt worden. Hierbei ging es nicht darum, neue Anforderungen festzulegen, sondern in erster Linie darum zu überprüfen, ob bestehende eingehalten werden. Eine Reihe von Kontrollen hat vor Ort stattgefunden. Andere sind in Form von Befragungen durchgeführt worden. Beispiele, die im Berichtszeitraum als dringlich bearbeitet wurden, sind nachstehend aufgeführt:

2.4.1 Tracking

Die personenbezogene Analyse des Surfverhaltens im Internet ist schon seit Jahren in der Kritik der Datenschützer. Nachdem die Aufsichtsbehörden des Bundes und der Länder in ihrem Beschluss vom 26./27. November 2009 (siehe Beschluss des Düsseldorfer Kreises "Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten"; Abdruck im Anhang) darauf hingewiesen hatten, dass bei der personenbezogenen Nutzerdatenanalyse die Vorschriften des Telemediengesetzes und des Bundesdatenschutzgeset-

zes zu beachten sind, war es nun an der Zeit, den Worten auch Taten folgen zu lassen.

Bei einer Prüfung des Einsatzes von "Google Analytics" bei 4105 Internetdomainadressen, deren Inhaberinnen und Inhaber ihren Geschäftssitz in Nordrhein-Westfalen haben, war bei 1379 der geprüften Angebote Google Analytics im Einsatz. Diese Prüfergebnisse habe ich als Ausgangspunkt für einen unfassenden Fragenkatalog genommen, den ich im Mai 2012 an die betroffenen 1379 Domaininhaber versandt habe. Zu allgemeinen Fragen, beispielsweise ob überhaupt eine Datenschutzerklärung auf der Internetseite vorhanden ist, bis hin zu speziellen Fragen, z.B. nach einem abgeschlossenen Vertrag zur Auftragsdatenverarbeitung zwischen dem Anbieter und Google, wurden die Anbieter zur Stellungnahme aufgefordert. Nur fünf von 1379 haben bislang nicht geantwortet. Hier werden weitere Maßnahmen folgen. Gut ein Drittel der befragten Unternehmen setzt aufgrund des Fragebogens und meiner Informationen Google Analytics zwischenzeitlich nicht mehr ein. Nach Angaben der übrigen Unternehmen sind die geforderten Maßnahmen von ihnen umgesetzt worden. Ob dies tatsächlich der Fall ist, werde ich in einem weiteren Prüflauf feststellen.

Die Resonanz auf diese Prüfung war durchweg positiv. Landes- und auch bundesweit haben die Unternehmen und Verbände wahrgenommen, dass der proaktive Kontrollansatz in Nordrhein-Westfalen verstärkt worden ist. Auch wenn die Prüfung für viele Unternehmen zunächst einen Mehraufwand bedeutete, so haben die meisten Unternehmen diese Art der Prüfung begrüßt. Nicht wenige haben dies auch zum Anlass genommen, andere datenschutzrechtliche Fragen im Unternehmen aufzugreifen, die mit meiner Hilfe geklärt werden konnten.

- Der große Erfolg der Prüfaktion zeigt, dass es sich lohnt, solche breit angelegten Prüfungen auch in Zukunft zu wiederholen und im Kontakt mit den Unternehmen den Datenschutz weiterzuentwickeln.

2.4.2 Der Landesbeauftragte vor Ort – "Task-Force-Einsätze" in Sachen Videoüberwachung

Dem Ziel, die Aufsicht vor Ort spürbar und sichtbar zu machen, bin ich im Bereich der Videoüberwachung schon einen Schritt näher gekommen. Hier wurden die Kontrollen vor Ort verstärkt.

Schon lange war klar: Gerade die Zulässigkeit von Videoüberwachungsanlagen lässt sich nicht immer vom Schreibtisch aus hinreichend beurteilen, und auch die betroffenen Personen und verantwortlichen Stellen beklagten gelegentlich die mangelnde Präsenz der Aufsicht vor Ort. Aufgrund einer personellen Verstärkung war es möglich, nicht nur in besonders gelagerten Ausnahmefällen Videokameras vor Ort in Augenschein zu nehmen und dabei mit den Beteiligten ins Gespräch zu kommen.

So führte das für Videoüberwachung zuständige Referat in einer ersten Testphase im Jahr 2012 in gut zehn Prozent der Fälle Informations- und Kontrollbesuche vor Ort durch. Die Erfahrungen waren durchweg positiv. Hier nur einige Beispiele:

- Es konnten umfassende und unmittelbare Eindrücke von der tatsächlich durchgeführten Videoüberwachung – auch unter Berücksichtigung der Örtlichkeiten – gewonnen werden. Häufig fand sich die vorangegangene schriftliche Darstellung bestätigt. In Einzelfällen zeigte sich aber auch, dass die Ausrichtung der Kameras verändert worden war, es weitere Kameras gab oder dass einzelne Kameras schon wieder abgebaut waren.
- Vielfach wurden bei den vor Ort geführten Gesprächen zusätzliche Informationen mitgeteilt, die für die Bewertung der Videoüberwachung von erheblicher Bedeutung waren.
- Zugleich erfolgte regelmäßig eine individuelle Beratung der Verantwortlichen, um entweder die datenschutzgerechte Durchführung der Videoüberwachung sicherzustellen oder auf den zeitnahen Abbau einzelner Kameras hinzuwirken.
- Ohne die Inaugenscheinnahme der Videoüberwachungsanlagen hätten manche Vorgänge nicht zufriedenstellend, viele andere nur mit erheblich höherem Zeitaufwand abgeschlossen werden können.

- Die betroffenen Personen fühlten sich wegen der Vorortkontrollen in ihrem Anliegen ernst genommen. Soweit Videoüberwachungsanlagen aufgrund ihrer Eingaben verändert oder deaktiviert wurden, fanden sie sich bestätigt. Andernfalls konnten ihnen nach dem Ergebnis des Ortstermins unnötige Sorgen genommen werden. Seitens der Betroffenen gab es viele positive Rückmeldungen.
- Allerdings reagierten auch die verantwortlichen Stellen ganz überwiegend positiv auf die Ortsbesuche, da sie Gelegenheit hatten, ihre Sicht der Dinge und ihre Gründe für die Videoüberwachung eingehend darzulegen. Durch die unmittelbaren Erklärungen meiner Mitarbeiterinnen und Mitarbeiter vor Ort fiel es ihnen oft leichter, Einschränkungen der Überwachung nachzuvollziehen oder gar die Empfehlung zum Abbau von Kameras zu akzeptieren.

Nach den positiven Erfahrungen soll die Zahl der Informations- und Kontrolltermine in Sachen Videoüberwachung in der Zukunft schrittweise weiter erhöht werden.

➡ Meine Mitarbeiterinnen und Mitarbeiter arbeiten nicht nur "im stillen Kämmerlein", sondern sind zunehmend auch vor Ort präsent. Ich werde auch in Zukunft verstärkt Kontrollen vor Ort durchführen.

2.5 Ordnungswidrigkeiten

Die Ahndung von Verstößen gehört als ultima ratio ebenfalls zur Aufsicht. Regelmäßig muss ich Ordnungswidrigkeitenverfahren, z.B. wegen nicht erteilter Auskunft, einleiten. Wegen materiell-rechtlicher Verstöße gegen den Datenschutz werden ebenfalls Verfahren eingeleitet.

So wurde im Berichtszeitraum ein Ordnungswidrigkeitenverfahren gegen ein Dienstleistungsunternehmen, das Lastschriftverfahren im Rahmen der EC-Kartenzahlung abwickelt, mit einem Bußgeld von 60.000 Euro abgeschlossen (siehe zum elektronischen Lastschriftverfahren Bericht 2011 unter Ziffer 4.3). Das Unternehmen hatte unzulässigerweise Daten über Ort, Zeitpunkt und Höhe von Zahlungsvorgängen an ein Schwesterunternehmen weitergegeben. Dieses anony-

misierte die 400.000 Zahlungsverkehrdaten zwar anschließend und wertete sie nur statistisch aus. Die vorangegangene Weitergabe erfolgte jedoch mit den entsprechenden Kontodaten. Da es sich um sensible Daten handelte, die nur für die Zahlungsabwicklung verarbeitet werden durften, war die unzulässige Übermittlung mit einem Bußgeld zu ahnden. Zugunsten des Unternehmens war zu berücksichtigen, dass das Unternehmen die Weitergabe von Kontoverbindungsdaten an Dritte bereits vor dem öffentlichen Bekanntwerden des Sachverhalts eingestellt hatte und sich bei dessen Aufklärung kooperativ zeigte. Gemeinsam mit anderen Aufsichtsbehörden habe ich zwischenzeitlich die Datenverarbeitungsprozesse zum elektronischen Lastschriftverfahren insgesamt geprüft. Die dabei entwickelten Vorgaben hat das Unternehmen umgesetzt. Daher entsprechen seine Datenverarbeitungsprozesse zum elektronischen Lastschriftverfahren nun den datenschutzrechtlichen Anforderungen.

➡ Auch weiterhin werde ich Verfahren wegen einer Ordnungswidrigkeit einleiten, soweit dies als wirksames Mittel der Datenschutzkontrolle geboten ist.

2.6 Anordnungen und Beanstandungen

Auf der Grundlage des im Jahre 2009 neugefassten § 38 Abs. 5 Bundesdatenschutzgesetz (BDSG) wurden in einzelnen Fällen gegen Firmen Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten angeordnet.

Ebenso ist es in mehreren Fällen zu Beanstandungen gegenüber Behörden gekommen.

In einem Verfahren gegen den Betreiber eines Flirt-Portals, das die Bewertung von "Dates" ermöglicht, habe ich eine förmliche Anordnung erlassen, da das Unternehmen nicht bereit war, meine Forderung nach einer datenschutzfreundlichen Lösung umzusetzen (siehe zur Vorgeschichte Bericht 2011 unter 6.7). Über diesen Dienst können ohne Einwilligung der Betroffenen sowohl deren Erscheinungsbild und Auftreten bis hin zur "Kussqualität" und der Frage, ob "man sich näher gekommen" ist, bewertet und über die Plattform veröffentlicht werden.

Daher habe ich den Betreiber aufgefordert, die bereits erhobenen Angaben zu löschen und zukünftige Bewertungen nicht ohne wirksame Einwilligung der Betroffenen zu erheben und zu veröffentlichen. Gegen die Anordnung wurde der Rechtsweg beschritten, so dass sich das Verfahren derzeit noch in gerichtlicher Klärung befindet.

In einem weiteren Fall ließ sich der Inhaber eines Handwerksbetriebs auch nach mehrmaligen Hinweisen auf eine datenschutzwidrige Videoüberwachung im Übermaß in seinen Werkstatträumen nicht überzeugen, diese zu beenden. Da der Firmeninhaber anderweitige Maßnahmen ohne permanente und verdachtslose Erhebungen von Beschäftigtendaten nicht umsetzen wollte, wurde eine Verfügung zur Untersagung der Videoüberwachung erlassen, die von diesem angefochten worden ist. Auch dieser Fall befindet sich vor Gericht.

➡ In Fällen von grundsätzlicher Bedeutung, in denen sich die Verantwortlichen eindeutigen Anforderungen des Datenschutzes verweigern, werde ich weiterhin von der Möglichkeit der aufsichtsbehördlichen Anordnung nach § 38 Abs. 5 BDSG Gebrauch machen.

Entsprechendes gilt für Beanstandungen gegenüber Behörden und Körperschaften des öffentlichen Rechts (siehe Ziffern 3.6, 15.2, 15.3 und 15.8). Wegen der Einzelfälle wird auf die Darstellungen im Bericht verwiesen.

3 Schlaglichter auf die Aufsichtspraxis

3.1 Vorsicht bei Online-Spielen!

Im Bericht 2011 habe ich bereits eindringlich auf das Gefahrenpotenzial hingewiesen, das Online-Spiele aufweisen. Tatsächlich nimmt in der Praxis die Zahl konkreter Hinweise stetig zu.

Insbesondere im Rahmen der Einführung eines neuen Online-Spiels im Herbst 2011 kam es zu zahlreichen Beschwerden. Dieses Spiel, das zu den gefragten "Kriegs-Shootern" gehört, kann nur betrieben werden, wenn Nutzerinnen und Nutzer ein Zusatzprogramm auf dem PC installiert haben. Dieses Programm dient der Nutzung der Online-Vertriebsplattform des Spieleanbieters, die gleichzeitig alle Funktionen eines Sozialen Netzwerkes bereitstellt.

Die Betroffenen kritisierten in diesem Zusammenhang nicht nur, dass sie vor dem Kauf des Spiels nicht ausreichend darüber informiert wurden, dass das Spiel nur nach Installation der Zusatzsoftware und bei dauerhafter Internetverbindung genutzt werden könne. Vielmehr wurde befürchtet, dass die Spiele-Plattform die Festplatten ausspioniere. Begründeten Anlass boten die ursprünglichen Formulierungen der Endbenutzer-Lizenzvereinbarung und der Datenschutz-Richtlinie des Unternehmens. Mit diesen räumte sich der Spieleanbieter weitreichende Rechte ein, die Computer der Nutzerinnen und Nutzer zu überwachen und deren Daten zu sammeln und zu verwerten.

Aufgrund der Beschwerden habe ich einen umfangreichen Fragenkatalog zu den Datenverarbeitungsprozessen an das Unternehmen übersandt sowie die Endbenutzer-Lizenzvereinbarung und die Datenschutz-Richtlinie umfassend überprüft.

Als Ergebnis stellte sich heraus, dass es sich bei der zur Nutzung des Spiels erforderlichen Zusatzsoftware tatsächlich nicht um eine sogenannte Spyware handelt, die die Festplatten der Nutzerinnen und Nutzer auf Inhalte durchsucht. Allerdings verstießen zahlreiche Klauseln der Datenschutz-Richtlinie gegen deutsches Datenschutzrecht. Auf meine Hinweise hat der Spieleanbieter bereits mit Änderungen der Vertragsbedingungen reagiert und rechtswidrige Klauseln entfernt. Die hierin geregelten weitreichenden Möglichkeiten der Datennutzung hat

das Unternehmen, wie es mir versicherte, nicht ausgeschöpft. Auch bei diesem Anbieter ist aber die Datenschutzerklärung nach wie vor insgesamt unübersichtlich und schwer verständlich.

➡ Ich setze mich dafür ein, dass insbesondere bei Online-Spiele-Angeboten nicht nur die datenschutzrechtlichen Anforderungen beachtet werden, sondern Nutzerinnen und Nutzer auch über die dem Spielbetrieb zugrundeliegenden Datenverarbeitungsprozesse verständlich und umfassend informiert werden.

3.2 Schutz Minderjähriger bei Internetportalen und Online-Gewinnspielen für Kinder – Ein Herz für Kinder?

Internetportale, die speziell auf die Interessen und Fähigkeiten von Kindern und Jugendlichen zugeschnitten sind, sind nicht nur aus Sicht des Minderjährigenschutzes, sondern auch in datenschutzrechtlicher Hinsicht oft kritisch zu betrachten. Nicht selten verbergen sich hinter vermeintlich kindgerechten Seiten Anmeldeprozesse oder Gewinnspiele, mit denen umfassend Daten der Minderjährigen abgefragt werden.

Das Grundprinzip der Datensparsamkeit, das besagt, dass die Erhebung von personenbezogenen Daten nur erfolgen darf, sofern diese Daten für den jeweiligen Zweck unbedingt erforderlich sind, hat für Kinder und Jugendliche eine besondere Bedeutung. Vor allem die Jüngeren geben vielfach ihren Namen, Wohnort und sogar Fotos in die hierfür vorgesehenen Felder der jeweiligen Plattformen ein. Sie müssen den vorsichtigen Umgang mit ihren eigenen Daten und den Schutz ihrer Privatsphäre erst erlernen. Unternehmen, die solche Seiten im Internet anbieten, tragen daher eine besondere Verantwortung und sind aufgefordert, besonders sensibel bei Erhebung und Verarbeitung von Daten Minderjähriger vorzugehen. Dazu gehört auch, Datenschutzhinweise so zu platzieren und zu formulieren, dass ebenso Kinder und Jugendliche deren Inhalt und die mit der Datenpreisgabe verbundenen Risiken verstehen. Die Regelungen des Entwurfes der EU-Datenschutzgrundverordnung sind hier ein Schritt in die richtige Richtung. Danach dürfen personenbezogene Daten zumindest von Kindern

unter 13 Jahren ausdrücklich nur mit Einwilligung der Eltern erhoben werden.

Insbesondere beim Angebot von Online-Gewinnspielen für Kinder und Jugendliche ist mir aufgefallen, dass häufig weit mehr Daten der Teilnehmenden abgefragt werden als tatsächlich zur Feststellung der Gewinnerinnen und Gewinner sowie zur Übersendung der Gewinne nötig sind. Unabhängig von der Frage, ob nach dem Jugendschutz Kinder und Jugendliche überhaupt an Gewinnspielen teilnehmen dürfen, sind weder die Angabe der Postadresse noch Alter und Geschlecht der Kinder und Jugendlichen für die bloße Gewinnspielteilnahme erforderlich. Es genügt, die E-Mail-Adressen der Teilnehmenden bzw. der Eltern abzufragen. Bei einem eventuellen Gewinn kann dann die Gewinnbenachrichtigung per E-Mail erfolgen. Das häufig vorgetragene Argument der Anbieter von Online-Spielen, die große Fehlerquote bei E-Mail-Benachrichtigungen erfordere die zusätzliche Abfrage der Postadresse, ist nicht nachvollziehbar: Tippfehler können sowohl bei Eingabe der Postadresse als auch bei Eingabe der E-Mail-Adresse zu Zustellungsproblemen führen, und auch Werbebriefe landen häufig ungelesen im Müll und werden wie durch Spamfilter aussortierte E-Mails nicht gelesen.

➡ Auf meine Forderung hin haben Anbieter in NRW die Anmeldeprozesse zu den Internet-Portalen für die an Kinder und Jugendliche gerichteten Web-Angebote verändert, so dass die erforderlichen Informationen zum Datenschutz für die Nutzerinnen und Nutzer nunmehr verständlich sind. Auch den Eltern werden nun im Rahmen der Abfrage, ob sie mit der Teilnahme ihrer Kinder einverstanden sind, die Funktionen und Prozesse der Dienste erläutert, um eine informierte Entscheidung in Kenntnis der Risiken zu gewährleisten. Allerdings konnte im Bereich der Online-Gewinnspiele ein Unternehmen bisher nicht davon überzeugt werden, dass die Angabe der E-Mail-Adresse ausreicht. Ich werde die Angelegenheit weiter verfolgen.

3.3 Fehlgeschlagener Versuch zur Selbstregulierung bei Veröffentlichung digitaler Gebäudeansichten im Internet

Angesichts der Diskussion um Internetangebote wie Google Street View gab es Ende 2010 Überlegungen im Bundesrat und in der Bundesregierung, neue Regelungen im Bundesdatenschutzgesetz (BDSG) zu Geodaten und zum Schutz der Privatsphäre im Internet zu schaffen.

Die Bundesregierung wollte die Regelungen auf eine "rote Linie" beschränken, die zur Wahrung von Persönlichkeitsrechten gegen besonders schwere Eingriffe im Internet nicht überschritten werden dürfe. Im Übrigen sollte sich die Internetwirtschaft in freiwilligen Selbstverpflichtungen zu datenschutzfreundlichen Vorgehensweisen bekennen. Sofern eine solche Selbstregulierung nicht gelingen und nicht mit den Datenschutzaufsichtsbehörden abgestimmt sein sollte, hatte die Bundesregierung gesetzgeberische Schritte auch in diesen Bereichen angekündigt (siehe Bericht 2011 unter 4.1).

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) hatte im Dezember 2010 den Entwurf eines Datenschutz-Kodex für Geodatendienste vorgelegt. Anbieter von digitalen Straßenansichten im Internet beabsichtigten damit eine Selbstverpflichtung zur Umsetzung datenschutzrechtlicher Anforderungen.

Der Entwurf enthielt durchaus positive Ansätze, um den betroffenen Personen mehr Transparenz zu bieten. So sollte ein einheitliches Internetportal geschaffen werden, bei dem sich die Betroffenen über die Angebote der beteiligten Unternehmen informieren und Widerspruch gegen die Veröffentlichung von Bildern ihrer Straßenansicht einlegen können.

In einem entscheidenden Punkt blieb der Entwurf jedoch hinter dem zurück, was die Datenschutzaufsichtsbehörden mit einzelnen Anbietern von Geodatendiensten, etwa mit Google für dessen Angebot Street View, als Anforderung vereinbart hatten. So sah der Kodex nur einen nachträglichen Widerspruch gegen die Veröffentlichung von Häuserfassaden vor. Nach Auffassung der Datenschutzaufsichtsbehörden müssen Eigentümer und Bewohner jedoch bereits im Vorfeld der Darstel-

lung ihrer Häuser oder Wohnungen widersprechen können (siehe Bericht 2011 unter 4.1).

Die Unternehmen argumentierten, ein Vorabwiderspruch sei zu aufwändig und insbesondere kleine und mittelständische Unternehmen würden damit überfordert. Es gebe technisch keine Möglichkeit, die Widersprüche automatisiert umzusetzen.

Jedoch habe ich mit Unterstützung des nordrhein-westfälischen Ministeriums für Inneres und Kommunales eine Möglichkeit aufgezeigt, wie mit Hilfe von Hauskoordinaten der Landesvermessungsverwaltungen Widersprüche auf einfache Art und Weise den Adressen zugeordnet werden können. So wäre es möglich gewesen, ein "zentrales Widerspruchsregister" zu schaffen, so dass – etwa vergleichbar der sogenannten Robinson-Liste der Werbewirtschaft – Vorabwidersprüche von allen Unternehmen berücksichtigt werden könnten und sich die Betroffenen nicht an jeden einzelnen Anbieter wenden müssten. Die Internetwirtschaft hat diesen Vorschlag bedauerlicherweise nicht aufgegriffen.

Ein solches Register würde im Übrigen den Gesetzgeber der Notwendigkeit entheben, für derartige Fallkonstellationen Regelungen zu treffen, in denen angesichts der unübersehbaren Interessenvielfalt abstrakt-generelle Festlegungen im vorhinein kaum in angemessener Weise getroffen werden können.

Der Entwurf des von acht maßgeblichen Unternehmen unterzeichneten Geodaten-Kodex konnte vor diesem Hintergrund nicht die Zustimmung der Datenschutzaufsichtsbehörden finden (siehe Beschluss des Düsseldorfer Kreises "Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert" vom 8. April 2011; Abdruck im Anhang).

➡ Ein zentrales Widerspruchsregister würde ein sinnvolles Verfahren darstellen, das Betroffenen ermöglicht, die Wahrung ihrer Rechte selbst in die Hand zu nehmen. Ein Vorabwiderspruch ließe sich in solchen Fällen in technisch einfacher Weise umsetzen.

3.4 Soziale Netzwerke – nicht sozial zum Datenschutz

Nach wie vor bieten Soziale Netzwerke beliebte Möglichkeiten zur Kommunikation. Das Angebot wird ständig um neue Funktionalitäten ergänzt. Allerdings gehen damit auch immer neue Probleme bei den zugrunde liegenden Datenverarbeitungsprozessen einher.

Die Datenschutzbehörden des Bundes und der Länder haben sich erneut mit zwei Beschlüssen Ende 2011 ausdrücklich an die Betreiber gewandt und dringend geraten, die Netzwerke datenschutzgerecht zu gestalten (siehe Entschließung der Datenschutzkonferenz "Datenschutz bei Sozialen Netzwerken jetzt verwirklichen!" vom 28./29. September 2011 und Beschluss des Düsseldorfer Kreises "Datenschutz in sozialen Netzwerken" vom 8. Dezember 2011; Abdrucke im Anhang). Öffentliche Stellen wurden aufgefordert, von der Nutzung von Social–Plug-ins (Bausteine zur Gestaltung von Webseiten, die durch Anbieter Sozialer Netzwerke angeboten werden) und Bereitstellung von Profilseiten oder Fanpages auf solchen Plattformen abzusehen. Schließlich wurden auch die Betreiber privater Web-Sites auf die Risiken der Einbindung von Social-Plug-ins und der Nutzung von Fanpages hingewiesen, wenn sie die zugrunde liegende Datenverarbeitung nicht überblicken und damit die Nutzerinnen und Nutzer nicht hinreichend unterrichten können.

Problematisch ist die Einbindung von Social-Plug-ins besonders dann, wenn sie ohne hinreichende Information der Nutzenden und ohne Einräumung eines Wahlrechts erfolgt und durch den Besuch einer Website mit Social-Plug-in automatisch eine Übermittlung der Daten der Nutzerinnen und Nutzer ausgelöst wird, ohne dass eine entsprechende Einwilligung hierfür vorliegt.

Auf der Basis dieser gemeinsamen Beschlüsse der Aufsichtsbehörden habe ich die Landesregierung beraten und zudem die kommunalen Datenschutzbeauftragten in Nordrhein-Westfalen auf die besondere Verantwortung gegenüber den Bürgerinnen und Bürgern hingewiesen. Der Abruf von Informationen bei einer Behörde muss auch weiterhin möglich sein, ohne dass die Bürgerinnen und Bürger dafür gleichsam mit ihren Daten bezahlen und über die weitere Verarbeitung ihrer Daten bei Dritten keine Kenntnis haben.

Zusätzlich habe ich mich als Vorsitzender des Düsseldorfer Kreises gemeinsam mit der Vorsitzenden der Datenschutzkonferenz im Jahr 2012 mit einem Forderungskatalog an die Facebook Inc. gewandt und dringend appelliert, ein deutliches Zeichen für mehr Datenschutz zu setzen. Facebook hat sich auf die laufenden Prüfungen des irischen Datenschutzbeauftragten berufen und vorgeschlagen, diese Ergebnisse zunächst abzuwarten. Der Bericht des irischen Datenschutzbeauftragten liegt nun seit Ende September 2012 vor. Facebook hat die Funktion der Gesichtserkennung für den Bereich der Europäischen Union einstweilen abgestellt und damit der Kritik zumindest in diesem Punkt Rechnung getragen. In verschiedenen Bereichen wurden allerdings auch die Empfehlungen des irischen Datenschutzbeauftragten bislang noch nicht vollständig umgesetzt.

Nach wie vor lassen außereuropäische Anbieter die Nutzerinnen und Nutzer über die Datenverarbeitung im Unklaren. Die Datenschutzhinweise vermitteln auch nicht annähernd die Transparenz, die erforderlich ist, um eigenverantwortlich entscheiden zu können, ob unter den vorgegebenen Bedingungen eine Nutzung überhaupt gewollt sein kann. Überhaupt ist eine Bereitschaft, sich substantiell in Richtung Datenschutz zu bewegen, kaum zu erkennen.

