LDI NRW

Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Datenschutz und Informationsfreiheit

Bericht 2015

Zweiundzwanzigster Datenschutz- und Informationsfreiheitsbericht

des

Landesbeauftragten für Datenschutz

und Informationsfreiheit

Nordrhein-Westfalen

Ulrich Lepper

für die Zeit vom 1. Januar 2013

bis zum 31. Dezember 2014

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: 22. DIB LDI NRW
ISSN: 0179–2431
Düsseldorf 2015

Gedruckt auf chlorfreiem Recyclingpapier

1 Überblick

Die **Snowden-Enthüllungen** zeigen, wie staatliche Vorsorge zur allumfassenden Überwachung verkommen kann. Die Folgen für die Privatheit sind verheerend. Was muss der Staat tun, was können Bürgerinnen und Bürger unternehmen? Nicht Resignieren, sondern Reagieren ist gefragt! (Siehe hierzu unter 2.)

"Sicher ist sicher" darf nicht das allein entscheidende Motto sein. Auch die Freiheitsrechte müssen geschützt werden.

Schon der hierzulande immer wieder erhobene Ruf nach Ausweitung der **Videoüberwachung** folgt dem Grundmuster, vorsorglich erst einmal alles zu erfassen, was theoretisch auch nur annäherungsweise zur Vermeidung von Gefahren oder zur Aufklärung von Straftaten nützlich sein könnte. Dieses Muster findet sich sowohl im privaten als auch öffentlich-rechtlichen Bereich. (Siehe hierzu unter 6 und 9.1.)

Obwohl der Europäische Gerichtshof die Gefahren für eine freie Gesellschaft in eindrucksvoller Weise beschrieben hat, die mit einer anlasslosen flächendeckenden Verarbeitung von Daten aller Bürgerinnen und Bürger verbunden sind, hält der Ruf nach **Vorratsdatenspeicherung** von Telekommunikationsverbindungsdaten unverändert an. Eine freie Gesellschaft wird sich immer differenziert der Frage stellen müssen, wo die Grenzen zwischen der unerlässlich gebotenen Sicherheitsvorsorge des Staates einerseits und der Freiheit der einzelnen Grundrechtsträgerinnen und -träger andererseits zu ziehen sind. Eine Einzelfallanalyse, die sich auf belegbare Verdachtsmomente stützt und die einen eingrenzbaren Personenkreis betrifft, ist hierbei unerlässlich. (Siehe hierzu unter 3.3.)

Auch andere Maßnahmen der Sicherheitsbehörden, zum Beispiel **Funkzellenabfragen**, betreffen eine Vielzahl von einzelnen Bürgerinnen und Bürgern, die zwar nicht das Ziel behördlichen Handelns sind, aber angesichts der Streubreite dieser Maßnahmen zufällig erfasst werden. Wie sollen eine wirksame Kontrolle und ein gesellschaftlicher Diskurs möglich sein, wenn Feststellungen zum Ausmaß und zur Reichweite solcher Maßnahmen im Land nicht getroffen werden? (Siehe hierzu unter 9.2.)

Das novellierte **Verfassungsschutzgesetz NRW** untersagt zwar ausdrücklich eine "Online-Durchsuchung". Das Gesetz erlaubt dem

Verfassungsschutz aber den Zugriff auf zugangsgesicherte Telekommunikationsinhalte im Internet, ohne dass Bürgerinnen und Bürger noch in der Lage wären, den komplizierten Gesetzestext zu durchdringen und das Ausmaß ihrer Betroffenheit zu überblicken. Außerdem kann der Verfassungsschutz Daten zur Sicherung des Zugangs zu Informationen im Internet (PIN/PUK), anders als im Bund, ohne vorherige Kontrolle durch ein unabhängiges Gremium erheben. (Siehe hierzu unter 9.3.)

Wie ist es angesichts der Angriffsszenarien, die längst nicht mehr nur abstrakt sind, überhaupt um die **Datensicherheit in der öffentlichen Verwaltung** bestellt, der die Daten der Bürgerinnen und Bürger anvertraut sind, wenn knapp ein Drittel der Kommunen in NRW für den eigenen Verantwortungsbereich noch nicht einmal ein Sicherheitskonzept erstellt hat? (Siehe hierzu unter 11.)

Bei aller Empörung über den Umgang fremder Staaten mit dem Datenschutz sollten wir nicht aus den Augen verlieren, dass gigantische Datenmengen weltweit von Anbietern privater Dienste verarbeitet werden – zumal sich einige Anbieter an die Anforderungen des deutschen Datenschutzes offenbar nicht gebunden fühlen. Umso unverständlicher ist es, dass die Ressorts der Landesregierung nicht oder nur zögerlich meine Anregungen aufgreifen, wenn es darum geht, Daten der Bürgerinnen und Bürger, die sich online an Stellen des Landes wenden, bei der Nutzung von **sozialen Netzwerken** vor ungeklärten Zugriffen privater Anbieter zu schützen. (Siehe hierzu unter 4.2.)

- Neue Entwicklungen

Die Dynamik des Marktes bringt stets neue Fragestellungen hervor, die mit weiteren Herausforderungen für das Recht auf informationelle Selbstbestimmung verbunden sind:

So bieten vereinzelt deutsche Kfz-Versicherungsunternehmen Rabatte an, wenn Kundinnen und Kunden ihr Fahrverhalten analysieren lassen. Vergleichbare Überlegungen mit Daten zu Fitness, Ernährung und Lebensstil stellt nunmehr auch schon ein Krankenversicherungsunternehmen an. **Verhaltensbezogene Versicherungstarife** dieser Art erzeugen finanziellen Druck, Unternehmen tiefen Einblick in Lebensgewohnheiten und Gesundheit zu ermöglichen. Diese Entwicklung verfolge ich mit Sorge. Nicht nur Fragen des Datenschutzes sind

berührt – wir brauchen eine gesellschaftliche Debatte darüber, wo Grenzen für solche Geschäftsmodelle zu ziehen sind. (Siehe hierzu unter 5.1 und 5.2.)

Vielfältige neue **automatische Funktionen in modernen Kraftfahrzeugen** erzeugen oft ohne Wissen der Fahrerinnen und Fahrer immer mehr Daten, die miteinander verknüpft werden können und personenbezogene Aussagen über das Fahrverhalten ermöglichen. Wichtig ist zu wissen, welche Daten zu welchen Zwecken von wem wo verarbeitet werden. Welche datenschutzrechtliche Verantwortung tragen unter anderem Automobilhersteller, Händler und Werkstätten? Können Fahrerinnen und Fahrer überhaupt noch selbst über ihre Daten verfügen? Werden sie von elektronischen Zusatzdiensten entmündigt? (Siehe hierzu unter 7.1.)