Gleichwohl haben die deutschen Aufsichtsbehörden gegenüber dem Bundesministerium des Innern ihre Bereitschaft erklärt, unter Federführung der FSM (Freiwillige Selbstkontrolle Mulitmediadiensteanbieter e.V.) mit den großen Sozialen Netzwerken Gespräche über die gemeinsame Entwicklung eines deutschen Verhaltenskodex zur Selbstregulierung der Netzwerkbetreiber zu führen. In den Gesprächen vertrete ich die Aufsichtsbehörden. Im Berichtszeitraum konnten Ergebnisse noch nicht erzielt werden. Es bleibt abzuwarten, ob in dieser Branche Erfolge auf dem Verhandlungsweg erzielt werden können, nachdem bereits der Versuch, einen Kodex zu erarbeiten, gescheitert ist (siehe oben unter Ziffer 3.3).

➡ Meine Bemühungen sind nach wie vor von dem Bestreben getragen, die Netzwerkbetreiber zunächst im Verhandlungsweg von datenschutzfreundlichen Grundeinstellungen der Plattformen zu überzeugen. Daher begrüße ich, dass die Europäische Union auch außereuropäischen Anbietern von Diensten, die sich an Nutzerinnen und Nutzer in der Europäischen Union richten, ei-

nen wirksamen europäischen Datenschutzstandard auf hohem Niveau vorzugeben beabsichtigt.

3.5 Unzulässige Datenübermittlung von Patientendaten bei Fernwartung

Im Rahmen der Meldung einer Datenpanne gemäß § 42a Bundesdatenschutzgesetz ist meiner Behörde mitgeteilt worden, dass sensible Patientendaten bei einer automatisierten Fernwartung von medizinischen Diagnostikgeräten an die Herstellerfirma übertragen wurden.

Die Herstellerfirma benötigte für die Aufgabe lediglich gerätespezifische und sonstige nicht personenbezogene Daten. Bei einer internen Überprüfung stellte sie fest, dass im Rahmen der ihr übertragenen Fernwartung auch Patientendaten an sie übermittelt worden waren, die für ihre Aufgabe nicht erforderlich waren. Die Herstellerfirma informierte die Krankenhäuser und Arztpraxen, die mit ihrem Gerät Untersuchungen durchgeführt hatten, über diese systemwidrige und nicht datenschutzgerechte Datenübermittlung und nahm umfangreiche Untersuchungen zur Fehlersuche und –behebung auf. Dabei stellte sich heraus, dass es sich hierbei um einen Fehler handelte, der seine Ursache bereits in der Systementwicklung hatte. Um die weitere rechtswidrige Übermittlung von personenbezogenen Daten auszuschließen, werden nun bei den älteren Geräten dieses Herstellers die relevanten personenbezogenen Daten durch ein technisches Anonymisierungsverfahren vor der Übermittlung gleichsam "geschwärzt", da eine andere Lösung nicht mehr möglich ist. Wenn dies auch keine technisch optimale Lösung darstellt, werden so wenigstens weitere Datenschutzverstöße vermieden. In Bezug auf Neugeräte hat das Unternehmen zugesagt, die Software umzustellen.

- Bereits bei der Konzeption besonders von Systemen, die sensible Daten verarbeiten, muss besonderes Augenmerk auf die notwendigen technischen Datenschutzmechanismen gerichtet werden (privacy by design). Die weiteren Maßnahmen des Unternehmens werde ich kontrollieren.

3.6 Gravierender Datenschutzverstoß durch die Ratsvorlage einer Kommune

Veröffentlichung eines Testamentes in einer Ratsvorlage offenbart das Erbe zahlreicher Unbeteiligter

Noch in meinem letzten Datenschutzbericht 2011 hatte ich unter 12.1 darauf hingewiesen, dass personenbezogene Daten durch Kommunen im Rat nur offenbart werden dürfen, soweit entgegenstehende schützenswerte Interessen Einzelner oder Belange des öffentlichen Wohls nicht überwiegen.

Von einem Bürger wurde ich darüber informiert, dass eine Stadt in einer Vorlage für den öffentlich tagenden Hauptausschuss das vollständige Testament einer Erblasserin veröffentlicht hatte. Hierdurch wurden eine zweistellige Zahl von Erben und sonstigen Begünstigten sowie Art und Umfang der jeweiligen Beteiligung am Erbe bekannt. Die Veröffentlichung dieser besonders schutzwürdigen Daten erfolgte ohne Rechtsgrundlage.

➡ Da die Kommune zunächst weiterhin die Auffassung vertrat, rechtmäßig gehandelt zu haben, habe ich die Veröffentlichung gem. § 24 Datenschutzgesetz Nordrhein-Westfalen beanstandet. Darüber hinaus habe ich aufgrund der Erheblichkeit des Verstoßes bei der zuständigen Bezirksregierung angeregt, ein Bußgeldverfahren gegen die Verantwortlichen der Stadt einzuleiten.

4 Entwicklung des Datenschutzrechts

4.1 EU-Rechtsrahmen

Die Europäische Union plant, die Datenschutzbestimmungen in Europa weiter zu vereinheitlichen. Das Ziel, weitgehend übereinstimmende Regelungen zu schaffen, begrüße ich, sehe aber die vorgesehene Zentralisierung kritisch. Ob mit den Regelungen, die im Entwurf vorliegen, die beabsichtigte Rechtssicherheit zu erreichen ist, ist fraglich.

Es ist geplant, mit einer Datenschutz-Grundverordnung ("Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)") europaweit einheitliche Datenschutzregelungen für Unternehmen und Behörden zu schaffen (Entwurf der EU-Kommission: KOM (2012) 11). Diese Regelungen wären nicht mehr in nationales Recht umzusetzen, sondern gälten unmittelbar.

Die geplante "JI-Richtlinie" ("Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr") soll für die zuständigen Behörden mit den genannten Aufgaben gelten (Entwurf der EU-Kommission: KOM (2012) 10). Sie wäre noch in nationales Recht umzusetzen.

Beide Regelungen befinden sich zurzeit im Rechtssetzungsverfahren der EU.

Es ist erfreulich, dass sich im Entwurf der Grundverordnung einige moderne Ansätze wiederfinden:

- Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten
- Datenschutz durch Technik
- Datenschutzfreundliche Voreinstellungen
- Datenübertragbarkeit

- Mehr Transparenz durch mehr Informationspflichten
- Recht auf Vergessenwerden.

Die vorgesehenen verschärften Sanktionen bei Datenschutzverstößen können zu einer besseren Durchsetzung des Rechts beitragen. Bei einigen Neuerungen bestehen allerdings bereits jetzt Zweifel, ob sie durchsetzbar sind.

Ob die Grundverordnung das in Nordrhein-Westfalen und in Deutschland bestehende Datenschutz-Niveau beibehält, verbessert oder verschlechtert, ist in vielen Bereichen kaum einzuschätzen. Dies liegt auch daran, dass die Grundverordnung häufig generell gefasste Regelungen vorsieht, die erst durch die EU-Kommission ausgefüllt werden sollen.

Es ist zu befürchten, dass Folge dieser Unbestimmtheit zumindest erhebliche Unsicherheiten in der Rechtsanwendung für alle Beteiligten und in vielen Bereichen auch eine Abschwächung des Datenschutz-Niveaus sein werden. Die Grundverordnung sollte auch deshalb die Möglichkeit eröffnen, auf der Basis eines Mindestniveaus durch einzelstaatliches Recht weitergehende Regelungen zu treffen.

Die häufigen Ermächtigungen der Kommission, delegierte Rechtsakte zu erlassen, sollten zudem überprüft werden. Die wesentlichen Punkte müssen in der Verordnung selbst oder durch Gesetze der Mitgliedstaaten geregelt werden.

Die Anforderungen an technische und organisatorische Maßnahmen, die Datenschutz und Datensicherheit gewährleisten, sollten moderner geregelt werden: Dazu sollten die elementaren Datenschutzziele – Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit – als Ziele für technische und organisatorische Maßnahmen vorgegeben werden.

Der "One-Stop-Shop", bei dem eine Aufsichtsbehörde für ein Unternehmen zuständig ist, ist nur praktikabel, wenn die Regelung keine ausschließliche Zuständigkeit bestimmt, sondern eine "Federführung" festlegt. Sie sollte bei Sachverhalten, die schwerpunktmäßig die Anwendung nationalen Datenschutzrechts betreffen, nicht zur Anwendung kommen.

Das Kohärenzverfahren bindet die Aufsichtsbehörden in ein komplexes Konsultationsverfahren ein. Dies führt zu einer erheblichen Bürokratisierung und kann die Unabhängigkeit der Aufsichtsbehörden beeinträchtigen. Das Verfahren sollte vereinfacht, praktikabler gestaltet und auf die wesentlichen Fallgruppen beschränkt werden.

Die Unabhängigkeit der Aufsichtsbehörden, die in der Grundrechtecharta und im Vertrag über die Arbeitsweise der EU festgeschrieben ist, gilt auch gegenüber der EU-Kommission. Die vorgesehene Befugnis zur Letztentscheidung der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wäre damit nicht vereinbar.

Im Detail gibt es in vielen weiteren Bereichen Diskussionsbedarf. Ich hoffe, dass im weiteren Rechtsetzungsverfahren viele Punkte noch geklärt werden können.

Den Meinungsaustausch mit den Stellen, die an der Reform des Rechtsrahmens beteiligt oder daran interessiert sind, werde ich fortführen. Den Landtag habe ich über meine Einschätzung unterrichtet (siehe Landtags-Vorlagen 16/69 vom 6. August 2012 und 16/539 vom 19. Februar 2013), ebenso die Landesregierung. Daneben hatte ich Gelegenheit, in zahlreichen Vorträgen, Diskussionen und Gesprächen mit Mitgliedern des Landtags und des Bundestages, Vertretern der Landesregierung und der Bundesregierung, Mitgliedern des Europäischen Parlaments und der Europäischen Kommission sowie mit verschiedenen Verbänden meine Sichtweise einzubringen.

Die Datenschutzbeauftragten und Aufsichtsbehörden des Bundes und der Länder sind sich in der Bewertung der bisherigen Entwürfe zum neuen Rechtsrahmen einig. Ich freue mich, dass auch die Landesregierung NRW meine Bewertung im Wesentlichen teilt.

- Mir ist wichtig, dass die europäischen Rechtsgrundlagen modernisiert, verbessert und weiter vereinheitlicht werden. Dabei dürfen das bisherige Datenschutzniveau und damit der bisherige Grundrechtsschutz in Nordrhein-Westfalen und in Deutschland nicht verschlechtert werden. Die Zentralisierung von Rechtsetzung und Aufsicht bei der EU-Kommission muss vermieden werden. Klare und bestimmte Reglungen sind erforderlich,

um die nötige Rechtssicherheit für alle Beteiligten zu erreichen. Für diese Ziele setze ich mich ein.

4.2 Keine Umsetzung der EU-Richtlinie 2009/136/EG – "Cookie-Richtlinie" – in nationales Recht

In der EU-Richtlinie 2009/136 EG (E-Privacy- oder "Cookie-Richtlinie") wurde 2009 festgelegt, dass die Verarbeitung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät einer Nutzerin oder eines Nutzers gespeichert sind, nur nach Einwilligung zulässig sind.

Die Frist zur Umsetzung dieser Richtlinie in nationales Recht ist am 25. Mai 2011 abgelaufen. Im Sommer 2011 hat der Bundesrat auf Initiative des Landes Hessen zur Umsetzung der "Cookie-Richtlinie" und weiterer Punkte eine Bundesratsinitiative zur notwendigen Änderung des Telemediengesetzes beschlossen. Diese wurde jedoch von der Bundesregierung zurückgewiesen. Ebenso ein weiterer Gesetzentwurf der SPD-Bundestagsfraktion. Von Seiten der Bundesregierung ist derzeit keine Bereitschaft erkennbar, das Telemediengesetz zu präzisieren.

➡ Auch wenn die Vorgaben der sogenannten "Cookie-Richtlinie" bislang in Deutschland nicht in eine Gesetzesänderung eingeflossen sind, empfehle ich nordrhein-westfälischen Internet-Diensteanbietern, die Vorgaben der Richtlinie zu beachten. Schließlich geht es um das zentrale Erfordernis, das Internet unbeobachtet nutzen zu können.

4.3 Die Entwicklung des Beschäftigtendatenschutzgesetzes kommt nicht voran

Die bisherigen Bemühungen zur Schaffung eines Beschäftigtendatenschutzgesetzes (siehe Bericht 2011 unter 7.1) sind ins Stocken geraten, nachdem die Gesetzesberatungen des Bundes bisher ergebnislos verlaufen sind.

Im Hinblick auf dieses wichtige Gesetzesvorhaben haben die Datenschutzbeauftragten des Bundes und der Länder Eckpunkte vorgelegt,

die die Anforderungen an eine ausgewogene gesetzliche Regelung markieren (siehe Entschließung "Beschäftigtendatenschutz stärken statt abbauen" vom 16./17. März 2011; Abdruck im Anhang). Die seit langem beklagten Defizite beim Umgang mit Beschäftigtendaten am Arbeitsplatz könnten durch normenklare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung solcher Angaben ausgeräumt werden. Die Schwachstellen des bisherigen Gesetzentwurfs ließen sich beheben, wenn die von den Datenschutzbeauftragten aufgezeigten Anforderungen berücksichtigt werden.

➡ Ich setze mich unverändert für ein Beschäftigtendatenschutzgesetz ein und hoffe, dass die Vorschläge der Datenschutzbeauftragten in vollem Umfang im Zuge weiterer Gesetzesberatungen aufgegriffen werden.

5 Wirtschaft und Medien

5.1 Verhaltensregeln in der Versicherungswirtschaft

Die Versicherungswirtschaft hat sich verbindliche Verhaltensregeln zum Umgang mit Daten von Kundinnen und Kunden sowie Antragstellerinnen und Antragsstellern gegeben. Die Datenschutzaufsichtsbehörden haben damit erstmalig Verhaltensregeln nach § 38a Bundesdatenschutzgesetz (BDSG) anerkannt.

Nach langen Verhandlungen haben sich der Gesamtverband der Deutschen Versicherungswirtschaft e. V. und die Datenschutzaufsichtsbehörden auf Verhaltensregeln verständigt. Die Verhaltensregeln sollen die Datenerhebungen und -verwendungen beschreiben und konkretisieren, die die Versicherungen auf gesetzlicher Grundlage vornehmen. Sie ergänzen insoweit die Datenerhebungen und -verwendungen, die auf die nunmehr ebenfalls abgestimmte Einwilligungs- und Schweigepflichtentbindungserklärung gestützt werden müssen (siehe Bericht 2009 unter 6.4 und Beschluss des Düsseldorfer Kreises "Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft" vom 17. Januar 2012; Abdruck im Anhang).

Die Versicherungsunternehmen, die den Verhaltensregeln beitreten, erkennen diese als verbindlich an und verpflichten sich, deren Vorgaben zu beachten. Beispielsweise ist geregelt, inwieweit sie Daten an Vermittler, Rückversicherer oder Dienstleister weitergeben dürfen und in welcher Form eine Einwilligung erteilt werden kann. Aber auch die Datenschutzaufsichtsbehörden binden sich mit Anerkennung der Verhaltensregeln in ihrer Prüfpraxis.

Nicht in allen Punkten konnte Einigkeit mit der Versicherungswirtschaft erzielt werden, so dass etwa zu Bonitätsabfragen und Scoring sowie zur Werbung lediglich auf die Regelungen des Bundesdatenschutzgesetzes verwiesen wird. Angesichts der Tatsache, dass es sich um die ersten Verhaltensregeln überhaupt handelt und die Prozesse bei Versicherungen einem steten Wandel unterliegen, ist von einem Lernprozess bei allen Beteiligten auszugehen. Daher ist eine Evaluation der Verhaltensregeln vorgesehen.

➡ Es bleibt abzuwarten, ob die Verhaltensregeln den "Praxistest" bestehen und weitere Branchen dem Vor-

bild der Versicherungswirtschaft folgen und sich eigene Verhaltensregeln geben werden. Ich habe mir zum Ziel gesetzt, vergleichbare Aktivitäten auch in anderen Branchen zu fördern und befinde mich mit den Verbänden der Wirtschaft im Dialog.

5.2 Elektronische Ticketkontrollen in Bussen

Wer mit Bussen im öffentlichen Nahverkehr fährt und im Besitz eines Abo-Tickets im Chipkartenformat ist, hat vermutlich schon erlebt, dass das Ticket beim Einsteigen zur Kontrolle an ein Lesegerät gehalten werden muss. Viele werden sich fragen, was bei einer solchen Ticketkontrolle geschieht. Wird erfasst, wann und wo ich Bus fahre?

Mit dieser Frage haben sich im Berichtszeitraum mehrere Fahrgäste an mich gewandt, insbesondere aus dem Bereich des Verkehrsverbunds Rhein-Ruhr (VRR). Datenschutzrechtlich verantwortlich ist nicht der VRR, sondern sind die verschiedenen Verkehrsunternehmen, die sich in dem Verkehrsverbund zusammengeschlossen haben. Da der VRR jedoch eine koordinierende Funktion in dem Verbund hat, habe ich zur Aufklärung des Sachverhalts auch ihn eingebunden. Dabei wurde über diese Frage hinaus eine regelmäßige Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten der Verkehrsunternehmen und des Verbunds vereinbart.

Nach den gewonnenen Erkenntnissen geschieht bei der elektronischen Einstiegskontrolle im Prinzip dasselbe wie bei einer herkömmlichen Kontrolle, bei der eine Kontrolleurin oder ein Kontrolleur mithilfe eines mobilen Lesegeräts die Fahrausweise überprüft. Einziger Unterschied: Bei der elektronischen Einstiegskontrolle wird das Ticket nicht nur gelegentlich, sondern zu Beginn jeder Fahrt kontrolliert.

Das Kontrollgerät gibt ein Signal, wenn das Ticket räumlich und zeitlich gültig ist. Bei personengebundenen Karten werden der Busfahrerin oder dem Busfahrer zudem Name, Alter und Geschlecht des Fahrgastes angezeigt. Dies ermöglicht eine Plausibilitätskontrolle, ob die Person, die in den Bus einsteigt, auch tatsächlich Inhaberin oder Inhaber des Abonnements ist. In Zweifelsfällen kann die Vorlage eines Lichtbildausweises verlangt werden.

Während des Kontrollvorgangs wird zudem geprüft, ob sich das vorgelegte Ticket auf der VRR-Sperrliste befindet. Dort werden beispielsweise als verloren oder gestohlen gemeldete Tickets geführt. Sollte ein vorgelegtes Ticket auf der Sperrliste vermerkt sein, wird es auf elektronischem Wege als ungültig markiert.

Die personenbezogenen Daten, die zur Kontrolle aus dem Ticket ausgelesen werden, werden nicht im System gespeichert. Es kann also nicht nachvollzogen werden, wer wann welchen Bus genutzt hat. Solche Bewegungsprofile wären in jedem Fall unzulässig.

Die Verkehrsunternehmen haben ein berechtigtes Interesse zu überprüfen, ob ihre Fahrgäste ein gültiges Ticket haben. Hierzu ist es erforderlich, die genannten personenbezogenen Daten zu nutzen.

➡ Sofern die elektronische Ticketkontrolle datenschutzgerecht ausgestaltet ist, kann sie ein zulässiges Mittel gegen Schwarzfahren sein. Bewegungsprofile der Fahrgäste dürfen dabei jedoch nicht erstellt werden.

5.3 Telefonwerbung und untergeschobene Verträge

Mit einer Verschärfung der Regelung über die Einwilligung in telefonische Werbung in § 7 Abs. 2 Nr. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) im August 2009 sollten verbotenes Telefonmarketing eingedämmt und Verbraucherinnen und Verbraucher wirksamer vor unerbetenen Werbeanrufen und ungewollten Verträgen geschützt werden. Geändert hat sich wenig.

Nach den Bestimmungen der §§ 4a, 28 Abs. 3 Satz 1 Bundesdatenschutzgesetz wie auch des § 7 Abs. 2 Nr. 2 UWG ist ein Werbeanruf gegenüber einer Betroffenen oder einem Betroffenen nur dann zulässig, wenn diese oder dieser vorher ausdrücklich eingewilligt hat. In der Praxis ergeben sich aber erhebliche Beweisprobleme hinsichtlich der Rechtmäßigkeit von Werbeanrufen, solange die erforderliche Einwilligung auch mündlich erfolgen kann. Oft bleibt unbeachtet, dass die Unlauterkeit des Werbeanrufs nicht zwingend das Zustandekommen eines wirksamen Vertrages verhindert.

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Behörde für Bußgeldverfahren wegen unzulässiger Werbeanrufe kann oft nur mit aufwändigen Ermittlungen und durch umfangreiche Prüfungen den Nachweis eines Rechtsverstoßes erbringen. Aus diesem Grund und auch wegen der begrenzten Kapazitäten dieser Behörde konnte bisher die abschreckende Wirkung der eingeführten Sanktionsmöglichkeiten nicht in dem angestrebten Maß erreicht werden (Bußgeldhöhe bis zu 50.000 Euro).

In meiner Behörde ist die Zahl von Beschwerden wegen der Verarbeitung personenbezogener Daten, die im Rahmen unzulässiger Telefonwerbung erhoben werden, nach wie vor hoch.

Das Land Nordrhein-Westfalen hat im September 2010 mit dem "Entwurf eines Gesetzes zur Fortentwicklung des Verbraucherschutzes bei unlauterer Telefonwerbung" einen Gesetzesantrag in den Bundesrat eingebracht (siehe Bundesrats-Drucksache 557/10). Danach sollte im UWG zusätzlich geregelt werden, dass die vorherige ausdrückliche Einwilligung "in Textform" vorliegen müsse. Zudem sollte eine auf einen Vertragsschluss gerichtete Willenserklärung erst wirksam werden, wenn sie durch eine nachfolgende Erklärung in Textform innerhalb von zwei Wochen bestätigt werde. Nur die sogenannte "Bestätigungslösung" schütze wirksam vor untergeschobenen Verträgen. Der Bundesrat hat im Mai 2011 dem Gesetzentwurf zugestimmt. Die Initiative wurde jedoch vom Bund bislang nicht aufgegriffen.

➡ Betroffenen empfehle ich, besonders wachsam zu sein und im Rahmen solcher Telefonkontakte keine personenbezogenen Daten preiszugeben. Bei angeblich telefonisch geschlossenen Verträgen besteht immer die Möglichkeit, zunächst Auskunft über gespeicherte Daten und, je nach Sachlage, auch ihre Löschung zu verlangen. Hinzuweisen ist ferner auf das Bürgerliche Gesetzbuch, in dem für Fernabsatzverträge Regelungen über den Widerruf innerhalb von 14 Tagen vorgesehen sind.

5.4 Telefonbücher im Internet

Die Zahl der elektronischen Telefonbücher im Internet nimmt stetig zu. Immer mehr ausländische Anbieter bieten diese Teilnehmerverzeichnisse im Netz an. Eine Vielzahl dieser Angebote müssen rechtlich hinterfragt werden.

Aufgefallen sind diese Angebote durch häufige Beschwerden, die sich insbesondere auf Internetseiten beziehen, die ihren Ursprung in Polen haben. Zu nennen sind Internetseiten wie "post-adresse.de", "telefonbuch-suche.com" und "plusadresse.com".

Die gesetzlichen Vorgaben für gedruckte und elektronische Teilnehmerverzeichnisse finden sich in §§ 104, 105 Telekommunikationsgesetz. Teilnehmerinnen und Teilnehmer können in solchen Verzeichnissen geführt und über sie kann Auskunft erteilt werden, wenn sie dies beantragt haben. Sie bestimmen dabei selbst, welche Daten in den Verzeichnissen veröffentlicht werden. Die Anträge werden über den jeweiligen Telekommunikationsdiensteanbieter der Teilnehmerin oder des Teilnehmers gestellt. Ebenso werden von ihm gewünschte Änderungen durchgeführt. Die Zahl und die Form der Beschwerden lassen jedoch den Schluss zu, dass in den Teilnehmerverzeichnissen der oben genannten Anbieter die gesetzlichen Vorgaben nicht beachtet werden. Es werden dort sowohl Daten veröffentlicht, die bislang in keinem anderen "Telefonbuch" zu finden sind, als auch Angaben, die über den beantragten Umfang hinausgehen. Die Datenherkunft ist bislang völlig ungeklärt. Neben Beschwerden, die mir vorliegen, wurden auch schon Strafanzeigen gegen die Betreiber dieser Seiten erstattet. Die Strafverfolgungsbehörden haben diese Verfahren jedoch einstellen müssen, da eine Täterin oder ein Täter nicht ermittelt werden konnte. Meine Handlungsmöglichkeiten sind eingeschränkt, da sich meine Aufsicht auf öffentliche und nicht-öffentliche Stellen mit Sitz in Nordrhein-Westfalen beschränkt.

- ➡ Um diese und auch andere ausländische Angebote kontrollieren zu können, werde ich zukünftig eine noch intensivere Kooperation mit den Aufsichtsbehörden anderer Länder anstreben.

5.5 Smartphone – smarter Schutz der Nutzungsdaten

Die Verbreitung von Smartphones nimmt immer mehr zu. Neben der Kommunikation ermöglichen sie auch die mobile Nutzung verschiedenster Funktionen eines Computers. Mit den umfassenden Möglichkeiten dieser Geräte steigt allerdings auch das Risiko von Datenmissbrauch.

Insbesondere in Bezug auf die vielen teilweise kostenlosen Apps (Applikationen) sind in jüngster Vergangenheit zahlreiche Verstöße der Anbieter gegen Grundprinzipien des Datenschutzes und der Datensicherheit bekannt geworden. Zwar bieten diese Programme oft nützliche Informationen und Unterstützung im Alltag, allerdings "zahlen" die Nutzerinnen und Nutzer – nicht selten ohne es zu bemerken – mit ihren Standort-, Adress- und Nutzungsdaten. Unklar ist in vielen Fällen, wozu die Anbieter diese Daten nutzen. Daher ist vor Installation jeglicher Applikationen die gründliche Prüfung der Datenschutzhinweise dringend anzuraten. Bei Zweifeln sollte eine App nicht installiert werden.

Eine weitere Gefahr der Ausspähung persönlicher Daten liegt darin, dass auf Smartphones sowohl das Betriebssystem als auch andere Software durch die Hersteller in der Regel vorinstalliert sind. Daher haben die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis) im Mai 2011 einen gemeinsamen Beschluss gefasst, mit dem sie die Unternehmen ausdrücklich auffordern, datenschutzfreundliche Grundeinstellungen der Endgeräte und Betriebssysteme sicherzustellen (siehe Beschluss des Düsseldorfer Kreises "Datenschutzgerechte Smartphone-Nutzung ermöglichen!" vom 4./5. Mai 2011; Abdruck im Anhang).

Im Berichtszeitraum wurden auch gegen in NRW ansässige Hersteller von Smartphones Vorwürfe erhoben, auf den Geräten eine Spyware zu installieren, mit der personenbezogene Daten bis hin zu Kommunikationsinhalten aufgezeichnet und an die Mobilfunkbetreiber übermittelt würden. Meine Ermittlungen bei den Unternehmen ergaben, dass alle für den deutschen Markt produzierten Geräte nicht mit der betreffenden Software versehen sind.

➡ Auch bei Smartphones müssen Nutzerinnen und Nutzer selbst entscheiden können, wem sie ihre persönlichen Daten für welchen Zweck zur Verfügung stellen wollen.

Daher ist meine Kernforderung an die Hersteller von Endgeräten und an die App, "privacy by design" zu beachten, das heißt, Geräte und Software so zu konzipieren, dass heimliche Datenerhebung unterbleibt, Datenverarbeitungsprozesse transparent sind und die Nutzerinnen und Nutzer ungewollte Datenerhebung unkompliziert unterbinden können.

5.6 Auskunfteien: Selbstauskunft nur bei Vorlage einer Personalausweiskopie?

Bei der Einholung einer Selbstauskunft verlangen Auskunfteien oftmals die Vorlage einer Personalausweiskopie. Sie argumentieren, dass dies zu Identifizierungszwecken erforderlich sei. Betroffene Bürgerinnen und Bürger vermuten dahinter Schikane und eine unzulässige Datensammlung.

Seit der Neufassung des § 34 Bundesdatenschutzgesetz (BDSG) im Jahr 2009 können die Betroffenen einmal im Kalenderjahr eine unentgeltliche Selbstauskunft über die zu ihrer Person gespeicherten Daten bei Auskunfteien einholen. Von diesem Recht machen die Bürgerinnen und Bürgern regen Gebrauch, was insbesondere in den ersten Jahren nach der Änderung zu einer Flut von Auskunftsbegehren bei den Auskunfteien führte.

Die Auskunfteien dürfen Selbstauskünfte nur an die tatsächlich betroffenen Personen erteilen und haben sich zuvor über die Identität der Antragstellerin oder des Antragstellers Gewissheit zu verschaffen. Zu diesem Zweck fordern viele Auskunfteien bei schriftlichen Anträgen eine Kopie des Personalausweises an. Für die Identitätsprüfung benötigen die Auskunfteien allerdings nur den Namen, die Anschrift und das Geburtsdatum der betroffenen Person.

Viele Betroffene befürchten, dass die Auskunfteien durch die Anforderung einer Personalausweiskopie weitere als die für die Identitätsprüfung erforderlichen Daten erheben, speichern und verarbeiten (etwa sensible Daten wie die Zugangs- und Seriennummer des Personalausweises). Zudem sehen viele die Vorlage einer Personalausweiskopie als Erschwernis und bürokratische Hürde an.

Verbraucherschützerinnen und Verbraucherschützer hingegen kritisieren immer wieder, dass Auskunfteien nicht generell Kopien von Ausweispapieren anfordern und oftmals Selbstauskünfte mit sensiblen Daten an nicht berechtigte Dritte übermitteln. Sie fordern die generelle Vorlage einer Ausweiskopie bei Einholung einer Selbstauskunft.

Zu diesem Spannungsfeld kommt hinzu, dass das im Jahr 2011 geänderte Personalausweisgesetz (PAuswG) die Verwendung von Personalausweisen restriktiv regelt und die Anfertigung von Personalausweiskopien von einigen Stellen aufgrund der Regelungen des PAuswG als unzulässig angesehen wird. Allerdings lässt sich weder der alten noch der neuen Fassung des PAuswG unmittelbar ein generelles Kopierverbot entnehmen. Der neue § 20 Abs. 2 PAuswG regelt lediglich die Unzulässigkeit des automatisierten Abrufs sowie der automatisierten Speicherung personenbezogener Daten zu anderen Zwecken als dem elektronischen Identitätsnachweis durch öffentliche und nicht-öffentliche Stellen. Der Entstehungsgeschichte der Vorschrift kann lediglich das Verbot des digitalen Kopierens der im Ausweis gespeicherten Daten entnommen werden. Reine Ablichtungen durch Ausweisinhaberinnen und -inhaber selbst oder auf deren Veranlassung zur Verwendung im Rechtsverkehr sind nicht per se untersagt. Ein generelles Vervielfältigungsverbot würde auch zu erheblichen Schwierigkeiten bei der praktischen Umsetzung des Auskunftsrechts der Betroffenen nach § 34 BDSG in den Fällen führen, in denen die Vorlage einer Ausweiskopie zum Zwecke des Identitätsnachweises in strittigen Fällen erforderlich ist.

Nach intensiver Erörterung der Frage sind Aufsichtsbehörden und Auskunfteien übereinstimmend der Auffassung, dass jedenfalls in folgenden Fallgruppen grundsätzlich keine Ausweiskopie vorzulegen ist:

- Die betroffene Person macht ihren Auskunftsanspruch nach § 34 BDSG in einem zeitlichen Zusammenhang zu einer vorherigen Benachrichtigung nach § 33 BDSG geltend (bis zu vier Wochen nach Benachrichtigung).
- Die Auskunftei hat keine Bonitäts- oder sonstigen Inhaltsdaten zu der betroffenen Person gespeichert.

Sofern Zweifel an der Identität der Auskunftsbegehrenden bestehen, kann die Auskunftei eine Kopie des Personalausweises verlangen, um

Übermittlungen personenbezogener Daten an Unbefugte zu verhindern.

Allerdings haben die Auskunfteien darauf hinzuweisen, dass Daten, die für die Identifizierung nicht erforderlich sind, geschwärzt werden können und sollten; dies gilt auch für das Passbild. Neben Name, Anschrift und Geburtsdatum kann zusätzlich die Angabe der Gültigkeitsdauer des Ausweises verlangt werden. Die Angabe des Geburtsortes darf nur verlangt werden, wenn die Auskunftei über ein entsprechendes Referenzdatum verfügt und dieses zur eindeutigen Identifizierung herangezogen werden soll.

Sobald die Personalausweiskopie zu Identifizierungszwecken nicht mehr benötigt wird, ist sie von den Auskunfteien zu vernichten. Sofern die Vorlage einer Personalausweiskopie von der betroffenen Person nicht gewünscht wird, besteht für sie die Möglichkeit, persönlich bei der Auskunftei vorzusprechen und dort den Ausweis lediglich vorzulegen.

➡ Soweit es zu Identifizierungszwecken erforderlich ist, dürfen Auskunfteien die Vorlage einer Personalausweiskopie mit Name, Anschrift, Geburtsdatum und zusätzlich der Gültigkeitsdauer verlangen. Weitere Daten dürfen nicht verlangt werden. Meine Behörde wird überprüfen, ob diese Vorgaben von den Auskunfteien eingehalten werden.

5.7 Anforderungen an die Ausleihe von Prüfungsprotokollen

Kaum eine angehende Juristin, kaum ein angehender Jurist kommt ohne sie aus: Protokolle von mündlichen Prüfungen zur Vorbereitung auf das Staatsexamen. Für die Examenskandidatinnen und -kandidaten sind die Protokolle vergangener Prüfungen häufig die einzige Möglichkeit, sich im Vorhinein einen Eindruck von den Prüferinnen und Prüfern und ihrem Prüfverhalten zu machen. Allerdings beinhalten die Protokolle eine Vielzahl personenbezogener Angaben über die prüfenden Personen, die nicht ohne weitere Prüfung übermittelt werden dürfen.

Das Sammeln und Entleihen von Gedächtnisprotokollen mündlicher Prüfungen des ersten und zweiten juristischen Staatsexamens sind seit vielen Jahren gängige Praxis und werden kommerziell angeboten. Den Interessentinnen und Interessenten werden von ehemaligen Prüflingen gefertigte Protokolle gegen Entgelt zur Verfügung gestellt. Schreiben sie anschließend Protokolle ihrer eigenen Prüfung und geben diese an das Unternehmen weiter, bekommen sie Rabatt auf das Entgelt.

Die Prüfungsprotokolle enthalten eine Fülle personenbezogener Daten über die jeweiligen Prüferinnen und Prüfer. In den Protokollen befinden sich Angaben über ihre Namen und ihre Person, Einschätzungen ihres Charakters sowie Schilderungen des Prüfungsverlaufs, insbesondere der gestellten Fragen und der Reaktion der prüfenden Person auf Antworten der Prüflinge.

Grundsätzlich ist das Sammeln, Aufbewahren und Übermitteln von Prüfungsprotokollen zulässig, wenn die folgenden Anforderungen eingehalten werden:

- Vorlage der Prüfungsladung

  Die jeweiligen Examenskandidatinnen und -kandidaten müssen ihr berechtigtes Interesse an den in den Protokollen enthaltenen Daten darlegen. Dafür ist die Vorlage der Prüfungsladung erforderlich. Die ausleihende Stelle darf also Protokolle nur an diejenigen übermitteln, die eine Prüfungsladung vorlegen. Zudem dürfen nur Protokolle der in der Ladung genannten Prüferinnen und Prüfer herausgegeben werden.

- Keine Weitergabe von Schmähkritik und Formalbeleidigungen

  Der Übermittlung der Protokolle dürfen keine schutzwürdigen Interessen der Prüferinnen und Prüfer entgegenstehen. Die in den Protokollen enthaltenen Ausführungen etwa zum Prüfverhalten, zu Aussagen während der Prüfung und zur Einschätzung und Bewertung dieses Verhaltens betreffen den beruflichen Bereich und damit die sogenannte Sozialsphäre.

  Soweit diese Sphäre betroffen ist, wertet die Rechtsprechung das Interesse am Schutz der Angaben nur im Falle schwerwiegender Auswirkungen auf das Persönlichkeitsrecht der Betroffenen als schutzwürdig. Derart beleidigende oder unangemessene Bewertungen können bei Äußerungen eines Prüflings, der die Prüfung als

ungerecht empfand, durchaus vorkommen. Deswegen sind die Protokolle vorab auf eventuell enthaltene Formalbeleidigungen und Schmähkritik hin zu kontrollieren und solche Passagen aus den Protokollen zu entfernen.

- Benachrichtigungspflicht bei erstmaliger Übermittlung

  Die jeweiligen Prüferinnen und Prüfer sind über die erstmalige Übermittlung von Protokollen zu ihrer Person sowie in groben Zügen über die Art der übermittelten Daten zu unterrichten (§ 33 Bundesdatenschutzgesetz - BDSG).

  Die Benachrichtigung muss dabei nicht an die meist unbekannte persönliche Anschrift der prüfenden Person erfolgen. Ausreichend ist, wenn die Benachrichtigung an die Betroffenen persönlich an ihre Dienststelle adressiert wird (Name, Dienststelle, "persönlich/vertraulich"), so dass sie nicht auf dem Dienstweg von Dritten zur Kenntnis genommen werden kann.

- Meldepflicht

  Des Weiteren muss die ausleihende Stelle die Meldepflicht an die zuständige Datenschutzaufsichtsbehörde einhalten (§ 4d Abs. 1 BDSG).

➡ Ich habe die Unternehmen auf die genannten Anforderungen an die Protokollausleihe hingewiesen.

6 Videoüberwachung

6.1 Keine Videoüberwachung des öffentlichen Verkehrsraums durch Private!

Auch wenn es Privatpersonen und privaten Unternehmen unter bestimmten gesetzlichen Voraussetzungen erlaubt ist, ihr Eigentum per Videoüberwachung zu schützen, endet diese Befugnis jedoch in der Regel an der Grundstücksgrenze.

"My home is my castle", denkt Eigenheimbesitzer A und wählt – um seine "Burg" hinreichend zu schützen – die Waffen der modernen Informationstechnologie: In einem Baumarkt seines Vertrauens erwirbt er eine Videoüberwachungsanlage und greift, da es sich um ein Sonderangebot handelt, beherzt zu: Kamera 1 richtet er auf seine Hausfront, Kamera 2 erfasst den Gehweg sowie den Straßenabschnitt vor seinem Grundstück, den er gelegentlich als Parkplatz nutzt, und Kamera 3 ermöglicht ihm eine vorsorgliche Überwachung des Nachbargartens der Familie B. Die Anschaffungen bleiben nicht lange unbemerkt, und trotz aller sonstigen Unstimmigkeit ist sich die Nachbarschaft hier schnell einig: So geht es nun wirklich nicht!

Die Anliegerinnen und Anlieger haben Recht: Soweit die Überwachung auf die Wahrnehmung des Hausrechts gestützt wird, schließt dies nicht auch das Recht ein, im Eigentum anderer Personen stehende Grundstücke, öffentliche Straßen, Wege und Plätze mitzuerfassen. Im Ausnahmefall kann eine Erfassung öffentlicher Verkehrsflächen nur gerechtfertigt sein, soweit es lage- und situationsbedingt unvermeidbar ist, diese einzubeziehen, etwa weil eine Hauswand, die schon mehrfach beschädigt wurde, unmittelbar an den Bürgersteig grenzt. Dann muss allerdings die Überwachung auf das zwingend notwendige Ausmaß beschränkt werden und darf in der Regel maximal einen Meter in den Verkehrsraum hineinreichen; außerdem dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen Dritter überwiegen. Nachbarin B fasst es zutreffend zusammen: "'Your home is your castle', aber alles andere ist grundsätzlich tabu!"

Auch wenn der Vorgang fiktiv ist, handelt es sich durchaus um keinen Fall, der der Phantasiewelt entliehen ist, sondern um tagtägliche Prüfungspraxis meiner Behörde. Dabei lehrt die Erfahrung: Nachbarschaftsstreitigkeiten lassen sich mit den Mitteln des Datenschutzes

nicht lösen, und doch muss in jedem Einzelfall darauf geachtet werden, dass sich die Videoüberwachung von Eigenheimen zumindest auf das eigene Grundstück beschränkt. Ferner müssen entsprechende Hinweisschilder so angebracht werden, dass Gäste noch vor Betreten des Grundstücks auf die Videoüberwachung aufmerksam gemacht werden.

Das Problem der zunehmenden Videoüberwachung öffentlichen Verkehrsraums durch Private setzt sich auch im Wirtschaftsleben fort: Einzelhandel, Versicherungen, Gastronomiebetriebe und andere Unternehmen erfassen bei dem Versuch, ihre Gebäude zu sichern, zunehmend Teile des öffentlichen Verkehrsraums. Der Einsatz von Software, um sogenannte "Privacy Zones" einzurichten, also Teile des Erfassungsbereichs auszublenden bzw. zu verpixeln, scheint dabei noch eher die Ausnahme als die Regel zu sein.

In einem Fall plante eine private Betreibergesellschaft dem Vernehmen nach sogar, den zentralen und mit festen Verkaufsständen versehenen Marktplatz einer großen Stadt durch Videokameras zu überwachen, weil es verschiedentlich zu Einbrüchen in die Verkaufsbuden gekommen war. Hier fehlte es nicht nur am Vorliegen eines der in § 6b Abs. 1 Bundesdatenschutzgesetz genannten zulässigen Zwecke der Videoüberwachung; es gab auch keine Belege für die Erforderlichkeit einer solchen Maßnahme, dagegen aber Anhaltspunkte, dass die schutzwürdigen Belange der betroffenen Marktbesucherinnen und -besucher überwiegen würden: Zum einen ist die Schutzbedürftigkeit regelmäßig in öffentlichen Räumen hoch, in denen sich Menschen typischerweise länger aufhalten und die zur Entfaltung der sozialen Kommunikation dienen, was vorliegend angesichts der Vielfalt von Verkaufsständen und einer großen Auswahl gastronomischer Angebote zweifellos der Fall war. Zum anderen würden durch die Videoüberwachung sämtliche Passantinnen und Passanten, die den dem Gemeingebrauch unterliegenden Platz in zweckentsprechender Weise zulässig nutzen, unter den "Generalverdacht" einer potentiellen Täterschaft gestellt.

Wird das insgesamt aufgezeigte Szenario einer ausufernden Videoüberwachung durch Private weitergedacht – und auch dazu bedarf es keiner besonderen Phantasie – besteht die Gefahr, dass zukünftig weite Teile des öffentlichen Verkehrsbereichs unzulässigerweise von privaten Videoüberwachungsanlagen erfasst werden, derer sich darüber hinaus eventuell auch die Polizei bedienen könnte. Das würde

zum einen das gesetzliche Erfordernis unterlaufen, polizeiliche Videoüberwachung ausschließlich bezogen auf Kriminalitätsschwerpunkte zuzulassen. Zum anderen würde vor allem aber auch das Recht der einzelnen Person verletzt, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung zu werden. Nach der Rechtsprechung des Bundesverfassungsgerichts gewährleistet das allgemeine Persönlichkeitsrecht nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen der Person, die sich in die Öffentlichkeit begibt, Rechnung (siehe BVerfG, Kammerbeschluss vom 23. Februar 2007, AZ: 1 BvR 2368/06). Einer ausufernden Videoüberwachung gilt es deshalb entschieden entgegenzuwirken, was in Zeiten, in denen die Videoüberwachungstechnologie immer preisgünstiger, bedienungsfreundlicher und leistungsstärker wird, eine stete Herausforderung darstellt.

➡ Ist es schon der Polizei nur in besonderen Ausnahmefällen erlaubt, öffentlichen Verkehrsraum mit Videotechnik zu erfassen, gilt dies erst recht für Private.

6.2 Keine Videoaufnahmen zu Techniktests auf Straßen

Forschung oder Techniktest? – Das ist dann die Frage, wenn ein Projekt im öffentlichen Verkehrsraum durchgeführt und dabei Videokameras eingesetzt werden sollen. Denn was zu dem einen Zweck in Ausnahmefällen zulässig sein kann, ist zum anderen Zweck noch lange nicht erlaubt.

Kameras sind längst auch im Bereich des öffentlichen Straßenverkehrs zu finden. So werden beispielsweise in Tunneln, auf Seitenstreifen oder vielbefahrenen Kreuzungen Kameras zu dem Zweck installiert, Verkehrsverläufe zu beobachten und den Verkehr zu lenken. Im Notfall kann die verantwortliche Stelle dann sofort eingreifen und geeignete Maßnahmen einleiten. Solange dabei nur Übersichtsaufnahmen gefertigt und weder Kfz-Kennzeichen noch sonstige personenbeziehbare Informationen erfasst werden, sind die Belange des Datenschutzes nicht berührt. Die Polizei setzt ihrerseits – bei hinreichendem Anfangs-

verdacht – Kameratechnik ein, um Geschwindigkeits- und Abstandsmessungen durchzuführen. Sie erfasst dabei die betroffenen Personen einschließlich der Kennzeichen ihrer Fahrzeuge personenidentifizierbar. Hierfür gibt es jedoch spezifische Rechtsgrundlagen.

Zunehmend planen darüber hinaus allerdings auch private Unternehmen und Forschungsteams, ihre Projekte im Bereich des öffentlichen Straßenverkehrs durchzuführen und Videokameras zu installieren, die das gesamte Geschehen zu Analysezwecken beobachten und ggfl. aufzeichnen oder zumindest Sequenzen zwecks späterer Auswertung von Messergebnissen erfassen sollen. Nicht immer werden die schutzwürdigen Belange der Verkehrsteilnehmerinnen und -teilnehmer hinreichend mit in die Projektplanung einbezogen und gewahrt.

Nach der bereits im vorhergehenden Beitrag ausgeführten Rechtsprechung des Bundesverfassungsgerichts gewährleistet das allgemeine Persönlichkeitsrecht nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen, der sich in der Öffentlichkeit begibt, Rechnung (siehe BVerfG, Kammerbeschluss vom 23. Februar 2007, a.a.O.).

Für die Unternehmen und Forschungsteams gibt es deshalb nur zwei Möglichkeiten:

Entweder es gelingt ihnen, ihre Vorhaben so zu konzipieren, dass mittels der Videokameras zu keinem Zeitpunkt personenbeziehbare Daten erfasst werden – eine Möglichkeit, die ohnehin stets vorrangig zu prüfen ist. Beispiele: Bei der Gesamterfassung einer Straßenszene müssen die Übersichtsbilder so unscharf sein, dass Personen weder erkannt noch durch Bildbearbeitung erkennbar gemacht werden können. Außerdem scheidet jegliche – auch die temporäre – Erfassung von Kfz-Kennzeichen aus, denn hierbei handelt es sich stets um personenbezogene Angaben (vgl. § 45 Satz 2 Straßenverkehrsgesetz). In Betracht kommt auch der Einsatz technischer Verfahren, die sicherstellen, dass Gesichter, Kfz-Kennzeichen usw. zuverlässig durch Verpixelung von Beginn an unkenntlich gemacht werden. Ist unter Berücksichtigung aller Umstände des Einzelfalles sichergestellt, dass keine personenbezogenen Daten erhoben und verarbeitet werden, werden die Belange des Datenschutzes nicht tangiert: Das Projekt kann durchgeführt werden.

Oder aber die Unternehmen und Forschungsteams müssten die personenscharfe Videobeobachtung oder -aufzeichnung im Rahmen ihrer Projekte auf eine Rechtsgrundlage stützen können. In Betracht kommt allein § 6b Abs. 1 Nr. 3 und Abs. 3 Bundesdatenschutzgesetz (BDSG). Zweifellos handelt es sich bei den Videokameras um optisch-elektronische Einrichtungen im Sinne der Vorschrift, mit denen ein Bereich des öffentlichen Straßenverkehrs und damit ein öffentlich zugänglicher Raum beobachtet werden soll. Es sei weiterhin unterstellt, dass die mittels der Kameras erhobenen Daten ausschließlich im Rahmen des Projektes verarbeitet und genutzt werden sollen. Dann müssten für die Beobachtung und Aufzeichnung jedoch insbesondere folgende Voraussetzungen erfüllt sein:

- Wahrnehmung eines berechtigten Interesses für einen konkret festgelegten Zweck:

  Bei dieser Tatbestandsalternative handelt es sich um einen bereits nach der Gesetzesbegründung eng auszulegenden Ausnahmetatbestand.

  Das BDSG erkennt die Berechtigung des Interesses institutionalisierter Forschungseinrichtungen, bestimmte wissenschaftliche Forschungsprojekte durchzuführen und zu diesem konkreten Zweck – soweit erforderlich – personenbezogene Daten zu verarbeiten, in verschiedenen Regelungszusammenhängen an. Dieses berechtigte Interesse kann deshalb auch im Rahmen des § 6b Abs. 1 Nr. 3, Abs. 3 BDSG Berücksichtigung finden. Dann müssen allerdings beide genannten Voraussetzungen erfüllt sein: Es muss sich um eine institutionalisierte Forschungseinrichtung handeln, und die Videoüberwachung muss zur Durchführung eines konkreten wissenschaftlichen Projekts erforderlich sein.

  Anders dagegen verhält es sich bei reinen Techniktests, bei denen Produkte unter Einsatz von Videokameras allein zu wirtschaftlichen und unternehmerischen Zwecken (Produktentwicklung und Qualitätssicherung) getestet werden sollen. Einem übergeordneten wissenschaftlichen Erkenntnis- oder Forschungszweck dienen diese Tests nicht. Hinsichtlich der Berechtigung dieses Interesses, öffentlichen Verkehrsraum aus

unternehmerischen Gründen zum "Versuchsfeld" für Realtests umzufunktionieren, habe ich erhebliche Bedenken.

- Erforderlichkeit, Verhältnismäßigkeit:

  Wenn die Videoüberwachung zur Wahrnehmung eines berechtigten Interesses für einen konkret festgelegten Zweck erfolgt, muss sie erforderlich sein, und es darf keine Anhaltspunkte dafür geben, dass die schutzwürdigen Belange der Verkehrsteilnehmerinnen und -teilnehmer überwiegen. Dies ist in jedem Einzelfall gesondert zu prüfen.

  Häufig lässt sich bereits die Erforderlichkeit der Verarbeitung personenbezogener Daten nicht feststellen, weil es beispielsweise im Rahmen eines Forschungsvorhabens auch genügen würde, Übersichtsaufnahmen einer Verkehrsszene zu fertigen oder Gesichter, Kfz-Kennzeichen usw. durch den Einsatz technischer Verfahren von Beginn an unkenntlich zu machen.

  Der Durchführung von reinen Techniktests stehen in der Regel die schutzwürdigen Belange der Verkehrsteilnehmerinnen und -teilnehmer entgegen.

  ➡ Die Verkehrsteilnehmerinnen und -teilnehmer müssen sich in aller Regel auch weiterhin von Kameras unbeobachtet im öffentlichen Verkehrsraum bewegen können. Die Straße darf nicht zur Feldteststrecke für private Unternehmen werden. Mit besonderer Aufmerksamkeit werde ich darüber wachen, dass die Freiheit des Einzelnen auch im öffentlichen Raum gewahrt bleibt (siehe ebenso den nachfolgenden Beitrag).

6.3 Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum

Derzeit schreiten Bestrebungen voran, Bürgerinnen und Bürger für unterschiedliche Zwecke mit "Erkennungstechniken" zu beobachten und ihre Verhaltensweisen zu analysieren. Der Einsatz erheblicher öffentlicher Mittel zur Förderung von entsprechenden Forschungsprojekten begegnet grundsätzlichen Bedenken.

Ziel dieser Projekte ist es, in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf "potenzielle Gefährder" frühzeitig zu entdecken. Zu derartigen Forschungsvorhaben zählt beispielsweise das Projekt INDECT ("Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung"), das von der Europäischen Union gefördert wird.

Mit Hilfe von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, soll das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Nicht "normgerechtes" Verhalten kann dazu führen, verdächtigt zu werden, zukünftig eine Straftat zu begehen.

Die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Entschließung zu der Thematik gefasst, für die ich mich sehr eingesetzt habe (siehe Entschließung "Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum - nicht ohne Datenschutz" vom 21./22. März 2012; Abdruck im Anhang).

Neben der Frage, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird, fordert die Konferenz, bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, die jeweils zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben zu informieren und ihnen Gelegenheit zur Stellungnahme einzuräumen. Ferner appellieren die Datenschutzbeauftragten an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen.

➡ Auch insoweit werde ich mit besonderer Aufmerksamkeit darauf achten, dass derartige, gleichsam auf Vorrat ohne Anlass unterschiedslos alle Bürgerinnen und Bürger erfassende Überwachungen im öffentlichen Raum nicht stattfinden. Hier geht es um Gefahren für die Freiheit der einzelnen Person, die weit über die mit der bisherigen Videoüberwachung verbundene Problematik hinausgehen.

6.4 Videoüberwachung in Handel, Gewerbe und Dienstleistung

Meine Behörde hat verstärkte Aktivitäten unternommen, um Unternehmen zu veranlassen, Videoüberwachung auch in Handel, Gewerbe und Dienstleistung datenschutzgerecht auszugestalten.

Sofern Eingaben von Beschäftigten oder Kundinnen und Kunden erkennen ließen, dass Videoüberwachungsanlagen etwa in Handelsunternehmen, Buchhandlungen, Bäckereigeschäften oder in der Gastronomie installiert worden sind, habe ich regelmäßig mit den Unternehmensleitungen das Gespräch gesucht, um einen datenschutzgerechten Einsatz dieses Überwachungsinstrumentariums in allen Betriebsteilen zu gewährleisten. Da meine Behörde der Vielzahl von Eingaben kaum im Einzelnen nachgehen könnte, ist die Vorgehensweise, Probleme "von oben" aufzugreifen, besonders geeignet, in der Fläche den Datenschutz zu verbessern. Während sich Unternehmensleitungen, wie zahlreiche Kontakte bestätigt haben, durchweg einsichtsvoll zeigten, Datenschutzmängel in eigener Verantwortung abzustellen, ist bei manchem Interessenverband indessen noch Überzeugungsarbeit zu leisten.