Neue Fernsehgeräte (**Smart-TV**) können sowohl herkömmliche Fernsehsignale als auch Mediendienste anzeigen. Die Technik ermöglicht, die Nutzung auch des herkömmlichen Fernsehens zu analysieren. Dem Düsseldorfer Kreis, der Arbeitsgemeinschaft der Aufsichtsbehörden des Bundes und der Länder unter dem Vorsitz von NRW, ist es gelungen, in einer gemeinsamen Erklärung mit den Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten in Deutschland eine Position zur Freiheit der Mediennutzung zu bestimmen, der sich die Landesanstalten für Medien angeschlossen haben. Danach gilt es insbesondere, auch für das Fernsehen mit Smart-TV-Geräten Anonymität zu gewährleisten. (Siehe hierzu unter 4.1.)

- Datenschutz auf Ebene der EU

Maßstäbe für einen Datenschutz auf hohem Niveau hat auf europäischer Ebene in jüngster Zeit der Europäische Gerichtshof gesetzt, wie schon die Entscheidung zur Vorratsdatenspeicherung gezeigt hat. Mit seiner bemerkenswerten Entscheidung zu **Internet-Suchmaschinen** stärkt der Gerichtshof das Recht der Bürgerinnen und Bürger, nicht mit Hilfe von Suchmaschinen aufgefunden zu werden. (Siehe hierzu unter 3.4.)

Ob bei der **EU-Datenschutzreform** Rat, Parlament und Kommission die Chance ergreifen, das Recht auf informationelle Selbstbestimmung substanziell weiterzuentwickeln, werden die Beratungen in Brüssel noch zeigen müssen. Möglicherweise führen Kompromisse zu einem Datenschutzniveau, das nicht eindeutig bestimmbar und im

Ergebnis eher niedriger ist als das der bisherigen Regelungen. Wesentliche Wertungen darf der Gesetzgeber nicht dem Verwaltungsvollzug überlassen. Kritisch sehe ich auch die Tendenz, wesentliche Elemente der (Eigen-)Verantwortung von Unternehmen und Behörden auf die Datenschutzaufsicht zu verlagern, indem etwa die in Deutschland bewährte betriebliche oder behördliche Selbstkontrolle in Frage gestellt wird. Ich begrüße aber die in sämtlichen Entwürfen vorgesehene Stärkung der Kontrolle durch die unabhängigen Datenschutzbehörden. (Siehe hierzu unter 3.5.)

- Irrweg in Deutschland

Vor dem Hintergrund der europarechtlichen Entwicklungen kann ich mich über die Pläne der Bundesregierung zur Änderung des Unterlassungsklagegesetzes nur wundern. Danach sollen nun auch **Verbraucherschutzverbände** und andere Institutionen in großem Umfang gegen Datenschutzverstöße vorgehen. Ohne Anlass erteilt die Bundesregierung dem herkömmlichen System der Datenschutzkontrolle damit eine Abfuhr. Statt die öffentlich-rechtliche Datenschutzaufsicht, die rechtsstaatlichen Anforderungen unterliegt, in ihrer unabhängigen grundrechtswahrenden Funktion zu stärken, sollen privatrechtliche Parallelstrukturen errichtet werden. Nicht nur als Steuerzahlerinnen und Steuerzahler müssen Bürgerinnen und Bürger kritische Fragen stellen. (Siehe hierzu unter 3.6.)

- Datenschutz in der Fläche

Ohne Eigenverantwortung der datenverarbeitenden Stellen – seien es Unternehmen oder Behörden – lässt sich in der Fläche Datenschutz kaum verwirklichen. Weder eine Datenschutzbehörde noch andere öffentliche Institutionen können die Verantwortung vor Ort ersetzen und sollten dies auch nicht tun. Bei mehr als 700.000 Unternehmen und einer Vielzahl öffentlicher Stellen in NRW muss ich wegen der begrenzten Ressourcen meiner Behörde neue Instrumente einsetzen, um auch in der Fläche dem Datenschutz Geltung zu verschaffen. Dazu gehört, **Zertifizierungen** auf freiwilliger Grundlage zu fördern. Solche Maßnahmen, die von Unternehmen aus eigenem Antrieb veranlasst werden, bieten eine Chance, zu mehr eigenverantwortetem Datenschutz zu gelangen. NRW ist es gelungen, bundesweit Anstöße hierzu zu geben und sich im Kreis der Aufsichtsbehörden von Bund und Ländern auf konkrete Anforderungen an solche Verfahren zu

verständigen, die schon jetzt eingesetzt werden können. (Siehe hierzu unter 3.1.)

Auch die **Landesdatenschutzkonferenz**, zu der ich auf Wunsch des Landtags Vertreterinnen und Vertreter von Kommunen, Wirtschaft, Verbraucherschutz, Gewerkschaften, Kammern und Landesbehörden eingeladen habe, unterstützt meine Initiative zu einer Stärkung des Datenschutzes durch freiwillige Zertifizierungen. (Siehe hierzu unter 3.2.)

Als weiteres Instrument setze ich verstärkt auf **Aufklärung durch Informationen**, um Bürgerinnen und Bürger soweit wie möglich in die Lage zu versetzen, ihre Rechte bereits selbst wahrnehmen zu können**.** Erkenntnisse aus der täglichen Aufsichtspraxis werden so aufbereitet, dass Bürgerinnen und Bürger zunächst selbst ihre Datenschutzrechte einschätzen und auf dieser Grundlage weitere Schritte ergreifen können. Ebenso habe ich gemeinsam mit anderen Datenschutzbehörden Orientierungshilfen für Unternehmen und Behörden entwickelt, die über die für sie geltenden datenschutzrechtlichen Anforderungen informieren. Als Beispiele seien genannt:

- Orientierungshilfe zur Videoüberwachung "Sehen und gesehen werden" (siehe hierzu unter 6.1)
- Tipps zum Selbstdatenschutz im Internet, auch besonders für Jugendliche (siehe hierzu unter 2)
- Orientierungshilfe "Soziale Netzwerke" (siehe hierzu unter 4.2)
- Orientierungshilfe "Datenschutzanforderungen an App-Entwickler und App-Anbieter" (siehe hierzu unter 4.3)
- Orientierungshilfe "Cloud Computing" (siehe hierzu unter 2)
- Hinweise "Personalausweis und Datenschutz" (siehe hierzu unter 5.7)
- Orientierungshilfe "Einholung von Selbstauskünften bei Mietinteressenten" (siehe hierzu unter 5.5)
- Anwendungshinweise zu Daten für Werbezwecke (siehe hierzu unter 5.8).