So hat eine erste Diskussion mit dem Handelsverband Deutschland e.V. -Der Einzelhandel-, der die Datenschutzaufsichtsbehörden um ein Gespräch gebeten hatte, wie eine Videoüberwachung bei seinen Mitgliedsunternehmen datenschutzgerecht durchgeführt werden könne, bisher zu keinem befriedigenden Ergebnis geführt. In einer von mir moderierten Besprechung mit Vertreterinnen und Vertretern von Aufsichtsbehörden sowie des Verbands wurden die folgenden, für eine datenschutzgerechte Videoüberwachung in Handelsunternehmen unverzichtbaren Prüfungsschritte und Maßnahmen erläutert:

Nach Maßgabe des § 6b Bundesdatenschutzgesetz (BDSG) ist eine Videoüberwachung durch private Unternehmen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Kundinnen und Kunden sowie der Beschäftigten überwiegen. Damit genügt für Unternehmen und Betriebe kein bloßer Verweis auf einen der gesetzlich genannten Zwecke zur Rechtfertigung des Einsat-

zes der Videoüberwachung. Eine Diskussion allein des Gesetzesmerkmals der "Wahrnehmung berechtigter Interessen" verdrängt nicht pauschal die übrigen Tatbestandsvoraussetzungen des § 6b BDSG.

Der Einzelhandel ist durch verschiedene Erscheinungsformen geprägt, z.B.:

- Branche (z.B. Lebensmittel, Bekleidung, Kosmetik, Sportartikel, Bücher, Elektronik, Bereiche in Tankstellen oder Apotheken),
- Betriebsform (z.B. Bedienungs- oder Selbstbedienungsgeschäft, Filialunternehmen, Galerien, Ladenpassagen),
- Kombinierte Erscheinungsformen (Einzelhandel kombiniert mit Gastronomie, z.B. Cafés in Buchhandlungen; Cafés/Kaffeehausketten mit Warenverkauf).

Eine Beurteilung der Zulässigkeit einer Videoüberwachung auch bei vergleichbaren Erscheinungsformen ist nicht schematisch möglich. Vielmehr können weitere Faktoren (z.B. örtliche Lage, Vorkommnisse in der Vergangenheit) ausschlaggebend sein, die stets eine auf den jeweiligen Einzelfall bezogene Beurteilung erfordern.

Im Hinblick auf die verschiedenen Tatbestandsvoraussetzungen des § 6b BDSG sind deshalb folgende Punkte zu berücksichtigen:

- Beobachtung und/oder Aufzeichnung:
- Nicht nur die Videoaufzeichnung, sondern bereits ein Beobachten mittels Videokameras stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung Betroffener dar. Der Einwand, dass eine Aufzeichnung (z. B. im Black-Box-Verfahren), die nur bei Feststellung bestimmter Vorkommnisse gesichtet und ansonsten nach einer im vorhinein festgelegten Frist ungesehen gelöscht werde, weniger intensiv in die Rechte der Betroffenen eingreife als eine Beobachtung, vermag in dieser Allgemeinheit nicht zu überzeugen. Datenschutzrechtlich relevant ist vielmehr, dass personenbezogene Daten durch eine Aufzeichnung reproduzierbar festgehalten werden und so weiteren Personen zugänglich gemacht werden können. Damit bleibt das Risiko einer missbräuchlichen Verwendung von Daten insoweit größer als bei einer reinen Beobachtung.

- Die Zulässigkeit einer Beobachtung und/oder Aufzeichnung mittels Videokameras hängt unter anderem davon ab, welcher Zweck hiermit jeweils verfolgt wird. Beispiele: Bezweckt Videoüberwachung ein direktes Einschreiten in Gefahrensituationen, wird regelmäßig eine Beobachtung ausreichen. Steht eine nachträgliche Aufklärung von Schadensfällen oder Straftaten im Vordergrund, kann eine Aufzeichnung in Betracht kommen.

- Wahrnehmung des Hausrechts

  Die Verhinderung von Straftaten (z.B. Diebstahl, Sachbeschädigung, Raubüberfälle) und deren beweiskräftige Zuordnung zu bestimmten Personen gehört zur Wahrnehmung des Hausrechts. Allerdings kann sich hierauf nur berufen, wer zur Ausübung des Hausrechts befugt ist (Beachtlich ist dies etwa bei Betreibern von Einkaufszentren, die zur Wahrnehmung des Hausrechts zwar in den Ladenpassagen, nicht aber in den vermieteten Geschäften berechtigt sind.).

- Wahrnehmung berechtigter Interessen

  Hierbei handelt es sich um einen nach dem Willen des Gesetzgebers eng auszulegenden Ausnahmetatbestand: Es muss sich um berechtigte Interessen der für die Videoüberwachung verantwortlichen Stelle handeln. Die allgemeine Strafverfolgung ist nicht Aufgabe privater Stellen, sondern bleibt den Strafverfolgungsbehörden vorbehalten.

- Erforderlichkeit und Verhältnismäßigkeit

  Eine Videoüberwachung kommt nur in Betracht, wenn keine anderweitigen, die Betroffenen weniger beeinträchtigenden Möglichkeiten zur Erreichung des angestrebten Zwecks bestehen. Selbst wenn eine Videoüberwachung als erforderlich angesehen werden sollte, darf sie nur erfolgen, wenn der hiermit verbundene Eingriff in die Rechte der Betroffenen zu dem angestrebten Ziel nicht außer Verhältnis steht. Insoweit stellen sich beispielsweise folgende Fragen:

  Welche konkreten Vorkommnisse gab es in der Vergangenheit?

  Auf welche konkreten sicherheitsrelevanten oder gefährdungsgeneigten Bereiche ist die Videoüberwachung auszurichten

(keine flächendeckende Videoüberwachung, kein Erfassen der persönlichen Identifikationsnummern von Bankkarten beim bargeldlosen Bezahlen)?

Welche organisatorischen Maßnahmen sind vorrangig zu ergreifen (z.B. bei Warenumtausch)? Genügt eine Videoüberwachung zu bestimmten Zeiten (z.B. zur Gebäudesicherung außerhalb der Geschäftszeiten)?

- Offene oder verdeckte Videoüberwachung

  Eine verdeckte Videoüberwachung kommt nach § 6b BDSG nicht in Betracht.

- Beschäftigtendatenschutz

  Die verantwortlichen Stellen im Einzelhandel müssen insbesondere den Beschäftigtendatenschutz berücksichtigen. In erster Linie ist hier zu beachten, dass eine dauerhafte verdachtslose Überwachung von ständigen Arbeitsplätzen der Beschäftigten nach der arbeitsgerichtlichen Rechtsprechung unzulässig ist (siehe Bericht 2011 unter 7.3).

- Löschung

  Gespeicherte Daten müssen unverzüglich gelöscht werden (§ 6b BDSG). Der Gesetzgeber geht von einer Regelfrist von ein bis zwei Arbeitstagen aus, innerhalb der der Bedarf geklärt werden muss und zur Zweckerfüllung (z.B. zur beweiskräftigen Zuordnung von Straftaten zu Personen) nicht mehr benötigte Aufnahmen zu löschen sind.

- Vorabkontrolle

  Zudem ist eine Vorabkontrolle erforderlich, soweit automatisierte Datenverarbeitungen bei der Videoüberwachung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen (§ 4d Abs. 5 BDSG). Eine komplex ausgestaltete Videoüberwachung im Einzelhandel wird regelmäßig eine solche dem Datenschutz und der Datensicherheit dienende Maßnahme erfordern.

Im Hinblick darauf, dass der Handelsverband Deutschland e.V. -Der Einzelhandel- im Sinne einer generalisierenden Betrachtung davon

ausgeht, die Durchführung einer Videoüberwachung sei wegen einer im Einzelhandel bestehenden Gefährdungslage grundsätzlich erforderlich, sind weitere Gespräche bisher als nicht zielführend erachtet worden. Dem Verband wurde vielmehr vorgeschlagen, interne Verhaltensregelungen gemäß § 38a BDSG zu erstellen, um diese anschließend im Düsseldorfer Kreis zu beraten.

In anderen Fällen hatte ich mehr Erfolg. In Besprechungen konnten ein Unternehmen der Gastronomiebranche sowie ein Arbeitgeberverband davon überzeugt werden, dass für Videoüberwachungen der Gästeaufenthaltsbereiche sowie der ständigen Arbeitsplätze der Beschäftigten keine Rechtsgrundlage besteht und diese Maßnahmen daher unzulässig sind. Das Unternehmen hat die einzelnen Kameraerfassungsbereiche überprüft und die vorgenommenen Änderungen dokumentiert. Die Videoüberwachung durfte danach in dem empfohlenen eingeschränkten Umfang weiterbetrieben werden. Der Arbeitgeberverband hat in Aussicht gestellt, auch andere Mitgliedsunternehmen bei Bedarf im Sinne des erzielten Ergebnisses zu beraten.

Einer von vielen weiteren Fällen betraf die im Ergebnis ebenso zufriedenstellende Überprüfung von Videoüberwachungseinrichtungen bei einem überregionalen Buchhandelsunternehmen mit zahlreichen Filialen, denen zum Teil Cafés angeschlossen sind. Vertretern der Unternehmensleitung und dem betrieblichen Datenschutzbeauftragten wurden insbesondere die zur Umsetzung der aufgezeigten Anforderungen gebotenen Maßnahmen erläutert. Nach eingehenden Überprüfungen hat das Unternehmen u.a. folgende Ergebnisse berichtet:

- Die geringe Anzahl der mit Videoüberwachung ausgestatteten Filialen wurde weiter reduziert. In von einem Wettbewerber übernommenen Filialen wird die Notwendigkeit von Videoüberwachungen mit dem Ziel überprüft, sie möglichst aufzugeben.
- In allen Filialen wurde vor Inbetriebnahme durch den betrieblichen Datenschutzbeauftragten unter Beteiligung der Geschäftsführung, der Filialleitung, des Betriebsrats und des mit der Montage der Anlage beauftragten Dienstleisters eine Vorabkontrolle durchgeführt.
- Die Filialleitungen wurden angewiesen, sämtliche Videokameras, die Café-Gäste aufnehmen könnten, zu entfernen oder ihre Ausrichtung so zu verändern, dass diese nicht abgebildet werden. An-

geordnet wurde ebenso, nicht betriebene Videokameras oder Attrappen zu entfernen, die bei Café–Gästen den Eindruck einer Videoüberwachung erwecken.

Besonderes Augenmerk sollte in Zukunft bei der Neueinrichtung oder der Modernisierung von Videoüberwachungsanlagen auch auf eine Prüfung der Angebote von Sicherheitsfirmen gelegt werden. Leider stehen Werbeaussagen, die offerierte Hard- und Software gewährleiste den Datenschutz, zuweilen nur auf dem Papier.

➡ Die Videoüberwachung in Unternehmen bedarf einer gründlichen betriebsinternen Überprüfung durch die Unternehmensverantwortlichen und ihre betrieblichen Datenschutzbeauftragten vor Ort. Darüber hinaus sind die Hersteller und Anbieter von Anlagen zur Videoüberwachung gefordert, die Belange des Datenschutzes schon bei der Geräteentwicklung und der Projektplanung einzubringen.

6.5 Ausbildung unter Videoüberwachung? – Nein danke!

Auf dem Sektor der Aus-, Fort- und Weiterbildung werden – neben öffentlichen Stellen – vor allem auch zahlreiche private Unternehmen tätig. Die Angebote sind dabei vielfältig, doch eines ist überall gleich: Videoüberwachung und Ausbildungssituationen passen nicht zusammen.

Für öffentliche Schulen und Ersatzschulen ist dieses Thema inzwischen ausdiskutiert. So konnte bereits im Bericht 2009 unter 4.2 über die Einigkeit mit dem Schulministerium in Sachen Videoüberwachung in Schulen berichtet werden: Unter Berücksichtigung der spezifischen Regelungen des Schulgesetzes Nordrhein-Westfalen (SchulG) ist eine Videoüberwachung während des laufenden Schulbetriebs in aller Regel unzulässig. Außerhalb des Schulbetriebs richtet sich die Zulässigkeit der Videoüberwachung nach § 29b Datenschutzgesetz Nordrhein-Westfalen (DSG NRW).

Doch wie verhält es sich mit Bildungseinrichtungen privater Anbieterinnen und Anbieter, die weder dem SchulG noch dem DSG NRW un-

terfallen? Eine Eingabe gab Anlass, dieser Frage bis hin zum Informations- und Kontrollbesuch vor Ort näher nachzugehen.

Vorgetragen worden war, dass in einem privaten Bildungsinstitut Computerräume mit Videokameras ausgestattet seien, mit denen die Teilnehmenden der Bildungsmaßnahmen sogar während der Unterrichtszeiten überwacht würden. Ein Auskunftsersuchen an das Institut brachte weitere Erkenntnisse: Die Überwachungsanlage bestand aus einer Vielzahl von Kameras, die in Unterrichtsräumen, Übungswerkstätten, Aufenthaltsbereichen, Fluren sowie dem Ein- und Ausgangsbereich installiert und dauerhaft aktiviert waren. Als Gründe hierfür wurden Diebstähle und Vandalismusschäden genannt; die Videoüberwachung sei als effektives Mittel zur Verhinderung ähnlicher Vorkommnisse erschienen und daher schrittweise ausgedehnt worden. Der erste Eindruck einer "Generalüberwachung" fand sich bei dem Ortstermin bestätigt; die Vielzahl der installierten Kameras ließ nicht erkennen, dass die Videoüberwachung zielgerichtet in einer Art und Weise erfolgte, zu der es keine weniger einschneidenden und die schutzwürdigen Belange der betroffenen Personen angemessen berücksichtigenden Alternativen gab.

Dies widerspricht jedoch der Wertung des Bundesdatenschutzgesetzes (BDSG): Nach Maßgabe des § 6b BDSG ist eine Videoüberwachung öffentlich zugänglicher Bereiche eines privaten Bildungsinstituts zur Wahrnehmung des Hausrechts nur zulässig, soweit sie erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Teilnehmenden, Lehrkräfte und sonstigen Beschäftigten überwiegen. Ob diese Voraussetzungen vorliegen, lässt sich letztlich nur in jedem konkreten Einzelfall unter Berücksichtigung aller besonderen Umstände – also bezogen auf jede einzelne Kamera und jeden überwachten Bereich – beurteilen. Einige Feststellungen gelten aber allgemein:

- Zur Erforderlichkeit: Auch wenn es vereinzelte Diebstähle und Vandalismusschäden gibt, darf weder mit "Kanonen" noch mit "Schrotflinten" auf "Spatzen geschossen" werden. Zunächst ist zu prüfen, ob keine weniger einschneidenden Maßnahmen (z.B. Angebot von Schließfächern, Abschließen von Schränken und Räumen außerhalb der Veranstaltungen) in Betracht kommen. Zu beachten sind dabei auch die jeweiligen Verantwortungssphären: Die Teilnehmenden haben selbst auf ihre

Wertsachen Acht zu geben und diese vor Diebstahl zu schützen. Damit geht die Verantwortung der Lehrkräfte einher, während ihrer Schulungsveranstaltung dafür Sorge zu tragen, dass das Institut weder durch Diebstähle noch durch Vandalismus geschädigt wird. Wenn alle ihrer Verantwortung Rechnung tragen, dürfte sich eine Videoüberwachung oft schon aus diesem Grund erübrigen.

- Zur Verhältnismäßigkeit: Sowohl die Teilnehmenden als auch die Beschäftigten haben ein überwiegendes schutzwürdiges Interesse daran, vor, während und nach den Schulungsveranstaltungen nicht durch Videokameras überwacht zu werden. Eine dauerhafte und flächendeckende Videoüberwachung scheidet deshalb aus. Wenn es wirklich nicht anders geht, kann eine punktuelle (z.B. gezielt auf Schränke, wertvolle technische Einrichtungsgegenstände wie Beamer oder Ausgänge von Selbstlernräumen gerichtete) oder temporäre (z.B. auf Zeiten außerhalb des Unterrichtsbetriebs beschränkte) Videoüberwachung in Betracht kommen, wobei auch hier stets die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen sind.

  ➡ In einer privaten Bildungseinrichtung kommt eine Videoüberwachung allenfalls als ultima ratio und auch nur dann in Betracht, wenn es keine Anhaltspunkte dafür gibt, dass die schutzwürdigen Belange der Teilnehmenden und Beschäftigten überwiegen. Videokameras gehören grundsätzlich weder in Schulungsräume noch in Bereiche, die in den Pausen sowie vor und nach dem Unterricht der Erholung dienen.

6.6 Videoüberwachung im Spielcasino

Spielcasinos sind oft mit umfangreichen Videoüberwachungsanlagen ausgestattet, um Besucherinnen und Besucher sowie Beschäftigte "im Auge" zu behalten. Bei Einrichtung und Betrieb dieser Anlagen sind jedoch die datenschutzrechtlichen Anforderungen zu beachten.

Meine Behörde hat die Videoüberwachung in einem Spielcasino überprüft. Anlass hierfür waren Meinungsverschiedenheiten zwischen Unternehmensleitung und Betriebsrat über den Umfang der Videoüberwachung in den Räumlichkeiten des Spielcasinos.

Nach einer Bestandsaufnahme war festzustellen, dass die mit Bildaufzeichnung erfolgende Überwachung der Räumlichkeiten durch die zahlreichen installierten Videokameras nicht etwa einheitlich nach § 8 Spielbankgesetz NRW (SpielbG NRW) zu beurteilen ist. Nach dieser den räumlichen Geltungsbereich festlegenden Vorschrift sind die Eingänge und Spielräume der Spielbank (Raumüberwachung) und die Spieltische (Spielüberwachung) zur Zugangskontrolle, zur Verhinderung, Aufdeckung und Verfolgung von Straftaten und zur Sicherung des Vertrauens der Öffentlichkeit in ein ordnungsgemäßes Spiel mit optisch-elektronischen Einrichtungen zu überwachen. In den betreffenden Bereichen waren 75 Videokameras installiert.

Zwischen der intensiven Betroffenheit der Beschäftigten durch die ständige Videoüberwachung und den Auswirkungen dieser Maßnahme auf die Besucherinnen und Besucher ist zu differenzieren: Während letztere wegen ihrer nur zeitweiligen Anwesenheit als Gäste im Spielcasino nur gelegentlich von der Videoüberwachung betroffen sind, unterliegen die Beschäftigten dieser Art der Überwachung auf Dauer und können ihr äußerstenfalls nur durch Aufgabe ihres Arbeitsverhältnisses entgehen. Daher ist insbesondere aus Gründen des Beschäftigtendatenschutzes zu prüfen, ob und ggf. welche Einschränkungen bei den Videoüberwachungsmaßnahmen geboten sind, ohne den Zweck des § 8 SpielbG NRW zu unterlaufen.

Hier bietet sich ein Rückgriff auf § 6b Bundesdatenschutzgesetz (BDSG) an. Diese Vorschrift ist neben § 8 Abs. 1 SpielbG NRW anwendbar. Nach § 6b Abs. 1 Nr. 3 BDSG ist – wie bereits zuvor dargelegt - die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die gemäß § 8 Abs. 1 SpielbG NRW konkret bestimmten Zwecke werden in Wahrnehmung berechtigter Interessen des Spielbankunternehmens grundsätzlich durch Einsatz von Videoüberwachungsmaßnahmen verfolgt werden können. Allerdings sind Videoüberwachungen unzulässig, wenn Anhaltspunkte für

überwiegende schutzwürdige Interessen der betroffenen Beschäftigten vorliegen. Insofern ist von erheblichem Gewicht, dass die lückenlose Überwachung der Räumlichkeiten des Spielcasinos einen weitreichenderen Eingriff in das Recht der betroffenen Beschäftigten auf informationelle Selbstbestimmung darstellt als eine lediglich anlassbezogene, z.B. auf kritische Spielverläufe beschränkte Videoüberwachung. Der damit vorliegende Zielkonflikt, dass auf die weiträumigen Videoüberwachungsmaßnahmen nicht verzichtet werden kann, weil sie gesetzlich vorgeschrieben sind und sich zudem als geeignetes Instrumentarium erwiesen haben, etwa unklare Spielverläufe im Interesse aller Beteiligten aufzuklären, lässt sich allerdings auflösen:

Insoweit kommen technisch-organisatorische Maßnahmen in Betracht, die dem Beschäftigtendatenschutz gerecht werden. Die Videotechnik ist z.B. imstande,

- bestimmte festzulegende Bildbereiche (insbesondere dauerhaft eingerichtete Arbeitsplätze von Beschäftigten) durch Verpixelung o.ä. auszublenden oder
- Objekte (etwa Körpersilhouetten) in zuvor markierten Bildbereichen unkenntlich zu machen, so dass diese auch bei einer Personenbewegung ausgeblendet bleiben.

Solche und weitere Maßnahmen können den mit der ständigen Erfassung der Beschäftigten einhergehenden Überwachungsdruck entscheidend verringern, ohne dass die gemäß § 8 Abs. 1 SpielbG NRW vorgeschriebenen Beobachtungszwecke in Frage gestellt werden. Mit diesen Maßnahmen werden die Persönlichkeitsinteressen der Betroffenen hinreichend berücksichtigt, und zugleich wird das Gebot der Datenvermeidung und Datensparsamkeit beachtet (§ 3a BDSG).

Die oben genannten Vorgaben gelten auch für andere räumliche Bereiche innerhalb der Spielbank, für die § 8 Abs. 1 SpielbG nicht ausdrücklich Anwendung findet, z.B. für die Kassenboxen. Auch dort müssen Maßnahmen zur zielgerichteten Videoüberwachung des Geldwechselvorgangs möglich sein, die mit den Anforderungen des Beschäftigtendatenschutzes in Einklang stehen.

Soweit sich die Videoüberwachung teilweise auch auf einen Gastronomiezwecken gewidmeten Raumbereich erstreckte, wurde darauf hingewiesen, dass dies zu einer erheblichen Beeinträchtigung des Persön-

lichkeitsrechts der dort verweilenden Gäste des Spielcasinos führt. Diese dürfen in solchen Räumlichkeiten Entspannung erwarten und nicht dem Gefühl ausgesetzt sein, dass ihr Verhalten ständig beobachtet wird. Durch eine einfache Ausblendung dieses Beobachtungsbereichs lässt sich dies vermeiden.

Im Übrigen hat der Casinobetreiber eine Löschung der gespeicherten Videobilddaten nach einem Zeitraum von sieben Tagen als bedarfsgerecht angesehen und damit die nach dem Spielbankgesetz maximale Aufbewahrungsdauer nicht ausgeschöpft.

- Dem Casinobetreiber wurden zahlreiche Hinweise zur Ausgestaltung der Videoüberwachung gegeben. Es empfiehlt sich, Einzelheiten zur Ausgestaltung und zum Ausmaß der Videoüberwachung unter Abwägung der gesetzlichen Anforderungen des § 8 SpielbG einerseits und des Beschäftigtendatenschutzes andererseits in einer Betriebsvereinbarung zu regeln.

7 Beschäftigtendatenschutz

7.1 Krankheitsatteste nicht an Fachvorgesetzte

Eine große Kommune hatte in einer Dienstordnung die Vorlage von Arbeitsunfähigkeitsbescheinigungen im jeweiligen Dienstbereich, mithin an unmittelbare (Fach-)Vorgesetzte geregelt. Dadurch sollten diese darüber informiert werden, ob Bedienstete mit attestierter Arbeitsunfähigkeit berechtigt der Arbeit fernbleiben und wie lange die jeweilige Arbeitsunfähigkeit voraussichtlich andauern wird. Dieser Meldeweg ist jedoch unzulässig.

Beamtete Beschäftigte einer öffentlichen Stelle haben eine krankheitsbedingte Dienstunfähigkeit gemäß § 62 Abs. 1 Satz 2 Landesbeamtengesetz NRW auf Verlangen nachzuweisen. Entsprechendes gilt für angestellte Beschäftigte gemäß § 5 Abs. 1 Satz 2 Entgeltfortzahlungsgesetz. Die Vorlage ist für die Durchführung des Dienst- und Arbeitsverhältnisses (z.B. für die Entgeltfortzahlung oder fürsorgerische Maßnahmen der Dienststelle) sowie für organisatorische Fragen der Personalplanung und des Personaleinsatzes erforderlich. Indessen ist nicht geregelt, welcher Stelle bei der Arbeitgeberin oder beim Arbeitgeber die Arbeitsunfähigkeitsbescheinigung (AU-Bescheinigung) vorzulegen ist.

Datenschutzrechtlich unzulässig ist die Vorgabe, die AU-Bescheinigung über Fachvorgesetzte an die Personalstellen einzureichen, weil aus dieser Unterlage auch die behandelnde (Fach-)Ärztin oder der behandelnde (Fach-)Arzt erkennbar ist und sich hieraus (etwa im Fall einer psychiatrischen Behandlung) Rückschlüsse auf die Art der Erkrankung ergeben können.

Die Vorlage der AU-Bescheinigung bei den unmittelbaren Vorgesetzten ist zudem nicht erforderlich. Für ihre weitere Planung genügt es, von der Arbeitsunfähigkeit und ihrer etwaigen Dauer zu erfahren. Eine Prüfung der Krankmeldung fällt insbesondere nicht in die Zuständigkeit der unmittelbaren Fachvorgesetzten. Dienst- oder arbeitsrechtlich erforderliche Maßnahmen werden von der Personalstelle eingeleitet und im Rahmen der Personalaktenführung berücksichtigt. Diese unterrichtet die Vorgesetzten lediglich über etwa erforderliche dienst- oder arbeitsrechtliche Maßnahmen.

Nachdem die Kommune zunächst an ihrer langjährigen Praxis festzuhalten gedachte, hat sie mitgeteilt, meiner Empfehlung zu folgen, die Attestvorlage neu so zu organisieren, dass die Nachweise der Erkrankung nicht den jeweiligen Fachvorgesetzten, sondern unmittelbar dem Fachbereich Personal und Organisation zugeleitet werden.

- Arbeitgeberin oder Arbeitgeber dürfen nicht verlangen, AU-Bescheinigungen zunächst den unmittelbaren Vorgesetzten vorzulegen. Die aus diesen Bescheinigungen ersichtlichen ärztlichen Fachgebiete lassen auf sensible Gesundheitsdaten der Beschäftigten schließen. Insoweit besteht eine Erhebungsbefugnis lediglich für die Personalstelle. Die Datenschutzpraxis in den öffentlichen Stellen werde ich auch insoweit weiter aufmerksam verfolgen.

7.2 Beschäftigtenüberwachung bei Logistikunternehmen

Vor Einsatz umfangreicher, mit Erhebungen und Speicherungen von Beschäftigtendaten verbundener Telematiksysteme ist stets zu prüfen, ob sich Unternehmensziele ohne solche Maßnahmen erreichen lassen.