Ein anderes Instrument, um Datenschutz trotz begrenzter Ressourcen auch in der Fläche zu kontrollieren, sind **Querschnittsuntersuchungen**. Sie geben Aufschluss, in welchen Bereichen weitere Kontrollen angezeigt sind. Die Erfahrungen mit der Querschnittsuntersuchung zur Datensicherheit im Bereich der Kommunen bestärken mich darin, das Instrument auch in anderen Bereichen einzusetzen. (Siehe hierzu unter 11.)

- Informationsfreiheit

Mit der Informationsfreiheit geht es auf Gesetzgebungsebene nicht weiter. Die Landesregierung hat zwar eine "Open.NRW-Strategie" veröffentlicht. Es ist aber nicht ersichtlich, dass das Informationsfreiheitsgesetz NRW im Sinne einer weitergehenden Transparenz fortentwickelt wird und insbesondere Pflichten der Behörden zur Veröffentlichung von Informationen festgeschrieben werden sollen. Nach den Erfahrungen in der Aufsichtspraxis halte ich eine Fortentwicklung des Transparenzgedankens für dringend geboten. (Siehe hierzu unter 12.1.)

- Ausblick

Die Herausforderungen an die Kontrolle des Datenschutzes und der Informationsfreiheit nehmen ständig zu. Insbesondere mit Blick auf die bevorstehende EU-Datenschutzreform ist – unabhängig von vorgesehenen neuen Aufgaben – abzusehen, dass meine Behörde allein im Bereich Koordination und Zusammenarbeit mit anderen Behörden auf nationaler und auf EU-Ebene weitere Anforderungen erfüllen muss. Dies wird mit dem bisherigen Personalbestand auch dann nicht zu bewältigen sein, wenn – wie geschildert – verschiedene Instrumente in meiner Behörde eingesetzt werden, um mit begrenzten Ressourcen optimale Ergebnisse erzielen zu können. Ich bin gewiss, dass der Landtag die Bedeutung des Datenschutzes und der Informationsfreiheit im Blick behält und eine angemessene Ausstattung der Behörde auch in Zukunft ermöglichen wird.

Ulrich Lepper Düsseldorf, im Frühjahr 2015

2 Snowdens Enthüllungen: Reagieren statt Resignieren

Wegen der Enthüllungen Edward Snowdens seit Juni 2013 ist das gesamte Thema Datenschutz unter neuen Voraussetzungen zu diskutieren. Die Datensicherheit ist danach anscheinend in vielen Bereichen nicht mehr gewährleistet.

Die veröffentlichten Dokumente weisen auf umfangreiche Überwachungsaktivitäten durch den US-Geheimdienst National Security Agency (NSA) und weitere westliche Dienste hin. Besonders in den Bereichen der Telekommunikation und internetbasierter Dienste werden demnach massenhaft personenbezogene Daten unzähliger Menschen aus aller Welt gesammelt und gespeichert. Dazu sollen Datenleitungen angezapft, Programme gehackt und Verschlüsselungen gebrochen werden. In den USA ansässige Unternehmen werden zur Herausgabe ihrer Datenbestände an Sicherheitsbehörden veranlasst. Daneben wird auch gezielte Spionage erwähnt, zum Beispiel das Abhören der Telefone von Regierungsmitgliedern, einschließlich des Telefons der Bundeskanzlerin.

Internet und elektronische Kommunikation sind für das private und berufliche Leben vieler Menschen in unserem Land unverzichtbar. Ein Gefühl ständiger Überwachung oder zumindest die Befürchtung, jederzeit zum Gegenstand der Ausforschung werden zu können, tragen zur Verunsicherung bei.

Diese Situation stellt Politik, Gesellschaft, Wirtschaft und Behörden vor neue Herausforderungen. Unabhängig davon können alle, die privat telefonieren, im Internet surfen, mailen, chatten usw., selbst etwas für die Sicherheit ihrer eigenen Daten tun.

- Forderungen an die Politik

Es ist Aufgabe der Politik, die rechtlichen und technischen Rahmenbedingungen für besseren Datenschutz in der Praxis zu schaffen.

Der internationale Datenverkehr zwischen verantwortlichen Stellen im Europäischen Wirtschaftsraum und Empfängern in den USA oder anderen Drittländern, bei denen ein angemessenes Datenschutzniveau nicht gewährleistet ist, beruht zum Großteil auf Abkommen und Vertragswerken, die jeweils als Garantie zum Schutz der Persönlichkeitsrechte dienen sollen. Beispiele dafür sind das Safe-Harbor-

Abkommen mit den USA oder die Standardvertragsklauseln. Diese und andere Garantien haben unverhältnismäßige Zugriffe durch Geheimdienste offenbar nicht verhindert.

Deshalb müssen die bisher geltenden Entscheidungen der EU bezüglich des internationalen Datenverkehrs mit Drittstaaten ausgesetzt oder zumindest zügig überarbeitet werden. Eine bereits eingeleitete Überprüfung der Safe-Harbor-Entscheidung durch die EU-Kommission weist in die richtige Richtung.

In diesem Zusammenhang sollten die aktuellen Verhandlungen zum Freihandelsabkommen TTIP genutzt werden, um das Thema Datenschutz zwischen der EU und den USA voranzubringen.

Ohnehin sind für den weltweiten Datenverkehr internationale Standards von großer Bedeutung. EU und Bundesregierung sind hier gefragt.

Außerdem empfehle ich, Zusammenarbeit und Kontrolle der Geheimdienste – auch der EU-Mitgliedstaaten – auf den Prüfstand zu stellen.

Weiterhin ist eine ständige Verbesserung der technischen Infrastruktur in NRW und anderswo eine wichtige Voraussetzung, um dauerhaft die globale Interaktionsfähigkeit zu sichern. Hochwertige Verschlüsselungstechnik ist besonders zu fördern. Das entspricht auch der Pflicht des Staates, die Vertraulichkeit und Integrität informationstechnischer Systeme zu gewährleisten, die das Bundesverfassungsgericht 2008 beschrieben hat.