Ein überregional tätiges Logistikunternehmen plante, ein telematisches Auswertungssystem einzurichten, das Fehlverhalten von mit Auslieferungsfahrten betrauten Beschäftigten lokalisieren und dokumentieren sollte. Im Vordergrund standen die Zwecke Unfallvermeidung und Kontrolle der beschäftigten Fahrerinnen und Fahrer. Unter anderem sollten die Fahrerinnen und Fahrer durch Kontrolle zu umweltschonenderem Fahrverhalten angehalten werden. Hierzu sollten die Daten des Auslieferungsfahrzeugs nach Erreichen der jeweiligen Niederlassung automatisiert auf einen zentralen Server übertragen und mit den Zustell- und Abholinformationen der Auslieferungsfahrerinnen und -fahrer verbunden werden. Die so verknüpften Daten sollten tabellarisch erfasst werden sowie 30 Tage abrufbar bleiben.

Das Unternehmen wurde darauf aufmerksam gemacht, dass aus Gründen des Beschäftigtendatenschutzes erhebliche Zweifel gegen

diese Vorgehensweise bestehen. Demgegenüber bieten sich einfachere und datensparsamere technisch-organisatorische Lösungen an, die bestimmte unerwünschte Verhaltensweisen ebenso verhindern, Gefahren im Straßenverkehr verringern und den Kraftstoffverbrauch senken können.

- So kommt etwa anstelle einer permanenten Aufzeichnung des Motorenlaufs im Stand der Einbau einer handelsüblichen elektronischen Motorabschaltung zur Kraftstoffeinsparung in Betracht.
- Zusätzlich zu bereits installierten Rückfahrkameras, die schon zu einer Reduzierung der Schadensfälle beim Zurücksetzen der Fahrzeuge geführt hatten, wurden ergänzende technische Maßnahmen (z.B. vom Fahrzeugheck ausgehende Intervall-Warnsignale) vorgeschlagen.
- Um zu vermeiden, dass Beschäftigte während der Fahrt die Eingabeterminals für die ausgelieferten Waren bedienen, reichen elektronische Dateneingabesperren aus. Zu diesem Zweck müssen Bedienungsdaten und Bewegungsdaten des Fahrzeugs nicht erfasst und abgeglichen werden.
- Auch soweit das Unternehmen sicherstellen will, dass Auslieferungsfahrten nur mit angelegtem Sicherheitsgurt durchgeführt werden oder kontrolliert werden soll, ob vor Fahrtantritt die Luke zwischen Fahrerbereich und Laderaum geschlossen ist, sind anstelle elektronischer Aufzeichnungen alternative technische Lösungen denkbar.

Das Unternehmen hat daraufhin mitgeteilt, zunächst von der Einführung des Telematiksystems abzusehen und anderweitige technische Möglichkeiten zu prüfen.

➡ Logistikunternehmen benötigen zur Erhöhung der Verkehrssicherheit bei Auslieferungsfahrten keine komplexen Telematiksysteme. An das Gebot des § 3a Bundesdatenschutzgesetz zur Datenvermeidung und Datensparsamkeit ist zu erinnern.

7.3 Risiken von Fernwartungssoftware – Schutz der Betriebsangehörigen

Unter Fernwartung versteht man den Fernzugriff mittels einer Fernwartungssoftware (auch "Remote-Software" genannt) auf Systeme, wie PCs, Server oder Industrieanlagen, zu Wartungs- und Reparaturzwecken. Eine Fernwartungssoftware ermöglicht, auf andere PCs zuzugreifen, Daten zu übertragen oder gemeinsam an Projekten zu arbeiten.

Ein missbräuchlicher Einsatz der Fernwartungssoftware, etwa zur Ausforschung der PCs von Beschäftigten, ist aus technischer Sicht grundsätzlich möglich. So können z.B. Tastaturanschläge und Mausbewegungen nahezu in Echtzeit übertragen werden. Auch können Support-Techniker die Bildschirmansicht eines fremden PCs auf dem eigenen Bildschirm wiedergeben. Fernwartungssoftware darf nur unter den jeweils geltenden materiell-rechtlichen Voraussetzungen und technisch-organisatorischen Bedingungen verwendet werden, die einen Missbrauch soweit wie möglich ausschließen. Maßnahmen zur technischen Absicherung von Fernwartung werden vom Bundesamt für Sicherheit in der Informationstechnik empfohlen (abrufbar unter www.bsi.de). Sie eröffnen einen Weg zur datenschutzgerechten Ausgestaltung derartiger Zugänge.

Zudem sind in § 9 Satz 1 Bundesdatenschutzgesetz sowie dessen Anlage 1 Anforderungen festgelegt, die auch bei einer datenschutzgerechten Gestaltung von Wartungsprozessen zu berücksichtigen sind. Dazu gehört insbesondere, dass nur autorisierte Personen Zugang zu den Anlagen haben, mit denen personenbezogene Daten verarbeitet oder genutzt werden, der Zugriff Unbefugter ausgeschlossen sowie zu gewährleisten ist, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Für öffentliche Stellen ergeben sich vergleichbare Anforderungen aus § 10 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen.

➡ Den Unternehmen empfehle ich unbeschadet betriebsverfassungsrechtlicher Beteiligungspflichten stets nachdrücklich, gemeinsam mit dem Betriebsrat für die erforderliche Transparenz zu sorgen. Nur gut informierte Mitarbeiterinnen und Mitarbeiter können darauf

vertrauen, dass Fernwartungssoftware nicht missbräuchlich eingesetzt wird. Entsprechendes gilt für öffentliche Stellen.

7.4 Abgleich von Beschäftigtendaten mit Terrorismuslisten

Vor allem Außenhandelsunternehmen sind an vereinfachten Verfahren bei der Zollabfertigung interessiert und lassen sich deshalb auf einen Abgleich ihrer in sicherheitsempfindlichen Bereichen tätigen Beschäftigten mit den sogenannten Terrorismuslisten ein. Dieser Abgleich ist Bedingung für eine vereinfachte Zollabfertigung.

Mit dieser Praxis haben sich die Aufsichtsbehörden des Bundes und der Länder (Düsseldorfer Kreis) erneut befasst und darauf hingewiesen, dass derartige Screenings nur aufgrund einer spezifischen Rechtsgrundlage zulässig wären, die bisher nicht besteht (siehe Beschluss des Düsseldorfer Kreises "Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen" vom 22./23. November 2011; Abdruck im Anhang).

Demgegenüber hat der Bundesfinanzhof entschieden, die Erteilung eines AEO–Zertifikats "Zollrechtliche Vereinfachungen/Sicherheit" (AEO = Authorized Economic Operator – zugelassener Wirtschaftsbeteiligter) dürfe von der Bedingung abhängig gemacht werden, dass antragstellende Unternehmen ihre in sicherheitsrelevanten Bereichen tätigen Beschäftigten einer Sicherheitsüberprüfung anhand der sogenannten Terrorismuslisten der Anhänge der VO (EG) Nr. 2580/2001 und der VO (EG) Nr. 881/2002 unterziehen (Urteil vom 19.6.2012 - VII R 43/11 -). Grundlegende datenschutzrechtliche Fragen werden mit dieser Entscheidung allerdings unbeantwortet gelassen:

So wird eine bereichsspezifische Regelung für den Datenabgleich nicht für erforderlich gehalten, weil es nicht um staatliche Eingriffe in Form gesetzlich auferlegter Verpflichtungen gehe, sondern lediglich um (gesetzlich zulässige) Bedingungen zur Erlangung bestimmter Erleichterungen für Zollabwicklungsverfahren, zu deren Inanspruchnahme kein Wirtschaftsbeteiligter verpflichtet sei. Unberücksichtigt bleibt bei die-

ser Begründung allerdings die Frage, aufgrund welcher Rechtsgrundlage ein Unternehmen zu einem solchen Datenscreening befugt sein soll. Der Umstand, dass insoweit kein staatlicher Eingriff vorliegt, ist unbeachtlich. Entsprechende Arbeitgeberverpflichtungen enthalten die EU-Antiterrorverordnungen nicht.

Die von den Zollverwaltungen erwarteten Beschäftigtendatenabgleiche im Rahmen der AEO-Zertifizierung sind im Übrigen nicht erforderlich, weil Kreditinstitute ohnehin bei der Gehaltszahlung nach § 25c Kreditwesengesetz einen Abgleich mit den Terrorismuslisten vornehmen müssen. Weitere gesetzliche, zu solchen Datenabgleichen verpflichtende Vorschriften bestehen nicht.

Unbefriedigend bleibt auch der nach wie vor nicht ausreichende Rechtsschutz Betroffener gegenüber einer Aufnahme ihrer Daten in die Terrorismuslisten der Europäischen Union.

➡ Die Unternehmen befinden sich in einer Zwangslage zu Lasten des Datenschutzes der Beschäftigten. Hier ist der Gesetzgeber auf Bundesebene gefragt. Darauf ist die Bundesregierung hingewiesen worden.

8 Gesundheit/Sozialdaten

8.1 Das "SozialTicket" des Verkehrsverbundes Rhein-Ruhr

Mehrere Kommunen im Bereich des Verkehrsverbundes Rhein-Ruhr geben Monatskarten aus, die den werbenden Schriftzug "SozialTicket" auf der Rückseite tragen.

Im Rahmen einer Fahrausweiskontrolle können Umstehende, auch ohne der Kontrolleurin oder dem Kontrolleur über die Schulter zu schauen, den Status als Sozialleistungsempfängerin oder -empfänger ohne Weiteres erkennen. Die Offenbarung dieses personenbezogenen Datums an andere Personen als die Kontrolleurin oder den Kontrolleur wäre jedoch nur auf Grund einer Rechtsvorschrift oder Einwilligung der Betroffenen zulässig. Der Verkehrsverbund Rhein-Ruhr will diesem Erfordernis gerecht werden.

- ➡ Bei Fortführung der Sozialtickets im Jahr 2013 muss ein neutraler Aufdruck vorgesehen werden, der keine Hinweise auf den Status der Ticket-Inhaberin oder des Ticket-Inhabers zulässt.

8.2 Transparenz beim Gesundheitsdatenschutz

Gesundheitsdaten sind gesetzlich besonders geschützt, weil sie einen sensiblen Lebensbereich betreffen. Deshalb müssen die Patientinnen und Patienten in besonderer Weise darauf vertrauen können, dass ihr Recht auf informationelle Selbstbestimmung gewährleistet ist. Ohne Transparenz können sie ihr Recht allerdings nicht oder nur eingeschränkt eigenverantwortlich wahrnehmen.

Soweit im Behandlungsverhältnis zwischen Ärztinnen und Ärzten sowie Patientinnen und Patienten Daten in der Praxis durch die dortigen Angestellten verarbeitet werden, sind die Verarbeitungsschritte für die Betroffenen in der Regel verständlich und überschaubar. Die Transparenz der Verarbeitung nimmt jedoch mit jeder weiteren Stelle, die hierin einbezogen wird, ab.

Bereits im Falle einer ambulanten und erst recht im Rahmen einer stationären Behandlung in einem Krankenhaus ist davon auszugehen, dass Beschäftigte verschiedener Aufgabenbereiche (etwa der Röntgenabteilung oder des krankenhauseigenen oder externen Labors) Daten der Patientin oder des Patienten verarbeiten. Eine weitere Datenverarbeitung erfolgt, sobald ein Rezept bei einer Apotheke vorgelegt wird, weil die Beschäftigten der Apotheke durch das verschriebene Medikament sowie die Fachrichtung der verschreibenden Ärztin oder des Arztes Anhaltspunkte für die zu behandelnde Krankheit erhalten. Diese Informationen geben sie weiter, wenn sie das Rezept der jeweiligen gesetzlichen Krankenkasse zu Abrechnungszwecken übersenden.

Als Grundlage für die Erstattung der Behandlungskosten erhält die gesetzliche Krankenversicherung der Patientin oder des Patienten von den Leistungserbringern Gesundheitsdaten, weil sie diese für die Abrechnung der Leistungen benötigt. Der privaten Krankenversicherung werden die erforderlichen Daten durch die Patientin oder den Patienten zum Nachweis der Aufwendungen mit dem jeweiligen Erstattungsantrag übermittelt.

Die Komplexität der Datenverarbeitung, die sich im Zuge der Entwicklung arbeitsteiliger Untersuchungen und Behandlungen sowie der Einschaltung technischer Unterstützungsstellen ergeben hat, ist für die Betroffenen kaum noch transparent. Vor diesem Hintergrund sind in besonderer Weise rechtliche und technische Sicherungen gefordert, wie nachfolgend geschilderte Bespiele verdeutlichen:

Werden Patientinnen und Patienten in einem Krankenhaus einer Untersuchung mittels eines medizinischen Großgeräts, etwa eines Kernspintomographen, unterzogen, können sie grundsätzlich nicht in vollem Umfang erkennen, wie ihre Behandlungsdaten während und infolge dieser Untersuchung verarbeitet werden. Erfordert ein Diagnostikgerät eine aufwändige Betreuung und Wartung durch eine spezialisierte Fachfirma, ist in manchen Fällen auch das Krankenhaus nur eingeschränkt in der Lage, die Datenverarbeitungsprozesse zu überschauen. Hier kann es ohne Kontrolle zu unübersehbaren Verarbeitungsschritten kommen, wie der unter Ziffer 3.5 geschilderte Einzelfall zeigt.

Eine andersartige Komplexität weist die Einschaltung von Apothekenrechenzentren auf. Zur Vereinfachung von Abrechnungen sowie zur

Arbeits- und Kostenreduzierung sind Apotheken dazu übergegangen, die von gesetzlich versicherten Patientinnen und Patienten eingereichten Rezepte nicht unmittelbar zur Zahlung an die jeweiligen Krankenkassen weiterzureichen, sondern sich hierauf spezialisierter Apothekenrechenzentren zu bedienen. Dies ist vom Gesetzgeber ausdrücklich zugelassen worden (§ 300 Abs. 2 Fünftes Buch Sozialgesetzbuch). Weil ebenso hier eine Fülle sensitiver personenbezogener Daten verarbeitet werden und der Gesetzgeber überdies die Verarbeitung und Nutzung für andere als Abrechnungszwecke in anonymisierter Form ausdrücklich zugelassen hat, ist in besonderem Maße darauf zu achten, dass die datenschutzrechtlichen Anforderungen eingehalten werden, zumal die Patientinnen und Patienten von solchen, über den eigentlichen Abrechnungszweck hinausgehende Datenverarbeitungen in der Regel keine Kenntnis haben.

Neben der allgemeinen Sicherheit der eingesetzten informationstechnischen Systeme kommt es wesentlich auf die Anonymisierung sämtlicher Daten an, die Rückschlüsse auf Patienten zulassen. Dazu gehören auch Daten über die beteiligten Ärzte. Dabei reicht es oft nicht aus, dass die personenbezogenen Daten (wie Name, Geburtsdatum, Wohnort usw.) durch technische Anonymisierungsverfahren "geschwärzt" werden. Aufgrund der immer besser werdenden Datenanalyseverfahren besteht insbesondere bei sehr großen Datenmengen die Gefahr, dass Verknüpfungen erstellt werden können, die zu einem zusätzlichen Informationsgewinn führen, der eine Identifizierbarkeit von Personen ermöglicht, die bei isolierter Betrachtung der Einzeldatensätze nicht möglich wäre. Insbesondere für die Pharmaindustrie tätige Markforschungsinstitute verfügen über solche Analyseverfahren und beziehen darüber hinaus in diese Auswertungen Daten ein, die sie aus einer Vielzahl anderer Quellen gewonnen haben. Ob mit den eingesetzten Verfahren eine Anonymisierung tatsächlich erreicht wird, bleibt zu prüfen.

- Alle im Gesundheitswesen beteiligten Stellen, angefangen bei den Ärztinnen und Ärzten über die Krankenhäuser bis hin zu den Kassen, deren Vereinigungen, Abrechnungsstellen, Versicherern und den Apotheken sind nicht nur im Interesse der Patientinnen und Patienten, sondern auch im eigenen Interesse aufgerufen, für größtmögliche Transparenz zu sorgen. Ferner sind Vorkehrungen zur Datensicherheit laufend zu über-

prüfen. Dies gilt ebenso für Gerätehersteller und Wartungsunternehmen.

8.3 Orientierungshilfe für Krankenhäuser

Komplexe Informationssysteme für Patientendaten müssen insbesondere in Krankenhäusern, wie die vorangegangenen Ausführungen zeigen, besonderen datenschutzrechtlichen und technischen-organisatorischen Anforderungen genügen. Notwendige Maßnahmen für ihre datenschutzgerechte Gestaltung und Nutzung sind in der "Orientierungshilfe datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen" zusammengefasst (abrufbar unter www.ldi.nrw.de).

Die Datenschutzbeauftragten des Bundes und der Länder haben diese Orientierungshilfe unter Mitarbeit von Datenschutzbeauftragten verschiedener Krankenhäuser und der Kirchen konzipiert. Beteiligt waren ferner verschiedene Experten und Hersteller von Krankenhausinformationssystemen.

Zum einen konkretisiert die Orientierungshilfe die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. Zum anderen werden Maßnahmen zur technischen Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die Krankenhäuser und deren Datenschutzbeauftragte liegt damit erstmals ein Orientierungsrahmen für eine datenschutzgerechte Gestaltung und Nutzung solcher Verfahren vor.

➡ Die Orientierungshilfe betrachte ich als wesentlichen Impuls zur Hebung des Datenschutzniveaus. Sie wird zukünftig als Maßstab bei der Bewertung konkreter Verfahren im Rahmen meiner Kontroll- und Beratungstätigkeit dienen. Meine Behörde befindet sich bereits in Gesprächen zur Anwendung der Orientierungshilfe.

9 Sport

Bekämpfung des Dopings im Sport

Sportlerinnen und Sportler, die an internationalen Wettbewerben teilnehmen möchten, müssen sich Dopingkontrollen unterwerfen, die zum Teil erhebliche Eingriffe in ihr Recht auf informationelle Selbstbestimmung darstellen. Trotz der erreichten Fortschritte sehe ich nach wie vor weiteren Handlungsbedarf, um den Datenschutzinteressen der Athletinnen und Athleten Rechnung zu tragen.

Insbesondere müssen nationale und europäische Datenschutzstandards über die Bundesregierung an die Welt-Anti-Doping-Agentur (WADA) herangetragen werden. Bereits im vorherigen Berichtszeitraum hatte ich im Dialog mit der Nationalen Anti-Doping-Agentur (NADA) auf datenschutzrechtliche Verbesserungen bei der Dopingkontrolle hingewirkt (siehe Bericht 2011 unter 9.). Ich verfolge dabei nach wie vor zwei Ansätze: Zum einen muss der nationale Spielraum für eine datenschutzfreundliche Anwendung der WADA-Vorgaben ausgeschöpft werden, zum anderen bedarf es einer Annäherung des Welt-Anti-Doping-Codes an das Datenschutzniveau der Europäischen Union. Dabei darf nicht verkannt werden, dass der internationale Leistungssport insbesondere mit Blick auf sportliche Fairness und den Gesundheitsschutz der Athletinnen und Athleten auf wirksame Dopingkontrollen angewiesen ist. Eingriffe in die Persönlichkeitsrechte der Betroffenen durch die Erhebung sensibler personenbezogener Daten müssen sich jedoch auf das erforderliche Maß beschränken.

Der NADA habe ich ein Konzept empfohlen, das einen unabhängigen Ombudsmann für Datenschutz vorsieht, der als Ansprechpartner für die Sportlerinnen und Sportler deren Beschwerden, Anregungen und Eingaben neutral aufgreift und mit ihnen Anregungen für datenschutzrechtliche Verbesserungen entwickelt. Der Ombudsmann hat seine Tätigkeit inzwischen aufgenommen. Die Anliegen der Betroffenen werden vertraulich behandelt, auch ist es möglich, dass sich Athletinnen und Athleten anonym an den Ombudsmann wenden.

Da die datenschutzrechtlichen Fragestellungen im Zusammenhang mit Dopingkontrollen einen internationalen Bezug aufweisen, können Lösungen nicht allein durch die deutsche Datenschutzaufsicht herbeige-

führt werden. Aus diesem Grund habe ich im Sportausschuss des Deutschen Bundestages meine Position verdeutlicht und die Bundesregierung eindringlich darum gebeten, sich für die Umsetzung meiner Vorschläge gegenüber der WADA einzusetzen.

Im Hinblick auf die Verhandlungen auf internationaler Ebene über die Revision des WADA-Codes und seiner Ausführungsbestimmungen habe ich der Bundesregierung empfohlen, mit Nachdruck darauf hinzuwirken, dass das im derzeitigen Meldesystem von der WADA vorgegebene hohe Maß an Zentralität und Verfügbarkeit von Daten korrigiert wird. Dabei sollten die folgenden Änderungen erreicht werden:

- Personenbezogene Daten der Sportlerinnen und Sportler sind grundsätzlich nur auf nationaler Ebene bei **einer** Stelle, in Deutschland bei der NADA, verfügbar.
- Die nationale Stelle prüft vor einer Übermittlung personenbezogener Daten an die WADA oder an andere Stellen, einerlei, ob im In- oder im Ausland, anhand definierter Tatbestände, ob die Voraussetzungen für eine personenbezogene Abfrage erfüllt sind.
- Die Übermittlung personenbezogener Daten ist nur in den einzelnen Fällen möglich, in denen eine Kontrolle beabsichtigt ist.

  Für das Zugreifen auf personenbezogene Daten sämtlicher Sportlerinnen und Sportler ohne näher definierten Anlass ist ein Grund nicht erkennbar, auch dann nicht, wenn das System nur innerhalb bestimmter Zeiträume vor Wettkämpfen einen Datenzugriff ermöglicht. Eine Auswertung von Daten auf aggregierter Grundlage sowohl bei der WADA als auch bei anderen Stellen reicht demgegenüber in der Regel aus, um prüfen zu können, ob und inwieweit – auf einer nächsten Stufe – personenbezogen weitere Kontrollen, durch wen auch immer, zur Gewährleistung gleicher Chancen bei Wettkämpfen geboten sind.
- Zur Weitergabe von personenbezogenen Daten in Länder ohne angemessenes Datenschutzniveau werden dort Vorkehrungen zum Schutz der Daten im Sinne von EU-Standards getroffen.
- Abfragen werden protokolliert.
- Das System stellt sicher, dass die nationale Stelle Auskunfts-, Löschungs- und Berichtigungsansprüche erfüllen kann, einerlei, ob

Daten bei der nationalen Stelle oder bei anderen Stellen verarbeitet werden.

Die Bundesregierung habe ich ferner gebeten darauf hinzuwirken, dass bei den Verhandlungen

- **Löschungsfristen** über Ergebnisse von Kontrolluntersuchungen auf das für Dopingkontrollen erforderliche Maß begrenzt werden,
- der **Minderjährigenschutz** sichergestellt wird und
- die als Sanktion gegen Doping-Verstöße im Internet vorgesehene **Veröffentlichung** im Hinblick auf Eignung und Angemessenheit überprüft und begrenzt wird.

➡ Die Notwendigkeit wirksamer Dopingkontrollen steht außer Frage. Angesichts des nach wie vor bestehenden Verbesserungsbedarfs werde ich mich auch weiterhin für den Schutz der Persönlichkeitsrechte der Sportlerinnen und Sportler bei Dopingkontrollen einsetzen. Dabei appelliere ich an die Bundesregierung, in die Verhandlungen zur Novellierung des Welt-Anti-Doping-Codes europäische Datenschutzstandards einzubringen.

10 Hochschulen

Vertrauen ist gut, Kontrolle noch besser? – Plagiatchecks in Hochschulen

Das Aufspüren von Plagiaten nimmt in der öffentlichen Diskussion breiten Raum ein. Was ist den Hochschulen erlaubt und was ist verboten?

Soweit zum Zweck dieser Überprüfung personenbezogene Daten der Kandidatinnen und Kandidaten verarbeitet werden, sind auch datenschutzrechtliche Aspekte berührt. Wie immer stellt sich dabei die Frage, ob es eine Rechtsgrundlage gibt, die diese Datenverarbeitung erlaubt.

Auf eine Einwilligung der Studierenden oder Doktoranden als Rechtsgrundlage kann die Plagiatüberprüfung bereits deshalb nicht gestützt werden, weil die erforderliche Freiwilligkeit einer Einwilligungserklärung nicht sichergestellt werden könnte: Die Betroffenen wären nicht frei in ihrer Entscheidung, sich für oder gegen einen Plagiatcheck zu entscheiden, sondern würden sich – um nicht in den Verdacht eines Täuschungsversuchs zu geraten – vielmehr gezwungen sehen, keine Einwände zu erheben.

Deshalb kommt nur eine Rechtsvorschrift als Grundlage für den personenbeziehbaren Einsatz von Plagiaterkennungssoftware in Betracht. Das Hochschulgesetz Nordrhein-Westfalen (HG) enthält selbst keine solche Bestimmung, verweist aber auf die ergänzende Anwendung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW). Nach Maßgabe der §§ 12 ff. DSG NRW ist das Erheben, Verarbeiten und Übermitteln personenbezogener Daten grundsätzlich zulässig, wenn es zur rechtmäßigen Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Auf dieser Grundlage kann die Verwendung einer Plagiaterkennungssoftware durch den Prüfungsausschuss im Einzelfall in Betracht kommen, um die Chancengleichheit aller Prüflinge zu wahren und eine gute wissenschaftliche Praxis sicherzustellen. Jedenfalls wenn eine Hochschule derartige softwaregestützte Kontrollen nicht nur in Einzelfällen, sondern regelmäßig durchführen möchte, sollte diese Überprüfung zuvor durch eine bestimmte und normenklare Vorschrift in den jeweiligen Prüfungs- und Promotionsordnungen der Hochschule geregelt werden. Gemäß § 64 Abs. 2 HG ist es den Hochschulen möglich,

Bestimmungen zur Aufdeckung von Plagiat- und Täuschungsversuchen zu erlassen. Nach Maßgabe dieser Vorschriften müssen Kandidatinnen und Kandidaten die Überprüfungen ihrer Arbeiten mittels Plagiaterkennungssoftware hinnehmen.

Hochschulen müssen im Rahmen der Plagiatchecks allerdings weitere Datenschutzstandards beachten, insbesondere

- bedarf es einer transparenten Gestaltung des Verfahrens des Einsatzes der Plagiaterkennungssoftware; empfehlenswert ist eine zusätzliche vorherige Information bzw. "Warnung" der Betroffenen;
- ist den Grundsätzen der Datenvermeidung und der Erforderlichkeit sowohl in Bezug auf das Verfahren der Plagiatfeststellung selbst als auch im Rahmen der Auswahl des Softwareprodukts Rechnung zu tragen;
- kann die Plagiaterkennungssoftware zwar Anhaltspunkte für einen Verstoß geben oder einen zuvor schon bestehenden Verdacht erhärten; die Entscheidung, ob es sich um ein Plagiat handelt und welche Folgen sich aus dieser Feststellung ergeben, bleibt jedoch nach wie vor dem zuständigen Prüfungsgremium vorbehalten und ist von diesem in eigener Verantwortung zu treffen; insoweit gilt das Verbot, Entscheidungen ausschließlich auf automatisierter Grundlage zu treffen (§ 4 Abs. 4 DSG NRW);
- bedarf es wie bei jedem Verfahren der automatisierten Datenverarbeitung eines Sicherheitskonzepts nebst Vorabkontrolle sowie eines Verfahrensverzeichnisses.