Die Forderung, als Reaktion auf Terroranschläge Verschlüsselungstechniken zu beschränken oder gar zu verbieten, geht in die falsche Richtung.

➧ Viele nordrhein-westfälische Unternehmen sind darauf angewiesen, im Rahmen global angelegter Geschäftsbeziehungen rechtssicher agieren zu können. Die dafür nötigen Grundlagen müssen deshalb zügig im Licht der Snowden-Enthüllungen geprüft und weiterentwickelt werden. Bei der Diskussion über die bevorstehende europäische Datenschutz-Grundverordnung muss ein hohes Datenschutzniveau Maßstab der Politik sein.

- Datensicherheit in Unternehmen und Behörden

Die Snowden-Enthüllungen müssen für Wirtschaft und öffentliche Stellen Anlass sein, die Datensicherheit ihrer IT-Systeme zu überprüfen und, wo nötig, zu verbessern. Darauf habe ich die Landesregierung und die Kommunen Mitte 2013 ausdrücklich hingewiesen. In diesem Zusammenhang ist auch meine Querschnittsprüfung der Datensicherheit bei Kommunalverwaltungen zu sehen (siehe hierzu unter 11).

➧ Private und öffentliche Stellen müssen aus den Snowden-Enthüllungen Konsequenzen ziehen und erforderliche Maßnahmen für die eigene Datensicherheit umsetzen.

- Empfehlungen zum internationalen Datenverkehr

Besonders global tätige Unternehmen haben das Vertrauen in die Datensicherheit verloren. Internationaler Datenverkehr ist nur möglich, wenn bei allen daran beteiligten Stellen ein angemessenes Datenschutzniveau garantiert ist. Datenleitungen und Server in aller Welt müssen vor Zugriffen Dritter sicher sein. Das ist im Hinblick auf Aktivitäten der NSA und anderer Geheimdienste anscheinend nicht gewährleistet.

Unternehmen, Bürgerinnen und Bürger stellen vermehrt Fragen zur Rechtmäßigkeit bestimmter Cloud-Dienste. Die angebotenen Dienste sehen vielfach vor, dass eingestellte Daten rund um den Globus verschickt und verarbeitet werden. Zu Cloud-Diensten hat die Datenschutzkonferenz eine Orientierungshilfe erarbeitet (siehe www.ldi.nrw.de).

In der Beratung weise ich auf die besonderen Risiken hin, die mit dem Transfer personenbezogener Daten in die USA oder andere Drittstaaten ohne angemessenes Datenschutzniveau verbunden sind. Nutzerinnen und Nutzer sollten in diesem Bewusstsein und erst nach sorgfältiger Abwägung entscheiden, ob solche Dienste für sie in Frage kommen oder nicht. Allgemein gebe ich den Rat, mit Daten möglichst sparsam umzugehen. Dies dürfte auch im unternehmerischen Interesse liegen, denn von Datenzugriffen können Betriebsgeheimnisse ebenso betroffen sein wie personenbezogene Daten, was auch zu einem Reputationsschaden führen kann. Wenn Datentransfers in die

USA und andere Drittstaaten dennoch erfolgen sollen, empfehle ich dringend, bei den technisch-organisatorischen Sicherungsmaßnahmen höchste Standards anzuwenden. Dazu ist insbesondere starke Verschlüsselung zu empfehlen.

➧ Soweit Datentransfers in die USA und andere Drittstaaten unerlässlich sind, sollte jedes mögliche Instrument zur Erhöhung der Datensicherheit konsequent genutzt werden.

- Möglichkeiten zum Selbstdatenschutz

Politik, Wirtschaft und Verwaltung sind gefordert – aber auch wer selbst elektronische Dienste nutzt, kann zum Schutz der eigenen Daten und der Daten anderer viel beitragen. Maßnahmen zum Selbstdatenschutz sind in der Regel leicht zu erlernen und nach derzeitigem Kenntnisstand wirksam einsetzbar.

Hinweise zum Selbstdatenschutz gebe ich auf meiner Internetseite (www.ldi.nrw.de). Interessierte können sich dort unter anderem darüber informieren,

1. wie Daten verschlüsselt werden, um sie während der Übertragung im Internet vor unbefugtem Einblick zu schützen,
2. wie mit Hilfe von Anonymisierungsdiensten digitale Spuren im Internet verwischt werden können,
3. wie man sich gegen Viren, Würmer, Trojaner oder sonstige Schadsoftware auf seinen Rechnern schützen kann,
4. wie Passwörter sicher erstellt und benutzt werden können,
5. welche Ansprüche auf Auskunft, Berichtigung und Löschung bestehen und
6. welche Einstellungen in Endgeräten wie Smartphones oder WLAN-Routern, in Anwendungen wie Betriebssystemen oder Webbrowsern oder in Diensten wie Suchmaschinen oder sozialen Netzwerken zur Sicherheit der eigenen Daten vorgenommen werden können.

Im August 2014 habe ich zusammen mit dem Chaos Computer Club Düsseldorf (CCCD) eine "Cryptoparty" veranstaltet. Eine "Cryptopar-

ty" ist ein informelles Treffen, auf dem Interessierte sich über Möglichkeiten zur Verschlüsselung informieren können und erlernen können, diese praktisch anzuwenden. Nach kurzen Einführungsvorträgen erklärten Mitglieder des CCCD, wie die Software zur Verschlüsselung von E-Mails für verschiedene Betriebssysteme zu installieren ist, und halfen bei der Umsetzung. Hierzu waren die Gäste der "Cryptoparty" eingeladen, ihre Endgeräte mitzubringen sowie die Software zu installieren und anzuwenden. Ich freue mich, dass 50 Interessierte aus verschiedensten Berufszweigen die "Cryptoparty" besucht und zu einer gelungenen Veranstaltung gemacht haben. Meine Behörde bietet an, mit ihr per verschlüsselter E-Mail zu kommunizieren. Der dazu erforderliche Schlüssel kann von meiner Homepage heruntergeladen werden (www.ldi.nrw.de)

Ich beteilige mich weiterhin an verschiedenen Initiativen des Landes NRW zur Vermittlung von Medienkompetenz. Meine Behörde nahm 2014 erneut am Tag der Medienkompetenz im Landtag NRW teil. Die Veranstaltung stand unter dem Motto "Wir sind die Daten" und war dem Thema Big Data gewidmet. Meine Behörde hat dort Tipps zur Verschlüsselung angeboten. In einer lebhaften Podiumsdiskussion habe ich einerseits auf die Gewährleistungspflichten des Staates hingewiesen und andererseits die Möglichkeiten zum Selbstdatenschutz aufgezeigt.