➡ Der Einsatz von Plagiaterkennungssoftware durch Hochschulen ist nur unter den beschriebenen Voraussetzungen zulässig.

11 Kommunales

11.1 Neuer Personalausweis: Zertifizierung kommunaler Zweckverbände

Die Nutzung des neuen Personalausweises zur elektronischen Identifikation (eID-Funktion) gegenüber Kommunen setzt dort Berechtigungszertifikate voraus. Bedienen sich die Städte und Gemeinden gemeinsamer Rechenzentren zur Abwicklung elektronischer Prozesse, kann diesen die Berechtigung jedoch nicht ohne Weiteres erteilt werden.

Vor der Einführung der neuen Personalausweise war ich auf Bundesebene an der Erarbeitung von Leitlinien zur Erteilung von Berechtigungszertifikaten beteiligt worden (siehe Bericht 2011 unter 12.2). Hierbei war zwar eine Vielzahl von Geschäftsprozessen bei Wirtschaftsunternehmen und Behörden in den Blick genommen worden. Das Tätigwerden von Rechenzentren im Auftrag von Kommunen war jedoch zum damaligen Zeitpunkt noch nicht Gegenstand der Überlegungen gewesen. Nach Inkrafttreten des Gesetzes sind das Bundesverwaltungsamt, Rechenzentren und kommunale Spitzenverbände wegen der Thematik an mich herangetreten: Das Auslesen personenbezogener Daten aus den Personalausweisen darf auch durch öffentliche Stellen ausschließlich im Rahmen und zur Erfüllung der eigenen, originär ihnen zugewiesenen Kernaufgaben erfolgen. Da IT-Dienstleister häufig keine eigenen Aufgaben im kommunalverfassungsrechtlichen Sinne wahrnehmen, sondern Datenverarbeitung im Auftrag, kommt deren Zertifizierung nicht in Betracht. Das Gesetz hat insoweit nicht die dienende Unterstützungstätigkeit von Rechenzentren im Blick. Zudem sieht das Gesetz über die kommunale Gemeinschaftsarbeit NRW nicht vor, dass sogenannte Pflichtaufgaben zur Erfüllung nach Weisung von den Kommunen auf IT-Dienstleister, die als Zweckverbände IT-Aufgaben für die Kommunen wahrnehmen, übertragen werden dürfen. Mit dem Ministerium für Inneres und Kommunales NRW, den Kommunalen Spitzenverbänden sowie mit dem für die Zertifikate zuständigen Bundesverwaltungsamt habe ich schließlich eine datenschutzgerechte und auch in der Praxis effektive Lösung entwickelt: Die Bearbeitung z.B. von Bürgeranträgen verbleibt nach wie vor bei der jeweiligen Kommunalverwaltung. Die beteiligten Gemeinden und Gemeindeverbände können allerdings einem Zweckverband die

Aufgabe übertragen, kommunale Bürgerportale und Bürgerkonten einzurichten, die die Verbindung zwischen Bürgerinnen und Bürgern und der Gemeindeverwaltung herstellen. Funktion dieser Portale und Konten ist ausschließlich die Identifizierung der Bürgerinnen und Bürger. Für die Wahrnehmung dieser Aufgabe benötigt der Zweckverband die Berechtigung zur Nutzung der eID-Funktionen des neuen Personalausweises im Sinne des Personalausweisgesetzes, die er in eigener Zuständigkeit beantragen kann. Den Zweckverbänden wurde empfohlen, ihre Satzungen zeitnah zu ergänzen.

- Kommunale Zweckverbände erhalten die Zertifizierung zur Nutzung der eID-Funktion der Personalausweise im Rahmen kommunaler Datenverarbeitung im Auftrag lediglich für die Identifikation von Bürgerinnen und Bürgern über Bürgerportale und Bürgerkonten.

11.2 Meldeportal für Behörden statt zentrales Melderegister

Nordrhein-Westfalen verzichtet auf die Errichtung eines zentralen Landesmelderegisters. Nach den Vorgaben des Bundesmeldegesetzes ist in diesem Fall jedoch für Behörden alternativ ein Online-Zugang zu den Meldedatenbeständen auf einer unteren Ebene zu eröffnen. Dieser Forderung will das Land mit der Errichtung eines Meldeportals für Behörden (MpB) nachkommen, das zum Inkrafttreten des neuen Bundesmeldegesetzes am 1. Januar 2014 einsatzbereit sein soll.

Zur Umsetzung dieses Projektes arbeitet das Ministerium für Inneres und Kommunales NRW federführend mit den beteiligten Behörden des Landes in einer Arbeitsgruppe zusammen und hat die D-NRW Besitz-GmbH & Co. KG mit der Projektleitung beauftragt. Die Arbeitsgruppe erarbeitet seit 2011 die notwendige Konzeption und die technischen Einzelerfordernisse des zu erstellenden Portals.

Seit Projektbeginn wirken Mitarbeiterinnen und Mitarbeiter meines Hauses beratend mit, um bei der Umsetzung des Projektes einen umfassenden Datenschutz zu gewährleisten. Es kommt darauf an sicherzustellen, dass den zugriffsberechtigten Behörden über das Meldeportal nur die Daten aus dem Melderegister zur Verfügung gestellt wer-

den, die für deren Aufgaben auch erforderlich sind. Der Zugang zu Meldedaten muss zu Kontrollzwecken nachvollziehbar gestaltet werden. Keinesfalls darf die Portallösung dazu führen, dass im praktischen Ergebnis Zugang zu sämtlichen Daten aller Meldebehörden, wie dies bei einem zentralen Melderegister möglich wäre, eröffnet wird. Zugang kann nur in der Weise gewährt werden, dass lediglich Daten der einzelnen Meldebehörde zur Verfügung stehen, deren Daten für den jeweils von der abrufenden Behörde zu bearbeitenden Einzelfall erforderlich sind (Zugang nur von Behörde zu Behörde).

➡ Die Errichtung des Meldeportals für Behörden ist aus der Sicht des Datenschutzes derzeit auf einem guten Weg. Meine Behörde wird das Projekt auch weiterhin begleiten.

11.3 Smartphonenutzung durch Ordnungsbehörden

Auch im Bereich der Erfassung von Verkehrsordnungswidrigkeiten werden neue technische Mittel eingesetzt. Mehr und mehr interessieren sich die Kommunen in Nordrhein-Westfalen für die Datenerfassung via Smartphone. Am Beispiel einer Großstadt habe ich darauf hingewirkt, dass Smartphones zur Erfassung von Verkehrsordnungswidrigkeiten datenschutzgerecht genutzt werden.

Durch einen Hinweis bin ich darüber informiert worden, dass die Beschäftigten im Außendienst der städtischen Verkehrsüberwachung zur Erfassung von Verkehrsordnungswidrigkeiten mit Smartphones ausgestattet wurden.

Bedenken, ob eine datenschutzgerechte Nutzung dieser Geräte für diese Zwecke überhaupt möglich ist, konnten im Dialog mit der Stadt ausgeräumt werden. Es ist gelungen, die Speicherung, die Verarbeitung der personenbezogenen Daten in den Geräten selbst und die Übertragungswege durch Verschlüsselung zu sichern. Außerdem sind die Gefahren der Mobilkommunikation, die sich durch die Nutzung von Geräteschnittstellen (Bluetooth, WLAN und NFC) ergeben können, durch weitere organisatorische Festlegungen und technische Sicherungsmaßnahmen berücksichtigt worden:

Die dort genutzten Smartphones sind auf die Erfassung von Verkehrsordnungswidrigkeiten, auf die Fotofunktion (zu Dokumentations- und Beweiszwecken) sowie die Telefonfunktion beschränkt worden. Alle weiteren Funktionen, wie beispielsweise der Lokalisierungs-Dienst (GPS) sowie die damit einhergehende Erfassung und Speicherung der Senderkoordinaten, sind mit Blick auf den Beschäftigtendatenschutz durch ein für diese Zwecke entwickeltes Konfigurationsprogramm deaktiviert worden.

Smartphones ersetzen bei der Stadt die herkömmlichen Erfassungsgeräte sowie eine zu Dokumentations- und Beweiszwecken von den Beschäftigten der örtlichen Ordnungsbehörde mitgeführte Fotokamera. Dies soll mit einer spürbaren finanziellen Entlastung bei Anschaffung und Wartung der Geräte einhergehen. Darüber hinaus wird durch die unverzügliche Übertragung der erfassten Daten der bislang übliche wöchentliche Datenabgleich mit den herkömmlichen Erfassungsgeräten entbehrlich und damit eine wesentlich schnellere Fallbearbeitung möglich.

➡ Die Entwicklung auch in anderen Kommunen werde ich auf der Grundlage der gewonnenen Erfahrungen aufmerksam beobachten.

12 Polizei und Justiz

12.1 Verfassungsrechtliche Anforderungen an Quellen-Telekommunikationsüberwachung

Der Bedarf der Ermittlungsbehörden, in schwerwiegenden Fällen auf Inhalte der Telekommunikation verdächtiger Personen zuzugreifen, besteht unabhängig davon, ob die Telekommunikation in verschlüsselter oder unverschlüsselter Form stattfindet. Der Zugriff auf verschlüsselte Kommunikation ist jedoch ungleich problematischer, weil dabei legitime und wichtige Selbstschutzmechanismen der Telekommunikationsteilnehmerinnen und -teilnehmer außer Kraft gesetzt werden müssen. Beim Zugriff auf die Daten vor ihrer Verschlüsselung muss auch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme beachtet werden.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27. Februar 2008 (1 BvR 370/07) zur sogenannten "Online-Durchsuchung" nach dem damaligen nordrhein-westfälischen Verfassungsschutzgesetz klargestellt, dass eine Durchsuchung von privaten Endgeräten und eine Erhebung der dort gespeicherten Daten nur dann verfassungsrechtlich zulässig sein können, wenn sie dem Schutz überragend wichtiger Rechtsgüter dienen und weitere, enge Eingriffsvoraussetzungen wie auch verfahrensrechtliche Grundrechtssicherungen gesetzlich klar festgelegt werden. Daher dürfen Verfassungsschutzbehörden in NRW bisher keine Online-Durchsuchungen durchführen.

Das Problem des Zugriffs auf informationstechnische Systeme besteht aber auch im Bereich der strafrechtlichen Ermittlungen. Bei der sogenannten Quellen-Telekommunikationsüberwachung installieren Ermittlungsbehörden auf dem privaten Endgerät eine Software, mit deren Hilfe sie Telekommunikationsdaten vor der Verschlüsselung ausleiten. Das Bundesverfassungsgericht hat in seiner oben genannten Entscheidung ausgeführt, dass die Quellen-Telekommunikationsüberwachung gegenüber der Online-Durchsuchung dann eine geringere grundrechtliche Tragweite hat, "wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Kommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."

Unter Berufung auf die Ausführungen des Bundesverfassungsgerichts vertreten die Datenschutzbeauftragten des Bundes und der Länder in einer gemeinsamen Entschließung die Auffassung, dass die Strafprozessordnung (StPO) derzeit keine hinreichenden Differenzierungen für Quellen-Telekommunikationsüberwachungen enthält, die die verfassungsrechtlichen Vorgaben im Einzelnen aufgreifen (siehe Entschließung "Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten" vom 16./17. März 2011; Abdruck im Anhang).

Die Ermittlungsbehörden des Bundes und der Länder suchen nach einer verbesserten Software, die sicherstellt, dass sich bei der Anwendung Zugriffe auf die Überwachung der laufenden Kommunikation beschränken und planen, eine solche unter Regie der öffentlichen Hand zu entwickeln. Hierfür soll ein besonderes Zertifizierungsverfahren eingeführt werden, das die technischen Anforderungen, insbesondere die Beschränkung auf die laufende Telekommunikation, sicherstellen soll.

Gegenüber dem Ministerium für Inneres und Kommunales NRW und dem Justizministerium NRW habe ich betont, dass die verfassungsrechtlichen Anforderungen nicht allein auf technischem Wege sichergestellt werden können. Im Rahmen der derzeitigen Rechtslage erfordern solche Maßnahmen zudem weitere organisatorische und verfahrenssichernde Vorkehrungen. Hierzu gehört insbesondere, dass nicht nur für die Anordnung solcher Maßnahmen, sondern auch für deren Durchführung eine Kontrolle durch unabhängige Stellen vorgesehen wird, die nicht selbst mit den Ermittlungen oder der technischen Durchführung der Maßnahme befasst sind.

➡ Die Umsetzung der verfassungsrechtlichen Vorgaben im Bereich der Quellen-Telekommunikationsüberwachung werde ich weiterhin kritisch begleiten.

12.2 Vorsicht bei Öffentlichkeitsfahndung im Internet

Die polizeiliche Personenfahndung durch Veröffentlichungen im Internet ist an sich schon ein derart schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht, dass sie nur in Ausnahmefällen in Betracht gezogen werden sollte. Noch schwieriger stellt sich die Situation dar, wenn die Veröffentlichung nicht auf polizeieigenen Seiten stattfindet, sondern pri-

vate Betreiber wie zum Beispiel Soziale Netzwerke einbezogen werden.

Nach einem Beschluss der Innenministerkonferenz von Ende Mai/Anfang Juni 2012 soll eine bundesweite Strategie zu Voraussetzungen und Rahmenbedingungen für die Nutzung von Sozialen Netzwerken bei polizeilichen Fahndungen im Internet entwickelt werden. Dies haben die Datenschutzbeauftragten des Bundes und der Länder zum Anlass genommen, in einem gemeinsamen Schreiben an die Vorsitzenden der Innenminister- und der Justizministerkonferenz auf die Gefahren hinzuweisen, die von der Internetfahndung an sich und der Einbindung Sozialer Netzwerke für die Grundrechte der davon betroffenen Personen ausgehen.

Grundsätzlich gilt, dass die Polizei nach der Strafprozessordnung bei der Suche nach tatverdächtigen Personen oder wichtigen Zeuginnen und Zeugen die Öffentlichkeit einschalten darf, wenn es sich um Ermittlungen wegen einer erheblichen Straftat handelt und die Aufenthaltsermittlung auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre. Wenn kein Haftbefehl vorliegt, ist die Anordnung der Maßnahme, die gravierende Auswirkungen für die Betroffenen haben kann, einer Richterin oder einem Richter vorbehalten.

Wird die Veröffentlichung der Personenangaben, zu denen auch ein Bild gehören kann, nicht nur in einem lokal oder regional begrenzten Medium, sondern im Internet vorgenommen, hat dies die weltweite — und damit regelmäßig über den für das konkrete Ermittlungsverfahren erforderlichen Radius hinausgehende — Verbreitung und Recherchierbarkeit der Daten zur Folge; ein Schutz gegen unbefugte und unbefristete Weiterverbreitung ist nicht vorhanden, und eine durchgreifende Löschung im Sinne einer vollständigen Entfernung aus dem Internet ist nicht möglich. Die Resozialisierung nach Verbüßung der Strafe oder auch eine Wiederherstellung des Ansehens bei zu Unrecht verdächtigten Personen wird damit faktisch unmöglich sein.

Weitere Probleme ergeben sich, wenn private Unternehmen, insbesondere Soziale Netzwerke, in die Fahndung eingebunden werden:

Werden die Angaben zur Personenfahndung auf der Homepage privater Betreiber veröffentlicht, so gelangen sie auf deren Server und damit auch in einen fremden Herrschaftsbereich, der nicht dem deut-

schen Datenschutzrecht unterliegen muss. Ferner ist die Polizei bei derartiger "Auslagerung" der Daten z.B. für Löschung oder Berichtigung auf die Mitwirkung fremder Betreiber angewiesen und damit nur noch bedingt Herrin des Verfahrens.

Im Berichtszeitraum ist nicht bekannt geworden, dass in Nordrhein-Westfalen Fahndungen mit Hilfe des Internets vorgenommen worden sind.

➡ Gegenüber Fahndungsaufrufen im Internet sind Personenfahndungen über traditionelle Medien wie Printmedien, Fernsehen und Radio vorzuziehen. Die Fahndung im Internet muss wegen ihrer gravierenden und zeitlich kaum limitierbaren Auswirkungen auf enge Ausnahmefälle beschränkt bleiben. Die Ermittlungsbehörden müssen dann darauf achten, die Kontrolle über die Veröffentlichung so weit wie im Internet möglich in eigener Hand zu behalten. Schließlich darf nicht übersehen werden, dass das Geschäftsmodell privater Sozialer Netzwerke vielfach gerade darauf gerichtet ist, personenbezogene Daten zu sammeln, auszuwerten und miteinander zu verknüpfen. Daher lehne ich eine öffentliche Fahndung mit Hilfe privater Sozialer Netzwerke ab.

12.3 Datenschutz für HIV-infizierte Gefangene kann ohne Sicherheitsverlust verbessert werden

Aufgrund einer Diskussion im Rechtsausschuss des Landtags NRW hat das Justizministerium NRW einen Erlass zum Umgang mit HIV-infizierten Gefangenen im Justizvollzug überarbeitet und durch eine Regelung ersetzt, die den medizinischen Erkenntnissen Rechnung trägt und zugleich das informationelle Selbstbestimmungsrecht HIV-infizierter Gefangener achtet.

Der Landtag hat sich mit der Übermittlung von Gesundheitsdaten in nordrhein-westfälischen Justizvollzugsanstalten befasst. In diesem Zusammenhang ist er der Frage nachgegangen, welche Konsequenzen sich für den alltäglichen Umgang mit Gefangenen ergeben sollen, wenn bei ihnen eine HIV-Infektion festgestellt wurde. Stein des Anstoßes war insbesondere ein Erlass des Justizministeriums aus dem Jahre

1988, wonach die Information über eine eventuell festgestellte HIV-Infektion und die Zustimmung der oder des Mitgefangenen zur Bedingung für einen Umschluss, also stundenweisen gemeinsamen Aufenthalt von Gefangenen in einem Haftraum, gemacht wurden.

In der Sachverständigenanhörung vor dem Rechtsausschuss habe ich darauf hingewiesen, dass bereits die anstaltsinterne Weitergabe von Gesundheitsdaten wie z.B. einer HIV-Infektion eine Durchbrechung der ärztlichen Schweigepflicht darstellt, die einer strengen Zulässigkeitsprüfung unterliegt. Ferner habe ich hervorgehoben, dass es bei der Prüfung, ob die Information (und das Einverständnis) Mitgefangener zur Bedingung für einen Umschluss gemacht werden darf, nicht darum geht, das Recht auf körperliche Unversehrtheit gegen das informationelle Selbstbestimmungsrecht abzuwägen. Vielmehr stellt sich die Frage, ob die Information über eine festgestellte Infektion überhaupt ein geeignetes und erforderliches Mittel zum Schutz der Mitgefangenen darstellt: Es besteht die Gefahr einer gefährlichen Fehleinschätzung, wenn eine Infektion nicht positiv festgestellt wurde. Außerdem haben Sachverständige aus medizinischer und psychologischer Sicht die Geeignetheit und Erforderlichkeit der Information über festgestellte Infektionen mit Blick auf Ansteckungsrisiken bei normalem sozialem Umgang und auf Selbstschutzmöglichkeiten bei Intimkontakten generell in Frage gestellt.

➡ In der neuen Regelung vom Mai 2012 wird die Umschlussmöglichkeit positiv getesteter Gefangener nicht mehr an Information und Einverständnis der Mitgefangenen geknüpft. Insgesamt setzt das Justizministerium NRW stärker auf Aufklärung über Übertragungswege schwerwiegender Infektionen und verbesserte Möglichkeiten zum Selbstschutz der Gefangenen. Damit wird es auch dem Datenschutz der Betroffenen gerecht.

12.4 Zentrale Haftdatei: Konzeption verbessert

Bei den Arbeiten zur praktischen Ausgestaltung der Zentralen Haftdatei hat meine Behörde beraten und konnte wichtige datenschutzrechtliche Verbesserungen erreichen.

Auf ursprünglich bestehende Bedenken hatte ich seinerzeit hingewiesen (siehe Bericht 2009 unter 8.1 und Bericht 2011 unter 13.4). Das Erfordernis, eine beschränkte Anzahl von Gefangenendaten für eine schnellere Information der Aufsichtsbehörde und zur leichteren Beauskunftung Dritter zum zentralen Abruf zur Verfügung zu stellen, ist nunmehr dargelegt.

Im Weiteren war allerdings die Daten haltende Stelle der Zentralen Datei und damit die datenschutzrechtliche Verantwortlichkeit für die Datenverarbeitung unklar. Außerdem war eine Rechtsgrundlage für die vorgesehenen anlasslosen Datenübermittlungen an diese zentrale Stelle nicht ersichtlich.

Gemeinsam mit den Projektverantwortlichen wurde daher eine Neukonzeption erarbeitet.

Nunmehr findet anstelle einer zentralen "Vorratsdatenhaltung" wenigstens nur noch eine anlassbezogene Abfrage der Daten statt, die im Rahmen des verwendeten Datenverarbeitungsverfahrens ohnehin bereits mandantenbezogen — also nach verantwortlichen Stellen, das heißt Justizvollzugsanstalten, getrennt — auf einem gemeinsamen Server abgelegt sind. Zudem habe ich erreicht, dass nicht standardmäßig alle etwa 20 in Frage kommenden Datensätze übermittelt werden, sondern der Umfang der Antwort je nach Zielrichtung der Anfrage konzipiert und damit auf das Erforderliche beschränkt wird.

- Die Neukonzeption der Zentralen Haftdatei ist ein Beispiel für eine konstruktive Zusammenarbeit zwischen Exekutive und unabhängiger Datenschutzbehörde. Nach Auskunft des Justizministeriums NRW kommt die gefundene Lösung auch für die Anwendung in anderen Ländern, die Gefangenendaten mit Hilfe des Datenverarbeitungsverfahrens bearbeiten, in Frage.

12.5 Bundesweites Schuldnerportal mit datenschutzrechtlichen Verbesserungen

Der gesetzgeberische Entschluss, ein Schuldnerportal im Internet einzurichten, ist zugleich mit erheblichen datenschutzrechtlichen Risiken verbunden. Es ist mir gelungen, hier auf einige wichtige Verbesserungen hinzuwirken.

Das bundesweite Vorhaben, die bisher bei den Vollstreckungsgerichten zur Einsichtnahme für Berechtigte bereit gehaltenen Schuldnerverzeichnisse im Internet zur Verfügung zu stellen, wurde von einer bundesweiten Arbeitsgruppe unter Federführung des Landes NRW umgesetzt. Von Beginn an waren Angehörige meines Hauses beratend eingebunden (siehe hierzu umfassend meinen Bericht 2011 unter 13.8).

So wurde zunächst die von mir kritisierte ursprünglich vorgesehene Identifizierung der Abfragenden durch Kreditkarten nicht umgesetzt und stattdessen ein mehrstufiges Identifizierungsverfahren eingeführt. Das bloße Ankreuzen des legitimierenden Abfragezwecks wurde um ein Freitextfeld ergänzt, in dem der Abfragegrund erläutert werden muss.

Weitaus schwieriger war jedoch die Durchsetzung der datenschutzrechtlichen Perspektive bei der inhaltlichen Konkretisierung von Abfrage und ausgegebener Antwort. Hier war zunächst geplant, bei Eingabe von wenigen Suchkriterien Trefferlisten anzuzeigen, durch die auch die Eintragung einer Vielzahl von Personen bekannt geworden wäre, auf die sich der Abfragezweck nicht bezogen hätte. Noch rechtzeitig konnte ich eine gemeinsame Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder initiieren, in der auf dieses Problem hingewiesen und eine datenschutzfreundlichere Lösung gefordert wurde (siehe Entschließung "Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke" vom 8. Februar 2012; Abdruck im Anhang). Daraufhin kam es in diesem wesentlichen Punkt zu einer Änderung. Bei einer Abfrage von Privatpersonen wird nunmehr verlangt, dass zusätzlich zu Namen und Vornamen sowie Wohnsitz oder Vollstreckungsgericht weitere Daten eingegeben werden müssen, wenn die Suchanfrage sonst zu keinem eindeutigen Ergebnis führen würde. Nur in dem — kaum praktischen — Fall, in dem auch Geburtsdatum und Geburtsort übereinstimmen, könnten noch Treffer zu mehreren Personen übermittelt werden. Dies stellt einen wesentlichen Fortschritt dar, auch wenn für Personen, die selbst nicht im Schuldnerverzeichnis stehen, die Gefahr, mit namensgleich eingetragenen Schuldnern verwechselt zu werden, nicht ganz ausgeräumt ist, weil Geburtsdatum und –ort nicht immer anzugeben sind.

Ende 2012 stellte sich bei einem Arbeitstreffen mit Vertretern des Justizministeriums NRW heraus, dass die Umsetzung der geänderten Vor-

schrift mit einem weiteren Problem verbunden war: In den Fällen, in denen die Felder Geburtsdatum oder Geburtsort keine Angaben enthielten, war vorgesehen, die Leerfelder wie Treffer zu behandeln. In solchen Fällen sollten demnach Trefferlisten angezeigt werden, ohne zu wissen, auf wie viele Personen sich die Datensätze bezogen. Auch hier ist es mir gelungen, eine Änderung herbeizuführen. Die mangelnde Eingabe von Geburtsdaten beim Anlegen eines Datensatzes soll nicht zur Verletzung des Datenschutzes Dritter führen. Nach dem Wortlaut der Regelung soll nur dann ein Ergebnis angezeigt werden, wenn die Anfrage sich auf die gesuchte Person konkretisiert hat.

➡ Durch engagiertes und hartnäckiges Eintreten für den Datenschutz, aber ganz entscheidend durch das konstruktive Zusammenwirken mit den Datenschutzbeauftragten des Bundes und der Länder, konnten einige überschießende Grundrechtseingriffe bei der Errichtung des bundesweiten Schuldnerportals im Internet verhindert werden. Hierbei war auch die Zusammenarbeit mit dem Justizministerium NRW von Vorteil.

13 Zensus 2011

Nach umfangreichen Vorbereitungen wurde im Jahr 2011 mit der Durchführung eines registergestützten Zensus begonnen. Die aus Registern gewonnenen Daten wurden durch Stichprobenbefragungen ergänzt. Die Gesetzgebungsverfahren auf Bundes- und Landesebene habe ich intensiv begleitet. Während der Umsetzung habe ich kommunale Erhebungsstellen überprüft.

Nach Beginn des registergestützten Zensus wurden Stichprobenerhebungen (Haushaltsstichproben) durchgeführt. In diesem Erhebungsstadium habe ich bei verschiedenen Kreisen und einer kreisfreien Stadt vor Ort schwerpunktmäßig geprüft, ob die Anforderungen des Zensusgesetzes 2011 an die räumliche, organisatorische sowie personelle Trennung der Erhebungsstellen von anderen Verwaltungsstellen eingehalten worden sind. Diese in dem Ausführungsgesetz zum Zensusgesetz (ZensG 2011 AG NRW) konkretisierten Maßnahmen stellen die Abschottung der Erhebungsstellen von anderen Verwaltungsstellen sicher und gewährleisten so die statistische Geheimhaltung, ein Grundprinzip der amtlichen Statistik (siehe Bericht 2011 unter 10.).

Die Arbeit der Erhebungsstellen war jeweils durch eine interne Dienstanweisung geregelt.

Diese Stellen waren in den Kommunen räumlich getrennt von den übrigen Verwaltungsstellen untergebracht und verfügten über keine direkte Verbindung zu anderen Verwaltungsbereichen. Die Räumlichkeiten waren in der Weise abgetrennt, dass entweder der jeweilige Bereich oder die einzelnen Zimmer ohne Zugangsberechtigung nicht betreten werden konnten. Ein in einem Fall auch von außerhalb der Zensusstelle erreichbarer ungesicherter Zugang ist umgehend geschlossen worden. Gemäß § 7 Abs. 2 Satz 4 ZensG 2011 AG NRW waren in allen Erhebungsstellen separate Räume als Auskunftsbereiche reserviert.

Vor den Erhebungsstellen, für die jeweils eine eigene Postanschrift eingerichtet wurde, waren separate Briefkästen angebracht. Durch die Adressierung von Rückumschlägen für Individualbefragungen und durch die Angabe der Adresse der Erhebungsstellen auf ihren Schreiben wurde sichergestellt, dass diesen Stellen gemäß § 8 Abs. 1 ZensG 2011 AG NRW alle erkennbar für sie bestimmten Eingänge unverzüg-

lich und ungeöffnet zugeleitet wurden. Mit der Reinigung der Räume der Erhebungsstellen waren private Firmen beauftragt, die die Räume nur in Anwesenheit mindestens einer oder eines Beschäftigten der Erhebungsstelle betreten konnten.

Neben der räumlichen Unterbringung der Erhebungsstellen wurde besonderes Augenmerk auf ihre personelle Trennung von der übrigen Verwaltung gelegt. Nach § 7 Abs. 5 Satz 2 ZensG 2011 AG NRW durften die in den Erhebungsstellen beschäftigten Personen während ihrer Tätigkeit dort nicht mit anderen Aufgaben des Verwaltungsvollzugs betraut werden. In einer Kommune war problematisch, weil der Leiter der örtlichen Erhebungsstelle gleichzeitig mit einer Funktion im Leitungsbereich der Verwaltung betraut war. In einer anderen Erhebungsstelle wurde ein Mitarbeiter noch kurze Zeit zugleich in einem anderen Verwaltungsbereich eingesetzt. Die Kommunen sind meiner Empfehlung gefolgt und haben die erforderlichen personellen Maßnahmen zur Abschottung ergriffen.

Die Beschäftigten der Erhebungsstellen wurden vor Beginn ihrer Tätigkeit über die Beachtung der gesetzlichen Gebote und Verbote zur Sicherung des Datenschutzes belehrt und schriftlich zur Wahrung des Statistikgeheimnisses verpflichtet.

Bei der Verarbeitung von Einzelangaben in den den örtlichen Erhebungsstellen zur Verfügung gestellten Datenverarbeitungsanlagen waren die Abschottung der Statistikdaten gegenüber anderen Verwaltungsdaten und ihre Zweckbindung (§ 7 Abs. 3 ZensG 2011 AG NRW) jeweils durch die technische Trennung der in der Erhebungsstelle eingesetzten Computer von dem allgemeinen Verwaltungsnetz der Kommune gewährleistet.

Die elektronische Erfassung der Daten aus dem Fragebogen und deren Weiterleitung an den Landesbetrieb IT.NRW ließen keine Probleme erkennen.

Die ehrenamtlichen Erhebungsbeauftragten wurden in Schulungen auf der Grundlage des vom Landesbetrieb IT.NRW zur Verfügung gestellten Materials unterrichtet. Bei den Planungen zum Einsatz der Erhebungsbeauftragten wurde beachtet, diese gemäß den Vorgaben von IT.NRW nicht in ihrer eigenen Wohnstraße oder in einer der angrenzenden Straßen einzusetzen. Zudem wurde darauf geachtet, dass der ihnen zugeteilte Bereich möglichst außerhalb ihres Wohnbereichs lag.

In Einzelfällen wurden Straßen getauscht, um einen ausreichenden Abstand zwischen den Wohnungen von Erhebungsbeauftragten und ihren Erhebungsbezirken zu gewährleisten. In den sensiblen Sonderbereichen gemäß § 2 Abs. 5 Satz 2 ZensG 2011 (wie etwa Behindertenwohnheimen, Flüchtlingsunterkünften oder Justizvollzugsanstalten) und teilweise auch in den allgemeinen Sonderbereichen gemäß § 2 Abs. 5 Satz 1 ZensG 2011 (wie etwa Studentenwohnheimen oder Krankenpflegeschülerheimen) wurden die Erhebungen durch Mitarbeiterinnen und Mitarbeiter der jeweiligen Erhebungsstelle durchgeführt.

Die Erhebungsbeauftragten wurden in ihrer Einweisung darüber belehrt, die ausgefüllten Fragebogen sofort wegzuschließen, so dass Dritte keinen Zugang zu diesen erhalten konnten. Sie wurden angehalten, diese Unterlagen nicht erst nach Abschluss der gesamten Erhebungen in ihrem Bezirk der Erhebungsstelle auszuhändigen, sondern einzelne Fragebogenpakete in kurzen Intervallen abzugeben. Es konnte festgestellt werden, dass die örtlichen Erhebungsstellen die erforderlichen Schritte unternommen haben.

➡ Die Kontrollbesuche bei den Erhebungsstellen ergaben, dass der Zensus 2011 im Wesentlichen ohne Probleme durchgeführt wurde und lediglich vereinzelt Verbesserungsbedarf festzustellen war.

14 Technik

Verwendung von IPv6-Adressen: Aber bitte datenschutzgerecht!

Um die Kommunikation zwischen zwei Rechnern im Internet zu ermöglichen, werden sogenannte IP-Adressen benötigt. Diese sind vergleichbar mit den Rufnummern von Telefonanschlüssen. Jedem Telefonanschluss wird eine Nummer zugeordnet, unter der er über das Telefonnetz erreichbar ist. Ähnlich verhält es sich bei Rechnern, die über das Internet miteinander verbunden werden. Die IP-Adresse ist die "Rufnummer" eines Rechners im Internet. Auch diese "Rufnummer" ist ein personenbezogenes Datum und sagt viel über Nutzerinnen und Nutzer aus. Der Umgang mit diesem Datum muss datenschutzgerecht sein.

Grundsätzlich werden zwei Arten der Adressierung von Rechnern im Internet unterschieden. Eine Möglichkeit besteht in der festen Zuordnung einer IP-Adresse zu einem Rechner. Er ist somit immer unter derselben Rufnummer erreichbar. Die andere Möglichkeit besteht in der Vergabe von dynamischen IP-Adressen. Hierunter ist die zeitlich befristete Zuordnung einer IP-Adresse zu dem Rechner, beispielsweise für die Dauer einer einzelnen Sitzung im Internet, zu verstehen. Wenn die Verbindung zum Internet beendet wird, wird diese IP-Adresse wieder frei und kann einem anderen Rechner, der eine Internetverbindung aufbauen möchte, zugeordnet werden. Bei der dynamischen Vergabe von IP-Adressen wird somit ein und derselbe Rechner - je Sitzung im Internet - mit einer anderen IP-Adresse ausgestattet. Die dynamische Art der Vergabe von IP-Adressen ist die datenschutzfreundlichere Variante, da bei der Zuordnung fester IP-Adressen die Personenbeziehbarkeit deutlich vereinfacht wird.

Anfang Juni 2012 gab es den "World IPv6 Launch Day". Mit diesem medienwirksamen Ereignis wurde der offizielle Startschuss zur Einführung des neuen Internet-Protokolls Version 6 mit einem nahezu unbegrenzten Vorrat an IPv6-Adressen gegeben. Die unter IPv4 verfügbaren IP-Adressen reichen nicht mehr aus, um den zukünftigen Bedarf zu decken. Damit besteht nunmehr die Möglichkeit, allen Rechnern eine feste IP-Adresse zuzuordnen. Gleichzeitig erhöhen sich die datenschutzrechtlichen Anforderungen.

Mit IPv6 ist zu erwarten, dass eine Vielzahl von elektronischen Geräten des Alltags ebenfalls einen Netzwerkanschluss erhalten wird. Da mit IPv6 ein sehr großer Vorrat an IP-Adressen verfügbar ist, besteht die Möglichkeit, jedem Gerät auch eine individuelle IP-Adresse zu geben. Dem "Internet der Dinge" wird hierdurch eine neue Dimension eröffnet.

Damit wird ein enormer Gestaltungsspielraum zur Erstellung von persönlichen Profilen in ganz unterschiedlichen Bereichen des alltäglichen Lebens eröffnet. Hierzu zählen nicht nur die bereits bekannten Bewegungsprofile, die beim Surfen im Internet entstehen. Es können beispielsweise auch Verbrauchsprofile beim Einsatz von Messgeräten im Zusammenspiel mit intelligenten Versorgungsnetzen für Elektrizität und Gas erstellt werden, soweit diese Geräte mit dem Internet verbunden sind. Aber auch das vernetzte Fernsehgerät oder andere dann internetfähige elektronische Geräte im Haushalt können einen wichtigen Beitrag zur ganzheitlichen Profilbildung von Personen leisten. Auf diese Art und Weise kann der "gläserne Mensch" wahr werden. Den Möglichkeiten sind hier kaum Grenzen gesetzt.

Das bedeutet nicht, dass die alte IPv4-Welt komplett außer Betrieb gesetzt worden ist. Vielmehr ist ein sukzessives Umstellen über einen längeren Zeitraum zu erwarten. Während dieses Zeitraums wird es einen Mischbetrieb von IPv4 und IPv6 geben.

Um einem datenschutzgerechten Einsatz von IPv6 den Weg zu bereiten, haben die Datenschutzbeauftragten des Bundes und der Länder Hinweise in Form einer Orientierungshilfe gegeben.

Die Orientierungshilfe "Datenschutz bei IPv6 - Hinweise für Hersteller und Provider im Privatkundengeschäft" findet sich auf meiner Website (abrufbar unter www.ldi.nrw.de) und kann von dort kostenlos heruntergeladen werden.

➡ Auch bei IPv6 ist auf eine datenschutzgerechte Einführung und Anwendung zu achten. Dabei gilt es, die Chancen zu nutzen und die Risiken zu minimieren. Ein Unterschreiten der bisher erreichten Standards zur Gewährleistung eines angemessenen Datenschutzniveaus im Internet ist nicht hinnehmbar. Die Orientierungshilfe lege ich meiner Kontrollpraxis zugrunde.

15 Informationsfreiheit

15.1 Die Zukunft wird transparent! – Open Data im Zeitalter der Informationsfreiheit

Im elften Jahr nach Inkrafttreten des Informationsfreiheitsgesetzes (IFG NRW) rückt zunehmend das Thema Open Data ins Zentrum der öffentlichen Diskussion. Das ist richtig und wichtig, denn die Teilhabe an den Informationen der Verwaltungen ist für den demokratischen Meinungs- und Willensbildungsprozess wie auch für die Kontrolle staatlichen Handelns unerlässlich.

Befürchtungen vor Inkrafttreten des IFG NRW, Anträge der Bürgerinnen und Bürger auf Zugang zu den vorhandenen Informationen würden die Behörden lähmen oder den Stillstand der Verwaltung zur Folge haben, haben sich nicht bestätigt. Heute wissen wir, dass sich das IFG NRW in seiner derzeitigen Fassung bewährt hat.

Nunmehr müssen Forderungen nach "mehr Transparenz" aufgegriffen und das IFG NRW im Bereich Open Data weiterentwickelt werden. Gemeint ist mit "Open Data" – vereinfacht ausgedrückt – die von einem Antrag einzelner Personen unabhängige Bereitstellung und Veröffentlichung von Informationen und Daten der Verwaltung durch die öffentlichen Stellen selbst.

Eine Vielzahl von Daten darf bereits heute veröffentlicht werden, ohne dass hierzu eine Gesetzesänderung erforderlich wäre. Beispielsweise tangiert die Veröffentlichung von Angaben, die sich nicht auf einzelne Personen beziehen lassen, die Belange des Datenschutzes nicht. Werden auch sonstige Rechte (z.B. Urheberrechte) und Pflichten (z.B. besondere Geheimhaltungspflichten) nicht berührt, bestehen gegen die Veröffentlichung der Daten keine Bedenken. Wer sich die modernen und oftmals aufwändig gestalteten Homepages öffentlicher Stellen anschaut, wird hier bereits durchweg eine Fülle von Informationen finden, die die Verwaltungen von sich aus, also "freiwillig", veröffentlicht haben. Dies ist ein guter Anfang, der allein jedoch nicht ausreicht.

Nach den Erfahrungen in der Praxis sollte nunmehr ein weiter gefasster, proaktiver, verpflichtender Ansatz gewählt werden. Die Entschei-

dung über die Bekanntgabe von Informationen sollte nicht mehr der Disposition der öffentlichen Stelle überlassen bleiben. Vielmehr bedarf es einer gesetzgeberischen Entscheidung, die ein Höchstmaß an Offenlegung nicht nur erlaubt, sondern auch vorschreibt.

Die Weiterentwicklung des IFG NRW im Bereich Open Data ist also zum einen notwendig, um die Veröffentlichung bestimmter Verwaltungsdatenbestände unabhängig vom Behördenwillen festzuschreiben. Zum anderen ist sie erforderlich, soweit durch die Veröffentlichung von Daten in besonders geschützte Belange eingegriffen wird und dies nur auf der Grundlage eines Gesetzes zulässig ist.

Für einen ersten Schritt in Richtung eines Transparenzgesetzes bieten sich beispielsweise Festlegungen in folgenden Bereichen an:

- Veröffentlichung von Verträgen, die öffentliche Stellen mit privaten Unternehmen oder Personen geschlossen und bei denen es nicht selten entweder um die Verwendung öffentliche Gelder in erheblicher Höhe oder die Erfüllung öffentlicher Aufgaben mit Hilfe Dritter geht (siehe auch Bericht 2011 unter 16.1),
- Veröffentlichung von Gutachten und Forschungsergebnissen, die von öffentlichen Stellen in Auftrag gegeben und mit öffentlichen Geldern finanziert worden sind,
- Veröffentlichung von internen Handlungsempfehlungen, Richtlinien, Geschäftsanweisungen usw.

Ausnahmen von dieser Verpflichtung sollten sich auf das unbedingt notwendige Mindestmaß beschränken. Abgerundet würde die Einführung derartiger Veröffentlichungspflichten, wenn im IFG NRW zugleich ein subjektiver einklagbarer Anspruch der Bürgerinnen und Bürger auf Veröffentlichung mitverankert würde.

Im Übrigen ist der bewährte, auf Antrag der oder des Einzelnen zu gewährende Zugang zu bestimmten individuell benannten Informationen, der bislang das IFG NRW maßgeblich prägt, neben einem gesetzlichen "Standardkatalog" mit zu veröffentlichenden Informationen auch in Zukunft unerlässlich.

Wenn es gelingen würde, eine Verwaltungsebenen übergreifende Internetplattform aufzubauen, über die die Informationen der verschie-

denen Stellen vereinfacht aufgefunden und abgerufen werden können, wäre dies ein weiterer bedeutsamer Schritt in Richtung Transparenz. In diesem Zusammenhang ist allerdings mit Nachdruck dazu zu raten, eine solche Plattform ausschließlich in eigener, öffentlicher Regie zu errichten. Die Ausgestaltung eines solchen Systems in öffentlicher Regie kann sich schon von der technischen Konstruktion bis hin zu den Voreinstellungen auf die Funktionen beschränken, die für die Bereitstellung der Informationen für die Bürgerinnen und Bürger von Bedeutung sind (privacy by design und privacy by default). Die datenschutzrechtliche Verantwortung bleibt bei den betreibenden öffentlichen Stellen. In einem solchen System sind beispielsweise auch die Richtigkeit und Aktualität mitzuteilender Daten eher zu gewährleisten.

Insgesamt könnten von NRW als bevölkerungsreichstem Bundesland in Sachen "Transparenz der Verwaltung" wichtige Impulse über die Landesgrenzen hinaus ausgehen.

➡ Die mit der Landtagsinitiative "Open Government Strategie für Nordrhein-Westfalen vorantreiben" eingeleitete Diskussion zu mehr Transparenz öffentlichen Handelns kann ich aus Sicht der Informationsfreiheit nur begrüßen. Das IFG NRW sollte im Sinne von Open Data zügig weiterentwickelt werden.

15.2 Kein Grund zur Geheimhaltung des Kaufpreises von Müllsäcken

Ein Antragsteller beanspruchte bei einer Stadt die Auskunft, welchen Kaufpreis die erworbenen 6,6 Millionen gelben Säcke hatten – allerdings vergeblich: Die Stadt lehnte die Auskunftserteilung trotz Beanstandung mit Hinweis auf zu schützende Betriebs- und Geschäftsgeheimnisse ab.

Die Stadt berief sich zunächst nur darauf, dass der Kaufpreis ein Betriebs- und Geschäftsgeheimnis darstelle, bei dessen Offenbarung ein wirtschaftlicher Schaden entstünde; begründet wurde diese Behauptung nicht. Auf Nachfrage teilte die Stadt mit, dass durch die Mitteilung des Kaufpreises die Preiskalkulation des Vertragspartners öffentlich würde. Da bekannt sei, wie viele Säcke erworben worden seien, könne bei Kenntnis des Kaufpreises auch der Stückpreis eines Sacks

errechnet werden. Dies stelle jedoch einen Eingriff in die zu schützende Preiskalkulation des Vertragspartners dar, dem im Übrigen auch Vertraulichkeit zugesichert worden sei (siehe hierzu auch unter 15.4).

Ich habe darauf hingewiesen, dass die Kenntnis des Einzelpreises keinen Einblick in die Preiskalkulation gewähre. Ein solcher läge nur dann vor, wenn zu ersehen wäre, aus welchen Preiskomponenten – Materialkosten, Verarbeitungskosten, Personalkosten etc. – sich der Einzelpreis zusammensetze. Dies sei aber allein durch die Mitteilung des Kaufpreises nicht der Fall.

Trotz entsprechender Empfehlung, Beanstandung und Unterrichtung der Aufsichtsbehörde verweigert die Stadt bis heute die Mitteilung des Kaufpreises.

➡ Die inhaltlichen Gründe für die Informationsverweigerung sind nicht tragfähig. Vermutlich führt auch in diesem Fall die vertragliche Vertraulichkeitszusage zum fortgesetzten Verstoß gegen das Informationsfreiheitsgesetz Nordrhein-Westfalen.

15.3 Offenlegung von Verbandsempfehlungen zur Höhe von Vorstandsgehältern

Ein Sparkassenverband verweigerte einem Antragsteller die Einsicht in allgemeine Rahmenregelungen zur Höhe von Vorstandsgehältern. Begründet wurde dies mit dem Schutz der Persönlichkeitsrechte der Vorstandsmitglieder.

Der Antragsteller beantragte bei einem Sparkassenverband Akteneinsicht in die Empfehlungen des Verbandes zur Höhe der Gehälter kommunaler Sparkassenvorstände. Der Verband lehnte diesen Antrag ab und argumentierte, die Umsetzung der Empfehlungen erfolge einzelfallbezogen zwischen der Sparkasse und dem Vorstandsmitglied. Der Inhalt dieser Verträge unterfalle der Amtsverschwiegenheit. Dies gelte auch für die den Anstellungsverträgen zugrunde liegenden Empfehlungen der Sparkassenverbände.

Auf meinen Hinweis, dass im Rahmen des Informationsfreiheitsgesetzes Nordrhein-Westfalen (IFG NRW) die Pflicht zur Amtsverschwiegenheit entfalle und sich Verweigerungsgründe nur aus dem IFG NRW

selbst ergeben könnten, trug der Sparkassenverband ergänzend vor: Bei den Empfehlungen handele es sich zwar noch nicht um den "endverhandelten Vertrag", jedoch werde hierdurch der strukturelle Rahmen der individuellen Vorstandsverträge vorgegeben. Dieser unterfalle daher – ebenso wie der endverhandelte Vertrag – dem Schutz personenbezogener Daten gemäß § 9 Abs. 1 IFG NRW. Der Verband legte die Empfehlungen zur Prüfung vor. Daraus ergab sich, dass durch eine Offenlegung keine personenbezogenen Daten offenbart würden.

Durch eine Regelung im Sparkassengesetz Nordrhein-Westfalen (SpkG NRW) wird zudem festgelegt, dass die Gemeinden oder Gemeindeverbände als Träger der Sparkassen darauf hinwirken, dass die für die Tätigkeit im Geschäftsjahr gewährten Bezüge jedes einzelnen Mitglieds des Vorstands, des Verwaltungsrates und ähnlicher Gremien unter Namensnennung im Anhang zum Jahresabschluss gesondert veröffentlicht werden. Zwar ist die begehrte Berechnungsgrundlage für die Bezüge nicht nach der angesprochenen Regelung des SpkG NRW zu veröffentlichen, jedoch handelt es sich bei den Berechnungsfaktoren für die veröffentlichten und damit allgemein bekannten einzelnen Komponenten nicht um personenbezogene Daten. Der Informationszugang durfte daher nicht aufgrund der Regelung des § 9 Abs. 1 IFG NRW verweigert werden.

Da der Sparkassenverband weiterhin die Offenlegung der Gehälterempfehlungen verweigerte, wurde dieser Verstoß gegen das IFG NRW beanstandet.

➡ Trotz Beanstandung und Unterrichtung der Aufsichtsbehörde wurden die Verbandsempfehlungen nicht offengelegt. Es bleibt abzuwarten, ob zumindest das diesbezüglich eingeleitete Klageverfahren dem Antragsteller zu seinem Recht verhelfen wird.

15.4 Verträge sind trotz Vertraulichkeitszusagen in der Regel offenzulegen

Oft berufen sich öffentliche Stellen auf vertragliche Vertraulichkeitsvereinbarungen oder auf Betriebs- und Geschäftsgeheimnisse des Vertragspartners.

So wollte beispielsweise ein Bürger einer großen Kommune wissen, welches Honorar eine Beratungsfirma für die Begutachtung der Rechtmäßigkeit einer geplanten Gaspreiserhöhung erhalten habe. Erst nach jahrelangem Zögern wurde diese Information offengelegt. Dasselbe gilt für die Frage, zu welchem Preis eine Beratungsfirma ein Gutachten zu einer Großveranstaltung für eine Kommune erstellt habe. Auch diese Information wurde verweigert – und ist letztlich doch noch "durchgesickert".

Auch nach elf Jahren Informationsfreiheit herrscht in einigen öffentlichen Stellen die Auffassung vor, durch vertragliche Vertraulichkeitsvereinbarungen könnten Verträge vor den Augen der Öffentlichkeit verborgen werden. Dies ist jedoch nicht der Fall, da gesetzliche Offenlegungspflichten nicht durch privatrechtliche Vereinbarungen unterlaufen werden können. Es wäre vielmehr geboten, potentielle Vertragspartnerinnen und -partner bereits bei Vertragsschluss darüber aufzuklären, dass Verträge grundsätzlich öffentlich zugänglich sind. Nur soweit in den Verträgen tatsächlich Betriebs- und Geschäftsgeheimnisse oder personenbezogene Daten enthalten sind, müssten die betreffenden Regelungen geschwärzt werden. Nicht nur in Nordrhein-Westfalen stellt die beschriebene Verfahrensweise der öffentlichen Stellen ein Problem dar. Aus diesem Grund hatte die Konferenz der Informationsfreiheitsbeauftragten im Dezember 2010 die Entschließung "Verträge zwischen Staat und Unternehmen offen legen!" (Abdruck im Anhang) gefasst.

➡ Auch nach elf Jahren Informationsfreiheit hat sich die Erkenntnis, dass Verträge grundsätzlich offenzulegen sind, bei vielen öffentlichen Stellen noch nicht durchgesetzt. Es wäre daher wünschenswert, eine ausdrückliche Regelung in das IFG NRW aufzunehmen.

15.5 WDR muss Auskunft zu allen nicht journalistischen Themen erteilen

Der WDR vertritt seit Jahren die Auffassung, dem Anwendungsbereich des Informationsfreiheitsgesetzes Nordrhein-Westfalen (IFG NRW) nur im Rahmen seiner hoheitlichen Tätigkeit zu unterfallen. Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen (OVG NRW) hat nun klargestellt,

dass eine Auskunftspflicht zu allen Informationen besteht, die nicht journalistischer Natur sind.

Ein Journalist beantragte bereits im Jahr 2007 unter Berufung auf das IFG NRW beim WDR Auskünfte über Aufträge, die an private Unternehmen vergeben wurden. Der WDR lehnte dies mit dem Hinweis ab, der Rundfunksender unterfalle dem Anwendungsbereich des IFG NRW nur im Rahmen seiner hoheitlichen Tätigkeit, also dem Rundfunkgebühreneinzug und der Vergabe von Sendezeiten an Dritte. Alle anderen Bereiche seien durch die grundgesetzlich geschützte Rundfunk- und Pressefreiheit vor interessierten Blicken geschützt. Meine Behörde hat demgegenüber stets die Auffassung vertreten, die Auskunftspflicht des WDR bestehe für alle Tätigkeiten, die nicht dem geschützten journalistisch-redaktionellen Kernbereich zuzuordnen seien (siehe Bericht 2009 unter 17.3). Der Landesgesetzgeber hat inzwischen mit § 55a WDR-Gesetz eine Regelung getroffen, welche die Anwendbarkeit des IFG NRW auf den WDR festschreibt, es sei denn, dass journalistisch-redaktionelle Informationen betroffen sind.

Das OVG NRW hat nun entschieden, dass der WDR die beantragten Informationen erteilen muss. Alle Informationen, die in keinem inhaltlichen Zusammenhang mit der Programmgestaltung stünden, müssten offengelegt werden. Der WDR habe nun in jedem Einzelfall zu prüfen, welche Informationen dies seien. Dabei müsse er nachvollziehbar darlegen, warum eine Information wegen eines Rückschlusses auf ein Redaktionsgeheimnis einmal nicht erteilt werden könne.

Die beantragten Informationen hat der Antragsteller indes noch immer nicht erhalten: Der WDR hat gegen die Entscheidung des OVG NRW Nichtzulassungsbeschwerde beim Bundesverwaltungsgericht eingelegt.

➡ Die weitere Entwicklung werde ich mit Interesse verfolgen.

15.6 "Prozess der Willensbildung" eng auszulegen

Öffentliche Stellen stützen sich häufig, wenn sie ein Informationsbegehren ablehnen wollen, auf § 7 Abs. 2 Buchstabe a) Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW), der den behördlichen Willensbildungsprozess schützt.