Gemeinsam mit dem Medienkompetenz-Netzwerk NRW beim Grimme-Institut habe ich zudem Erläuterungen zu "Datenschutz im Netz auf einen Blick" erstellt (www.ldi.nrw.de).

Meine Behörde ist schließlich eingebunden in die nationale Koordinierung der Medienkompetenzangebote der Datenschutzaufsichtsbehörden im Rahmen des Arbeitskreises Datenschutz und Bildung der Datenschutzkonferenz. Als Ergebnis der Zusammenarbeit beteilige ich mich unter anderem am Internetauftritt www.young-data.de, der als gemeinsames Informationsangebot der deutschen Datenschutzbehörden ausgestaltet wird. Die Seite richtet sich besonders an Jugendliche und gibt ihnen Hinweise zum Umgang mit den eigenen Daten im Internet.

- Ich werde auch zukünftig das Informationsangebot zum Thema Selbstdatenschutz ausbauen. Dabei werde ich besonders für die Verschlüsselung

von Kommunikation im Internet werben und Kooperationen fortsetzen.

3 Entwicklung des Datenschutzrechts

3.1 Zertifizierung: Selbstregulierung für verlässlichen Datenschutz

Viele Unternehmen und andere verantwortliche Stellen möchten ihre Datenverarbeitung im Wege einer Zertifizierung überprüfen lassen und das Ergebnis gegenüber ihren Kundinnen und Kunden mit einem Siegel dokumentieren. Eine so verstandene freiwillige Zertifizierung, die verlässlich bestehende Datenschutzanforderungen spezifiziert und als ein aus eigenem Antrieb veranlasstes Vorgehen flächendeckend zu einer Überprüfung von vor Ort ergriffenen Datenschutzmaßnahmen zu führen vermag, kann einen bedeutenden Beitrag für den Datenschutz leisten.

In meinem Bericht 2013 habe ich angesprochen, dass ein Datenschutzaudit unter bestimmten Voraussetzungen ein Fortschritt für den Datenschutz wäre. Der Landtag NRW hat diese Überlegungen begrüßt und mich gebeten zu prüfen, inwieweit ein NRW-Datenschutzsiegel einen Beitrag zur Verbesserung des Datenschutzes leisten kann (LT-Drs. 16/1469). Hierbei sind alle rechtlichen und tatsächlichen Aspekte eines solchen Verfahrens zu berücksichtigen.

Grundlage der Überlegungen ist, dass einerseits selbstkreierte Audits ohne Anbindung an die Datenschutzaufsichtsbehörde wenig Verlässlichkeit bieten. Andererseits fehlt es für eine Auditierung in der Trägerschaft des LDI NRW an einer Rechtsgrundlage sowie an der personellen Ausstattung. Daher könnte der Mittelweg einer Zertifizierung durch private Träger anhand eines Prüfstandards, an dessen Erstellung die Aufsichtsbehörde im Rahmen ihrer Beratungsfunktion mitgewirkt hat, eine Lösung bieten.

In diesem Sinn haben mir die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) und der Bundesverband der Datenschutzbeauftragten Deutschlands e. V. (BvD) gemeinsam ein Konzept für ein Datenschutzsiegel im Bereich der Auftragsdatenverarbeitung vorgelegt. Es beruht auf der Vorstellung, dass die Siegelvergabe von nicht-öffentlichen Stellen in eigener Verantwortung im Wege der

Selbstregulierung auf der Grundlage von Standards durchgeführt wird, die auch von der Aufsichtsbehörde befürwortet werden. Ein wichtiges Element ist die Veröffentlichung des Prüfstandards. Bereits als veröffentlichter Leitfaden kann er einen Beitrag für mehr Rechtssicherheit in den Unternehmen leisten. Im Rahmen meiner Beratungsaufgabe habe ich die Arbeiten zu Zertifizierungsablauf und Prüfstandard begleitet und sehe sie als geeignete Grundlage für weitere Schritte (siehe www.ldi.nrw.de).

Diese Initiative hat auch der Düsseldorfer Kreis als Zusammenschluss der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich aufgegriffen. Er unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten, und hat hierfür Strukturmerkmale festgeschrieben (siehe Beschluss "Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden" vom 25./26. Februar 2014; Abdruck im Anhang).

Die Landesdatenschutzkonferenz hat sich ebenfalls mit dem Thema beschäftigt. Ihre Entschließung mit Anforderungen an Zertifizierungen sowie Empfehlungen an Landtag und Landesregierung sehe ich als Bestätigung des eingeschlagenen Weges (siehe hierzu unter 3.2).

➧ Ich freue mich, dass es gelungen ist, mit einer Initiative aus NRW auch bundesweit Anstöße für die Weiterentwicklung von Zertifizierungen zu geben. Ich werde das Thema weiterhin begleiten.

3.2 Landesdatenschutzkonferenz

Der Landtag NRW hat mich gebeten, zu einer Landesdatenschutzkonferenz einzuladen (LT-Drs. 16/1469). Im Fokus steht die Möglichkeit der Einführung eines Datenschutzsiegels in NRW.

Dem Wunsch des Landtags bin ich gerne nachgekommen. An der Landesdatenschutzkonferenz nehmen Vertreterinnen und Vertreter von Kommunen, Wirtschaft, Verbraucherschutz, Gewerkschaften, Kammern und Behörden teil.

Der Landtag unterstützt meine Überlegungen zu prüfen, wie mit Hilfe von Datenschutzsiegeln ein Beitrag zur Verbesserung des Datenschutzes in der Fläche erreicht werden kann (siehe hierzu unter 3.1). Die Landesdatenschutzkonferenz hat Anforderungen an die Vergabe von Datenschutzsiegeln und Empfehlungen an Landtag und Landesregierung beraten und eine gemeinsame Entschließung gefasst (Abdruck im Anhang).

➧ Die Landesdatenschutzkonferenz hat in dem unmittelbaren Dialog zwischen den verschiedenen Verantwortlichen weitere Impulse für die Verbreitung von Datenschutzsiegeln gegeben. Ich bin froh, dass die Landesdatenschutzkonferenz damit meine Initiativen zu einer Stärkung des Datenschutzes durch freiwillige Zertifizierungen unterstützt.