Ein Antrag soll danach abgelehnt werden, wenn sich der Inhalt der Information auf den Prozess der Willensbildung von und zwischen öffentlichen Stellen bezieht. Wohl kein anderer Verweigerungsgrund des IFG NRW wird in so zahlreichen Facetten fehlgedeutet wie dieser.

Zweck dieser Bestimmung ist es, die nach außen vertretene Entscheidung einer Behörde nicht dadurch angreifbar zu machen, dass interne Meinungsverschiedenheiten oder unterschiedliche Auffassungen zwischen mehreren beteiligten Stellen veröffentlicht werden. Das Prinzip der Einheit der Verwaltung soll dazu führen, dass staatliche Maßnahmen nicht als Entscheidung einer bestimmten Person oder einer Organisationseinheit, sondern als solche des Verwaltungsträgers wahrgenommen werden. Der benannte Verweigerungsgrund kommt daher nur dann zum Zuge, wenn sich aus den begehrten Unterlagen ergibt, dass ein streitiger Willensbildungsprozess in der Behörde oder zwischen Behörden stattgefunden hat. Informationen über Willensbildungsprozesse, bei denen keine streitigen Meinungen zum Ausdruck kommen, können nicht unter Berufung auf diesen Verweigerungsgrund abgelehnt werden.

Diese Auffassung hat das Oberverwaltungsgericht für das Land Nordrhein-Westfalen in einem Beschluss vom 28. Juli 2011 – 13a F 3/11 – bestätigt.

➡ Der Verweigerungsgrund des Willensbildungsprozesses hat nur einen engen Anwendungsbereich. Es bleibt zu hoffen, dass sich diese Erkenntnis nach dem Beschluss des OVG NRW weiter durchsetzt.

15.7 Finanzverwaltung - weiter Probleme mit der Informationsfreiheit?

Weder die "absichtsvolle Nichtregelung" eines Akteneinsichtsrechts in der Abgabenordnung (AO) noch das in § 30 AO geregelte Steuergeheimnis kommen als Begründung dafür in Betracht, das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) im Bereich der Finanzverwaltung nicht anzuwenden.

Die AO enthält selbst nach 30 Jahren des Rechts auf informationelle Selbstbestimmung keinen geregelten Anspruch auf Akteneinsicht in die

eigene Steuerakte. Die Rechtsprechung des Bundesfinanzhofs hat insoweit zur Rechtsfortbildung beigetragen, dass zumindest bei laufenden Steuerverfahren die Gewährung von Einsicht in die eigene Akte die einzig ermessensfehlerfreie Entscheidung darstellt.

Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen (OVG NRW) hatte folgenden Fall zu entscheiden:

Ein Insolvenzverwalter beantragte unter Berufung auf das IFG NRW bei einem Finanzamt die Übersendung von Speicherkontenauszügen einer Insolvenzschuldnerin. Die Finanzverwaltung lehnte dies mit dem Hinweis ab, die "absichtsvolle Nichtregelung" eines Akteneinsichtsrechts in der AO bringe den gesetzgeberischen Willen zum Ausdruck, gerade kein Einsichtsrecht einräumen zu wollen. Darüber hinaus stehe die Regelung des § 30 AO – das Steuergeheimnis – einem Informationszugang entgegen.

Das OVG NRW entschied dagegen, dass die "Nichtregelung" schon deshalb keine verdrängende Rechtsvorschrift darstellen könne, weil sie allein das Verhältnis zwischen den Steuerpflichtigen und der Finanzverwaltung betreffe. Da der Insolvenzverwalter demgegenüber Dritter sei, daher nicht derselbe Sachverhalt geregelt und nicht der gleiche Personenkreis wie durch das IFG NRW begünstigt werde, könne die "Nichtregelung" keine das IFG NRW verdrängende Rechtsvorschrift darstellen. Die Regelungen des IFG NRW fänden daher – wie in den anderen Verfahrensgesetzen auch – neben der AO Anwendung. Auch das Steuergeheimnis stehe der Anwendung des IFG NRW nicht entgegen. Die Vorschrift regele nur, welche Daten dem Steuergeheimnis unterliegen und unter welchen Voraussetzungen diese offenbart, verwertet oder abgerufen werden dürften. Über einen Anspruch der Steuerpflichtigen oder von Dritten gegenüber einer Finanzbehörde auf Auskunft sage die Vorschrift hingegen nichts aus. § 30 AO schließe daher nicht die Anwendbarkeit des IFG NRW aus, sondern müsse auf der Ebene der Verweigerungsgründe – unter dem Aspekt des Schutzes personenbezogener Daten – geprüft werden.

➡ Es bleibt zu hoffen, dass die Rechtsprechung des OVG NRW dem Bundesgesetzgeber den Rücken stärkt, bei der Novellierung der Abgabenordnung keine Bereichsausnahme für die Finanzverwaltung einzuführen.

15.8 Kommune kommt ihrer Pflicht zur Auskunft nicht nach

Eine Stadt verweigert meiner Behörde – trotz Beanstandung – beharrlich die Auskunft.

Ein Antragsteller begehrte von einer Stadt verschiedene Auskünfte zu einem neuen Baugebiet. Als sein Antrag abgelehnt wurde, wandte er sich mit der Bitte um Unterstützung an meine Behörde. Ein Auskunftsersuchen meiner Behörde wurde von der Stadt zunächst zurückgestellt. Trotz wiederholter Erinnerungen ging keine Stellungnahme ein. Telefonisch wurde zwar mehrfach eine baldige Antwort angekündigt, jedoch geschah nichts. Die Stadt wurde dabei stets daran erinnert, dass eine gesetzliche Pflicht bestehe, mir Auskunft zu erteilen. Nachdem weiterhin keine Antwort einging, musste die Nichterteilung der Auskunft und damit der Verstoß gegen das Informationsfreiheitsgesetz Nordrhein-Westfalen beanstandet werden.

➡ Es besteht eine gesetzliche Verpflichtung, mir Auskunft zu erteilen. Die jeweiligen Aufsichtsbehörden sollten deshalb auskunftsverweigernde Stellen anweisen, mir die erbetenen Auskünfte zu erteilen.

Anhang

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

81. Konferenz vom 16./17. März 2011

◆ **Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens - dringender Handlungsbedarf auf nationaler und europäischer Ebene**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass - wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[1] - EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems

[1]*Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.*

◆ Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z.B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit - auch für die Strafverfolgungsbehörden - zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

◆ Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die "Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. DieWartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alleWartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a)

nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)

- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden

◆ Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

◆ Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare

gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90 / DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis

  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z.B. im Internet) und bei Dritten zu unterrichten.

- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei insbesondere verdeckte Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien z.B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte

verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere
  - zu verbieten, die z.B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.
  - für Bereiche zu untersagen, die nicht nur "überwiegend", sondern auch der privaten Nutzung dienen.
- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.
- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen
  - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,
  - zur privaten Nutzung von Telekommunikationsdiensten,
  - zum Thema Whistleblowing,
  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs

82. Konferenz vom 28./29. September 2011

◆ Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro

verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 02. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

◆ Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen

können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

◆ Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den "Gefällt-mir"-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten

Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

◆ Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IPAdresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offen stehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.

- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.

- Hard- und Softwarehersteller sollten die "Privacy Extensions" unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.

- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.

- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.

- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.

Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte "Internet-Telefonbuch" whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien

gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

◆ Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe (1) der Arbeitskreise "Technik" und "Medien" zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

---

(1) http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

◆ Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,

2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,

3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,

4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und

5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

◆ Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z.B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 "Übermittlung von Flugpassagierdaten an die US-Behörden"; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 "Kein Ausverkauf von europäischen Finanzdaten an die USA!").

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 "Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich") zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

83. Konferenz vom 21./22. März 2012

◆ Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum - nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik - insbesondere der Videoüberwachung und dem Instrument der Mustererkennung - menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf "potentielle Gefährder" frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt "INDECT" (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit

der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

◆ Ein hohes Datenschutzniveau für ganz Europa

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,
- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und

- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

◆ Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweis-mittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

84. Konferenz vom 07./08. November 2012

◆ Einführung von IPv6 - Hinweise für Provider im Privatkundengeschäft und Hersteller

Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.

- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.

- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.

- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.

- Interface Identifier und Präfix sollten synchron gewechselt werden.

- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.

- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.

- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher

vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe "Datenschutz bei IPv6 - Hinweise für Hersteller und Provider im Privatkundengeschäft" präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

◆ Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten.

Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

◆ Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich "überzogene" Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

◆ Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der **Datenschutz-Grundverordnung** an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

  Jede Verarbeitung scheinbar "belangloser" Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich "belanglose" Daten von einer Regelung auszunehmen.

  Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.

- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.

- Mit Blick auf die Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

Entschließungen zwischen den Konferenzen:

◆ 22. August 2012 - Melderecht datenschutzkonform gestalten

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.
- Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

- Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.
- Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.
- Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.
- Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.
- Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.
- Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür - wie auch bei der Hotelmeldepflicht - außer Verhältnis zum Nutzen.

◆ 27. Juni 2012 - Orientierungshilfe zum datenschutzgerechten Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d.h. Anwendungsfälle, für die einzelnen

Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.

- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.

- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.

- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.

- Die Daten sollen an möglichst wenige Stellen übermittelt werden.

- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.

- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.

- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.

- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.

- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten

erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

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

Beschluss vom 26./27. November 2009

◆ 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 IPAdressen (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.

Beschluss vom 08. April 2011

◆ Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen **für Internet-Geodatendienste wie Google Street View zu verzichten.**

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotential für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.

- Eigentümer und Bewohner 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.

Beschlüsse vom 4./5. Mai 2011

◆ Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die "Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtunng muss ausgeschlossen sein.
3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)

- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht

- sowie die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

◆ Datenschutzkonforme Gestaltung und Nutzung von Krankenhaus-informationssystemen

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 Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der

Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

◆ Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik "persönliche" Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme ("Apps"), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein "Spion in der Hosentasche".

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

- **Transparenz bezüglich der Preisgabe personenbezogener Daten:**

  In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

- **Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:**

  Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z.B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

- **Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:**

  Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

- **Anonyme und pseudonyme Nutzungsmöglichkeiten:**

  Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer

Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff "Privacy by Design" fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design v. 29.10.2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport).

Beschlüsse vom 22./23. November 2011

◆ Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines "zugelassenen Wirtschaftsbeteiligten" (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen

von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt. Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.
- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.
- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

◆ Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das "auf der ganzen Linie" anonym oder mindestens

pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z.B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener "White Cards" erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. "Micropayment") zu erhalten (vgl. Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: "Anonymes elektronisches Bezahlen muss möglich bleiben!").

◆ Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben. Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,
- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe (http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf) der Arbeitskreise "Technik" und "Medien" zu entnehmen, die der Düsseldorfer Kreis zustimmend zur Kenntnis genommen hat.

Beschluss vom 08. Dezember 2011

◆ Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

- Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.

- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.

- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten - soweit keine Einwilligung vorliegt - ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und –nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.

- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.

- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

Beschluss vom 17. Januar 2012

◆ Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY[1] daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z.B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (*Krankenversicherung*)[2] benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5] Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY *[Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird]* selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht7

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

- Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[8] erhebt und für diese Zwecke verwendet.

  Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren[9] vor Antragstellung an die Versicherung XY übermittelt werden.

  Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

  Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.[10]

Möglichkeit II:

- Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

  - in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige

  - oder die erforderlichen Unterlagen selbst beibringe.

  Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[11] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY

konkrete Anhaltspunkte[12] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[13]

Möglichkeit I:

- Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

Möglichkeit II:

- Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.[14]

3.1 Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.[15]

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XYGruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter (*Internetadresse*) eingesehen oder bei (*Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse*) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt. Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.[25] Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet. Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet[26].

> Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.[28] Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die

Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden. Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren

Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

_____	_____
Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
_____	_____
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres)
_____	_____
Ort, Datum	*Unterschrift des gesetzlichen Vertreters*

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel – BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten

Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren. Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z.B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

> Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.

---

[1] Hier und im Folgenden kann anstelle von "die Versicherung XY" der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa "wir, die Versicherung XY") jeweils "wir" eingefügt werden.

[2] Hier kann die konkrete Sparte genannt werden.

[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite

der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

4 Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

5 Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG.

6 Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

7 Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

8 Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

9 Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

10 Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i.V.m. Abs. 4 VVG.

11 Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

12 Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

13 Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld

entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z.B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

14 Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

15 Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

16 Der Satzteil "für sich und" ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.

17 Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

18 In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

19 Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung,

Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

[20] Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z.B. Krankentransporte.

[21] Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

[22] Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

[23] "und sonstige Stellen" – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

[24] Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.

[25] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.

[26] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.

[27] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht. Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

[28] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.

[29] Durch die Formulierung "an den jeweiligen Betreiber" sowie die Aufnahme von "derzeit" im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.

[30] Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt. Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.

[31] Es zählt das Datum der Unterschrift im Antrag.

[32] Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/ Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

Beschluss vom 18./19. September 2012

◆ Near Field Communikation (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Entschließung vom 13. Dezember 2010

◆ Verträge zwischen Staat und Unternehmen offen legen!

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.

Entschließungen vom 23. Mai 2011

◆ Geplantes europäisches Nanoproduktregister – Transparenz für Bürgerinnen und Bürger!

Neue Technologien rufen bei Bürgerinnen und Bürgern nicht nur positive Reaktionen hervor, sondern stoßen häufig auf Skepsis oder lösen Ängste aus.

Grund hierfür ist nicht selten eine unzureichende Informationslage bis hin zur Zurückhaltung von Informationen für Verbraucherinnen und Verbraucher. Wer das Potential neuer Technologien ausschöpfen möchte, muss mit offenen Karten spielen. Das bedeutet, dass nicht nur Vorteile, sondern auch Risiken offen gelegt werden müssen, um einen demokratischen Diskurs und jedem Menschen eine informierte Willensbildung zu ermöglichen.

Ein aktuelles Beispiel ist der Einsatz von Nanotechnologie: Dabei geht es um künstlich hergestellte winzige Partikel (Nanomaterial), die heute schon in Baustoffen, Textilien sowie Kosmetika und zukünftig immer mehr in verbrauchernahen Produkten wie etwa Lebensmitteln eingesetzt werden. Nanotechnologie soll Produkte z.B. robuster machen. In einem Bericht aus dem Jahre 2009 (nano.DE-Report 2009) geht das Bundesministerium für Wissenschaft und Forschung davon aus, dass nanotechnologisches Know-how in den Bereichen Gesundheit, Informations- und Kommunikations- sowie Energie- und Umwelttechnik immensen Einfluss auf die Wertschöpfung nehmen wird. Ein Weltmarktvolumen von 15 % der globalen Güterproduktion wird prophezeit.

Wenigen ist dies bekannt, denn es besteht derzeit keine Pflicht, Produkte, die Nanomaterial enthalten, zu kennzeichnen. Erst 2013 wird eine solche Pflicht für Kosmetika bestehen. Für Lebensmittel wird die Kennzeichnungspflicht noch diskutiert. Zugleich – stellt die Nano-Kommission der Bundesregierung in ihrem Aktionsplan Nanotechnologie 2015 fest – fehlen vielfach grundlegende Kenntnisse über die Risiken bei der Exposition mit Nanomaterialien.

Die Informationsfreiheitsbeauftragten in Deutschland fordern die Bundesregierung auf, sich bei den Diskussionen und Verhandlungen auf europäischer Ebene dafür einzusetzen, dass Bürgerinnen und Bürgern ein direkter Zugang zu Informationen über Nanotechnologie in Produkten ermöglicht wird. Deshalb ist es notwendig, dass auch Bürgerinnen und Bürger Zugang insbesondere zu dem auf europäischer Ebene diskutierten Nanoproduktregister erhalten. Beim Einsatz neuer Technologien muss verstärkt auf Aufklärung, Transparenz und Einbindung der Menschen gesetzt werden.

◆ Informationsfreiheit – Lücken schließen!

Der Gedanke der Transparenz staatlichen Handelns ist beim Bund und den meisten Ländern seit einigen Jahren angekommen, wie die Informationsfreiheitsgesetze von Brandenburg (1998), der meisten anderen Länder und auch das Informationsfreiheitsgesetz des Bundes (2005) zeigen.

Vor diesem Hintergrund begrüßt die Konferenz der Informationsfreiheitsbeauftragten die Absicht der neuen Landesregierung von Baden-Württemberg, auch dort ein Informationsfreiheitsgesetz auf den Weg zu bringen. Dabei sollte allerdings, wie in Rheinland-Pfalz vorgesehen, dem Landesbeauftragten für den Datenschutz die Aufgabe der oder des Beauftragten für die Informationsfreiheit übertragen werden. Diese unabhängige Funktion eines oder einer Informationsfreiheitsbeauftragten fehlt gegenwärtig auch noch in Thüringen. Bayern, Hessen, Niedersachsen und Sachsen lehnen dagegen beharrlich jede gesetzliche Regelung für einen Anspruch der Bürgerinnen und Bürger auf Zugang zu behördlichen Informationen ab.

Dies führt zu absurden Ergebnissen: So haben die Bürgerinnen und Bürger gegenüber den Jobcentern mit gemeinsamer Trägerschaft durch Bundesagentur für Arbeit und Kommune auch in den vier Ländern ohne Informationsfreiheitsgesetze einen Anspruch auf der Grundlage des Bundesgesetzes. Dagegen besteht gegenüber den Jobcentern der Optionskommunen in ausschließlich kommunaler Trägerschaft in diesen Ländern kein Anspruch auf Informationszugang.

Unbefriedigend ist auch, dass die Bürgerinnen und Bürger bei Ersuchen auf Zugang zu Verbraucher- und Umweltinformationen nicht durchgängig die gesetzlich garantierte Möglichkeit haben, sich an die Informationsfreiheitsbeauftragten zu wenden. Eine Ombudsfunktion ist zwar in den meisten Informationsfreiheitsgesetzen vorgesehen, fehlt aber für Umwelt- und Verbraucherinformationen auf Bundesebene und in vielen Ländern.

Deshalb appelliert die Konferenz an die Gesetzgeber in Bund und Ländern, diese Regelungsdefizite zu beseitigen und "flächendeckend" allgemeine Regelungen für den Informationszugang zu schaffen und die Ombudsfunktionen der Informationsfreiheitsbeauftragten für Verbraucher-, Umwelt- und sonstige Informationen in Bund und Ländern gesetzlich zu regeln.

Entschließung vom 28. November 2011

◆ Informationsfreiheit ins Grundgesetz und in die Landesverfassungen

Demokratie und Rechtsstaat können sich nur dort wirklich entfalten, wo auch die Entscheidungsgrundlagen staatlichen Handelns offen gelegt werden. Bund und Länder müssen ihre Bemühungen weiter verstärken, für mehr Transparenz staatlichen Handelns zu sorgen. Eine verfassungsrechtliche Verankerung der Informationsfreiheit ist geboten.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland tritt dafür ein, den Anspruch auf freien Zugang zu amtlichen Informationen in das Grundgesetz und in die Landesverfassungen – sofern noch nicht geschehen – aufzunehmen. Staatliche Stellen müssen die ihnen vorliegenden Informationen grundsätzlich öffentlich zugänglich machen.

Entschließungen vom 12. Juni 2012

◆ Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!

Mit Besorgnis nehmen die Informationsfreiheitsbeauftragten in Deutschland zur Kenntnis, dass der freie Zugang zu Dokumenten der Europäischen Union gemäß Verordnung 1049/2001 erneut in Frage gestellt wird. Bereits im Jahre 2008 hatte die Europäische Kommission mannigfaltige Vorschläge zu einer drastischen Einschränkung des Zugangs zu europäischen Dokumenten vorgelegt, deren Folge eine massive Reduzierung der gebotenen Transparenz

des Handelns europäischer Institutionen gewesen wäre (vgl. Entschließung der Informationsfreiheitsbeauftragten in Deutschland vom 30. Juni 2008). Das Europäische Parlament forderte daraufhin zwar eine Stärkung der Informationsfreiheit, doch arbeiten die Mitgliedstaaten derzeit daran, genau das zu verhindern. Ein "Kompromisspapier" der dänischen Ratspräsidentschaft sah zuletzt vor, das Zugangsrecht zu Akten der Institutionen der Europäischen Union deutlich einzuschränken.

Während bislang alle Arten von Inhalten der Informationsfreiheit unterfallen, sollen zukünftig nur "formell übermittelte" Dossiers öffentlich einzusehen sein. Damit würden der Öffentlichkeit sämtliche Entwürfe oder Diskussionspapiere des Rats, der Kommission und des Parlaments vorenthalten. Dies würde auch Vertragsverletzungsverfahren, Wettbewerbs- und Kartellverfahren betreffen, die von hohem öffentlichem Interesse sind.

Die Konferenz lehnt die Ausnahme einzelner europäischer Institutionen von der Transparenzpflicht ab. Sie tritt dafür ein, dass insbesondere die Europäische Zentralbank und die Europäische Investitionsbank nicht nur hinsichtlich ihrer Verwaltungstätigkeiten auf mehr Transparenz verpflichtet werden.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an die Bundesregierung, sich im Europäischen Rat für mehr Transparenz einzusetzen. Verwaltung und Politik auf der Ebene der Europäischen Union dürfen nicht in bürokratische Geheimniskrämerei zurückzufallen. Die Forderungen des Europäischen Parlaments müssen endlich erfüllt werden. Gerade angesichts der zunehmenden Verantwortung, die den europäischen Institutionen von der gemeinsamen Außenpolitik bis zur Bewältigung der Finanzkrise zukommt, gilt es, alle Institutionen der Europäischen Union noch weiter zu öffnen. Denn: Vertrauen basiert auf Transparenz!

◆ Mehr Transparenz bei der Wissenschaft – Offenlegung von Kooperationsverträgen –

Die Kooperation zwischen Wissenschaft und Wirtschaft hat eine lange Tradition. Dies gilt für gemeinsame Institute ebenso wie für Stiftungsprofessuren und sonstige Formen der Zusammenarbeit.

Unternehmensfinanzierte Forschung nimmt einen immer größeren Anteil an der Wissenschaft ein. Deutschlandweit sollen inzwischen 660 Lehrstühle direkt oder indirekt von Unternehmen finanziert sein. Oft sind Motivation und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Beurteilung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch Voraussetzung. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; Geheimhaltung engt diese Freiheiten ein.

Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann nur durch eine konsequente Politik der Offenheit begegnet werden. Kooperationsverträge zwischen Wissenschaft und Unternehmen sind grundsätzlich offen zu legen. Eine solche Veröffentlichungspflicht sollte mindestens die Identität der Drittmittelgeber, die Laufzeit der Projekte, den Förderumfang und die Einflussmöglichkeiten der Drittmittelgeber auf Forschungsziele und -ergebnisse

umfassen. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe gesetzlich geschützte Interessen beeinträchtigt.

Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden wird. Eine reine Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Es bedarf vielmehr konsequenter Regelungen in den Informationsfreiheitsgesetzen des Bundes und der Länder.

Entschließungen vom 27. November 2012

◆ Mehr Transparenz bei Krankenhaushygienedaten

Das Vertrauen der Bevölkerung in das deutsche Gesundheitssystem, insbesondere in unsere Krankenhäuser, hat im Laufe der letzten Jahre abgenommen. Dies ist auch auf eine verbreitete Intransparenz zurückzuführen.

Zwar wurden in einem von einer Tageszeitung herausgegebenen Klinikführer Berlin- Brandenburg erstmals auch Hygienedaten veröffentlicht, jedoch nahmen nicht alle Krankenhäuser an der dieser Publikation zugrunde liegenden freiwilligen Datenerhebung teil. Das wurde unter anderem damit begründet, dass die nur zu internen Zwecken erhobenen Daten falsch interpretiert werden könnten und dass Patientinnen und Patienten möglicherweise andere Krankenhäuser wählen würden, wenn sie über entsprechende Vergleichsdaten verfügten.

Die Entscheidung für oder gegen ein bestimmtes Krankenhaus können die Patientinnen und Patienten aber nur dann verantwortlich treffen, wenn ihnen alle relevanten Parameter zur Verfügung stehen; dazu gehören auch die jeweiligen Hygienedaten und ihre Umsetzung in den einzelnen Kliniken. Nur eine standardisierte Melde- und Veröffentlichungspflicht für alle Hygienedaten ermöglicht es jedem Patienten und jeder Patientin, die jeweiligen Hygienestandards der Krankenhäuser zu bewerten und zu vergleichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher alle Verantwortlichen, insbesondere den Bundes- und die Landesgesetzgeber auf, für Transparenz bei Krankenhaushygienedaten zu sorgen. Dazu gehören auch standardisierte und weit reichende Melde- und Veröffentlichungspflichten und die Erweiterung der Qualitätsberichte der Krankenhäuser. Dies wäre ein wichtiger Schritt, um durch mehr Transparenz das Vertrauen der Bevölkerung in die Gesundheitsversorgung durch Krankenhäuser zu fördern.

◆ Parlamente sollen in eigener Sache für mehr Transparenz sorgen!

Die Informationsfreiheitsgesetze von Bund und Ländern nehmen die Parlamente von den für sonstige öffentliche Stellen bestehenden Transparenzpflichten aus. Die Konferenz der Informationsfreiheitsbeauftragten

in Deutschland sieht, dass der Kernbereich der Abgeordnetentätigkeit in der unabhängigen Wahrnehmung ihres Mandats nicht dem umfassenden Zugangsanspruch der Öffentlichkeit unterliegen kann. Defizite bei der Transparenz führen aber zu einem Verlust an öffentlicher Glaubwürdigkeit. Die Parlamente von Bund und Ländern sollten deshalb Vorreiter in Sachen Transparenz werden und Ausnahmen vom Informationszugang soweit wie möglich zurücknehmen.

In welchem Umfange Transparenz herzustellen ist, ist eine Frage des verfassungsrechtlich gebundenen, gesetzgeberischen Ermessens. Dieses verpflichtet die Parlamente dazu, die bereits vorhandenen Transparenzregelungen regelmäßig daraufhin zu überprüfen, ob sie sich bewährt haben oder ggf. zu konkretisieren und zu ergänzen sind.

Dabei sollten – soweit noch nicht geschehen – folgende Punkte berücksichtigt werden:

a. ein möglichst hohes Maß an Transparenz bei den weiteren Tätigkeiten und Einkünften von Abgeordneten unter Berücksichtigung von Berufsgeheimnissen. Den möglichen Besonderheiten des Mandats, insbesondere bei "Teilzeit"-Parlamenten, sollte Rechnung getragen werden,

b. Veröffentlichung von Tagesordnungen von Plena und Ausschüssen, ebenso Stellungnahmen, Protokolle und weitere Unterlagen, die Gegenstand der Beratungen sind,

c. Öffentlichkeit von Sitzungen der Fachausschüsse,

d. grundsätzliche Veröffentlichung von wissenschaftlichen Ausarbeitungen der Parlamentsdienste und sonstiger Gutachten,

e. Zugang zu Informationen über Beschaffungen, Reisen, Sachausgaben und sonstige kostenträchtige Vorhaben der Parlamente und ihrer Ausschüsse.

Hinweise auf Informationsmaterial

Neben dem aktuellen Datenschutz- und Informationsfreiheitsbericht können Sie bei uns weiteres Infomaterial kostenlos anfordern. 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: 0211/ 38424-0