3.3 Europäische Richtlinie zur Vorratsdatenspeicherung ist ungültig

Nachdem bereits im Jahr 2010 die deutschen Regelungen zur Vorratsdatenspeicherung vom Bundesverfassungsgericht für verfassungswidrig erklärt wurden, hat der Europäische Gerichtshof auch die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt.

In seiner Entscheidung vom 8. April 2014 aufgrund zweier Vorlageverfahren aus Irland und Österreich äußerte der Europäische Gerichtshof deutliche Kritik an der Vorratsdatenspeicherung (Rechtssachen C-293/12 und C-594/12). Die Entscheidung weist Parallelen zu der Entscheidung des Bundesverfassungsgerichtes vom 2. März 2010 auf, durch welche seinerzeit die deutschen Vorschriften zur Vorratsdatenspeicherung für verfassungswidrig erklärt wurden (siehe Bericht 2011 unter 13.1).

Der Europäische Gerichtshof betont insbesondere, dass die massenhafte und anlasslose Speicherung von Kommunikationsverkehrsdaten einen schwerwiegenden Eingriff in die Grundrechte auf den Schutz des Privatlebens und der personenbezogenen Daten darstellt. Derart

gravierende Eingriffe müssen sich auf das absolut Notwendige beschränken.

Die für ungültig erklärte Richtlinie enthalte zur Totalerfassung aller Verkehrsdaten jedoch keine hinreichenden Differenzierungen und Einschränkungen – etwa im Hinblick auf Zeit, geografische Ausdehnung und den betroffenen Personenkreis. Auch die Schwelle für Zugriffe auf Daten sei nicht hinreichend präzisiert. Ebenso bemängelt der Gerichtshof, dass eine vorherige Kontrolle der Zugriffe auf die gespeicherten Daten durch Gerichte oder unabhängige Verwaltungsstellen fehle. Zudem mangele es an konkreten und verbindlichen Vorgaben für technische und organisatorische Maßnahmen, um das notwendige Schutz- und Sicherheitsniveau zu gewährleisten. Die wirksame Kontrolle des Datenschutzes durch unabhängige Stellen setze unter anderem voraus, dass die Datenspeicherung auf dem Gebiet der Europäischen Union erfolge.

- Der Europäische Gerichtshof hat deutliche Worte gefunden und klare Grenzen für die anlasslose und umfassende Speicherung von Kommunikationsdaten aufgezeigt. Nach der Entscheidung kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtliche nicht mehr neu begründet werden. Wachsamkeit ist jedoch weiterhin geboten, da Rufe nach einer Vorratsdatenspeicherung auch nach den Entscheidungen aus Karlsruhe und Luxemburg nicht verstummen. Ich plädiere dafür, Überlegungen zum Schutz überragend wichtiger Rechtsgüter stattdessen auf geeignete Eingriffe im Sinne einer in einem rechtsstaatlichen Verfahren nachvollziehbar erstellten und autorisierten Verdachtsanalyse in Bezug auf einen bestimmbaren Kreis von Personen zu konzentrieren.

3.4 Suchmaschinen-Urteil des Europäischen Gerichtshofs

Mit Suchmaschinen lassen sich weltweit detaillierte Profile zu Personen erstellen. Das kann zu Nachteilen für die Betroffenen führen, die möglicherweise ein Leben lang mit früheren Äußerungen oder Veröffentlichungen zu ihrer Person konfron-

tiert werden. Der Europäische Gerichtshof hat nun in einem viel beachteten Urteil klargestellt, dass Suchmaschinenbetreiber – bei Suchanfragen zum Namen einer natürlichen Person – unter bestimmten Voraussetzungen ein Recht der Betroffenen auf Sperrung von Suchergebnissen umzusetzen haben (Urteil vom 13. Mai 2014 – C-131/12, "Google Spain").

Mit einer einfachen Suchanfrage anhand eines Namens können Internetnutzerinnen und -nutzer in Sekundenschnelle einen Überblick über die zu der Person im Internet verfügbaren Informationen erhalten. Diese betreffen potenziell zahlreiche Aspekte des Privatlebens, die von unterschiedlichen Stellen an verschiedenen Orten zu unterschiedlichen Zeiten ins Internet gestellt wurden. Sie wären ohne Suchmaschine nicht oder nur sehr schwer miteinander verknüpfbar. Suchmaschinen erstellen somit bei einer Suche anhand eines Namens für jede und jeden Interessierten ein mehr oder weniger detailliertes Profil der gesuchten Person.

Nach der Entscheidung des Europäischen Gerichtshofs (EuGH) haben die Suchmaschinenbetreiber eine eigene datenschutzrechtliche Verantwortung für die Datenverarbeitungsprozesse, die solche Persönlichkeitsprofile ermöglichen. Als verantwortliche Stellen müssen sie daher auch bei der Zusammenstellung der Suchergebnisse die gesetzlichen Anforderungen an die Verarbeitung personenbezogener Daten beachten.

Daraus leitet der Gerichtshof die Pflicht ab, bei einer Suchanfrage zu einer Person unter bestimmten Voraussetzungen Links zu Internetseiten von der Ergebnisliste zu entfernen. Die Pflicht kann unabhängig davon bestehen, ob die Informationen zu der Person auf den gefundenen Internetseiten rechtmäßig veröffentlicht werden oder nicht.

Die Pflicht, bei Suchanfragen anhand eines Namens unter bestimmten Voraussetzungen Fundstellen nicht anzuzeigen, begründet der Gerichtshof mit der potenziellen Schwere des Eingriffs in die Rechte der betroffenen Person. Die Wirkung des Eingriffs werde durch die besondere Bedeutung des Internets und der Suchmaschinen noch gesteigert – dadurch sei das mit der Ergebnisliste erstellte Profil überall verfügbar und allgegenwärtig.

Wegen der potenziellen Schwere kann ein solcher Eingriff nach Ansicht des EuGH nicht mit dem wirtschaftlichen Interesse des Suchma-

schinenbetreibers gerechtfertigt werden. Im Hinblick auf die berechtigten Interessen der Internetnutzerinnen und -nutzer am Zugang zu den Informationen verlangt der Gerichtshof einen angemessenen Ausgleich zwischen den Grundrechten der betroffenen Person und den Interessen der Informationssuchenden. Im Allgemeinen würden die Rechte der Betroffenen überwiegen. In besonders gelagerten Fällen hänge der Ausgleich jedoch von der Art der Information, ihrer Sensibilität für das Privatleben der Betroffenen, dem Interesse der Öffentlichkeit am Zugang zu der Information und der Rolle der betreffenden Person im öffentlichen Leben ab.

Anders als einige kritische Kommentare zur EuGH-Entscheidung vermuten lassen, beschränkt sich der Anspruch der Betroffenen auf Nichtanzeige bestimmter Fundstellen allein auf Suchanfragen anhand des Namens einer Person. Sonstige Suchanfragen, etwa zu thematischen Stichworten, bleiben von der Entscheidung unberührt: In ihren Ergebnislisten können sämtliche Links erscheinen – auch zu den Internetseiten und personenbezogenen Daten, die bei einer Suchanfrage zur Person nicht angezeigt werden dürften. Erst recht begründet das Urteil keine Verpflichtung, auf den verlinkten Internetseiten personenbezogene Daten zu schwärzen oder zu löschen.

Damit der EuGH den konkreten Fall überhaupt auf Grundlage der Europäischen Datenschutzrichtlinie entscheiden konnte, musste er zunächst zu ihrer räumlichen Anwendbarkeit gelangen. Der Suchmaschinenbetreiber hatte vorgetragen, seine Datenverarbeitung bei Suchanfragen würde nicht durch die in einem EU-Mitgliedsstaat befindliche Niederlassung, sondern von der Konzernmutter in einem so genannten Drittstaat ausgeführt. Daher sei kein europäisches Datenschutzrecht anwendbar. Der Gerichtshof wies dies zurück: Für die Anwendbarkeit der Richtlinie reiche es aus, dass die Niederlassung des Suchmaschinenbetreibers in dem EU-Mitgliedstaat die Aufgabe habe, dort Werbeflächen für die Suchmaschine zu verkaufen.

Die Datenschutzkonferenz hat in der Entschließung "Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen" vom 8./9. Oktober 2014 (Abdruck im Anhang) das Urteil als "fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet" gewertet und folgende Forderungen aus dem Urteil abgeleitet:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.
- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.
- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.
- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Welche Aufsichtsbehörde für einen Suchmaschinenbetreiber zuständig ist, richtet sich danach, wo dieser eine maßgebliche Niederlassung hat. Deshalb ist zum Beispiel für Google in Deutschland die Datenschutzaufsichtsbehörde von Hamburg zuständig, für Bing (Microsoft) die Datenschutzaufsichtsbehörde von Bayern. In NRW

gibt es derzeit keine maßgeblichen Niederlassungen großer Suchmaschinenbetreiber.

Das Urteil des Gerichtshofs wirft für die praktische Umsetzung im Einzelnen noch viele Fragen auf – nicht nur für Suchmaschinen, sondern auch für mögliche andere Anwendungsfälle.

➧ Ich freue mich, dass der EuGH so entschieden das Grundrecht auf informationelle Selbstbestimmung schützt. Er setzt damit Maßstäbe für die anstehende EU-Datenschutzreform.

3.5 EU-Datenschutzreform

Die Europäische Union arbeitet daran, die Datenschutzbestimmungen in Europa weiter zu vereinheitlichen. Diese Datenschutzreform ist ein umfangreiches und komplexes Vorhaben, in dem viele Interessen auszugleichen und viele Details zu beachten sind.

Im EU-Rechtsetzungsverfahren befinden sich die Datenschutz-Grundverordnung und die "JI-Richtlinie" mit Bezug auf Straftaten und Strafvollstreckung. Dieses EU-Recht soll bisheriges Recht ablösen: europäisches Recht in fast vollem Umfang und deutsches Bundes- sowie Landesrecht in weiten Teilen, wobei Einzelheiten noch offen sind. Die geplante Reform wird deshalb voraussichtlich erhebliche Auswirkungen in den meisten Rechtsbereichen entfalten, in denen Datenschutz eine Rolle spielt.

Zu den ersten Entwürfen der EU-Kommission habe ich bereits ausführlich Stellung genommen (siehe auch Bericht 2013 unter 4.1).

Inzwischen hat das Europäische Parlament eine Fülle von Änderungsanträgen zum Entwurf der Grundverordnung vorgelegt.

Der Rat der Europäischen Union, der die Regierungen der EU-Mitgliedstaaten repräsentiert, berät zurzeit über die Entwürfe der Grundverordnung. Er wird vermutlich ebenfalls umfangreiche Änderungswünsche formulieren.

Im nächsten Schritt, der voraussichtlich 2015 ansteht, werden die drei EU-Organe die Vorschläge im so genannten Trilog beraten mit dem Ziel einer gemeinsamen Endfassung für die Grundverordnung

und möglicherweise auch für die "JI-Richtlinie". Nach dem Inkrafttreten ist eine Übergangsfrist für die Geltung des neuen Rechts von derzeit zwei Jahren vorgesehen.

An der Diskussion auf Landes-, Bundes- und EU-Ebene beteilige ich mich weiterhin. Mir ist sehr daran gelegen,

1. dass der Schutz der informationellen Selbstbestimmung verbessert wird,
2. dass für Bürgerinnen und Bürger, Unternehmen und Verwaltungen praktikable und rechtssichere Regelungen geschaffen werden und
3. dass die Datenschutzaufsicht funktionsfähig und praktikabel ausgestaltet wird.

Manche Vorschläge und Beratungsbeiträge würden das bisherige Schutzniveau senken. Ich wünsche mir auch von der Bundesregierung mehr Einsatz für die Weiterentwicklung des Datenschutzstandards. Im Einzelnen sehe ich – neben vielen weiteren wichtigen Fragen – besonders die folgenden Punkte mit Sorge:

1. Es wird der Vorschlag diskutiert, für private Veröffentlichungen im Internet – besonders in sozialen Netzwerken – keine Datenschutzregeln mehr vorzusehen und so das Schutzniveau zu senken. Für betroffene Personen, deren Daten im Internet weltweit für alle veröffentlicht werden, ist es jedoch unerheblich, ob Privatpersonen oder Unternehmen dafür verantwortlich sind. Hier darf es zu keiner Verkürzung des Datenschutzes kommen.
2. Für vermeintlich "harmlose" Datenverarbeitungen wird vorschlagen, Standards von vornherein pauschal abzusenken (so genannter risikobasierter Ansatz). Spätestens im Zeitalter von Big Data mit umfassenden Verknüpfungsmöglichkeiten gibt es jedoch keine "harmlosen" Daten mehr.
3. Insbesondere bei Datenverarbeitung für personalisierte Werbung spreche ich mich dafür aus, dass nunmehr auf europäischer Ebene endlich das Einwilligungsprinzip konsequent eingeführt wird.

4. Die Entwürfe enthalten vielfach nur allgemeine Regelungsansätze. Damit ist die Gefahr verbunden, dass es über die Anwendung in der Praxis jahrelang Ungewissheit bei allen Beteiligten gibt – seien es Bürgerinnen und Bürger, Unternehmen oder Behörden. Ich spreche mich dafür aus, die wesentlichen Rechtsfragen unmittelbar in der Verordnung zu regeln, um Rechtssicherheit zu erhalten. Schließlich wird mit der Verordnung der Anspruch erhoben, eine direkt anwendbare, vollständige Regelung zu erzielen.

5. Tendenzen, die bisherige Eigenverantwortung von Stellen, die Daten verarbeiten, abzubauen und stattdessen den Datenschutzbehörden mehr Verantwortung zuzuweisen, lehne ich ab. Beispiele hierfür sind zum einen Vorschläge für Prüf- oder Genehmigungsverfahren durch die Aufsichtsbehörden, die weit über das bisher geltende Recht hinausgehen. Zum anderen betrifft dies Regelungen zu betrieblichen Datenschutzbeauftragten. Die ursprünglichen Entwürfe sehen die meisten Mitgliedstaaten leider nur als Bürokratieaufwand und sprechen sich dagegen aus. Ich werbe demgegenüber weiterhin dafür, das erfolgreiche deutsche Modell der internen Selbstkontrolle durch betriebliche und behördliche Datenschutzbeauftragte im Grundsatz zu übernehmen.

6. Mit neuen Regelungsansätzen zur Zuständigkeit der Aufsichtsbehörden ist auch eine verstärkte Abstimmung unter den europäischen Datenschutzbehörden erforderlich. Dafür wird ein komplexes System vorgeschlagen, das in kurzer Zeit abgestimmte Entscheidungen herbeiführen soll. Dies wird meine Behörde und die Zusammenarbeit der Datenschutzbehörden auf nationaler Ebene vor neue Herausforderungen stellen. Auch dazu habe ich bereits Vorschläge entwickelt.

   ➧ Ich setze mich weiterhin dafür ein, dass die europäischen Rechtsgrundlagen modernisiert, verbessert und weiter vereinheitlicht werden. Keinesfalls dürfen das bisherige Datenschutzniveau und damit der bisherige Grundrechtsschutz in NRW und in Deutschland verschlechtert werden. Gerne bin ich bereit, auch in der anstehenden Schlussphase

der Beratungen meine Arbeiten in dahingehende Bemühungen der Landesregierung einzubringen.

3.6 Unterlassungsklagen wegen Datenschutz – schädliche Parallelstrukturen

Mit der von der Bundesregierung geplanten Änderung des Unterlassungsklagengesetzes sollen Verbraucherschutzverbände sowie andere Institutionen künftig Datenschutzverstöße abmahnen und Datenschutzrechte vor Zivilgerichten kollektiv vertreten. Die Pläne verkennen die grundlegenden Unterschiede zwischen Verbraucherschutz und Datenschutz. Sie führen zu einer rechtstaatlich bedenklichen Zersplitterung von Zuständigkeiten und damit zu einer Schwächung der behördlichen Datenschutzaufsicht. Außerdem sind sie im EU-Recht nicht vorgesehen.

- Verhältnis Datenschutz und Verbraucherschutz

Datenschutz und Verbraucherschutz weisen zwar Berührungspunkte und auch Schnittmengen auf. In Bezug auf Ausgangspunkt, Reichweite und Zielsetzung bestehen jedoch erhebliche Unterschiede. Der Datenschutz zielt auf den Schutz des Persönlichkeitsrechts in Form des Rechts auf informationelle Selbstbestimmung ab und gründet sich unmittelbar auf verfassungsrechtliche Vorgaben. Der Verbraucherschutz hingegen hat die Position der einzelnen Verbraucherinnen und Verbraucher in ihrer Eigenschaft als Marktteilnehmer zum Ziel, die es im Hinblick auf Bedingungen eines freien Marktes zu schützen gilt. Im Ergebnis mögen Aktivitäten mit verbraucherschützender Zielsetzung auch dem Persönlichkeitsrecht "zugutekommen"; Entsprechendes mag ebenso für Aktivitäten aus Sicht des Datenschutzes gelten.

Ein Beispiel sind Fälle, in denen es um die Wirksamkeit vorformulierter Einwilligungserklärungen in Allgemeinen Geschäftsbedingungen geht. Mit der Beurteilung derartiger Sachverhalte aus Sicht des Verbraucherschutzes ist allerdings noch nicht in allen Fällen Abschließendes über die Rechtmäßigkeit einer dahinter stehenden Datenverarbeitung gesagt, etwa weil der Sachverhalt weitere in datenschutzrechtlicher Hinsicht relevante Fragen aufwirft. Umgekehrt wird die datenschutzrechtliche Perspektive nicht immer die Verbraucher-

schutzkomponente abdecken können, beispielsweise bei der Bewertung von Versicherungstarifmodellen, die bei "normkonformem" Verhalten Versicherten günstigere Tarife anbieten und im Gegenzug umfangreiche personenbezogene Daten zum Ernährungs-, Mobilitäts- oder sonstigen Verhalten verlangen. Über die datenschutzrechtliche Zulässigkeit solcher Modelle hinaus müsste nämlich die originär im Verbraucherschutz wurzelnde Frage in den Blick genommen werden, ob und wie in unserem Rechtssystem noch eine (echte) Wahlfreiheit zwischen verschiedenen Tarifen für Verbraucherinnen und Verbraucher gewährleistet werden kann (siehe hierzu unter 5.1 und 5.2).

Der Gesetzentwurf übersieht, dass die Bereiche Datenschutz und Verbraucherschutz voneinander zu unterscheiden sind. Datenschutz ist nicht Verbraucherschutz und umgekehrt. Auf dem Gebiet des Datenschutzes kann weder ein Vorgehen verschiedener Stellen mit unterschiedlicher Zielsetzung noch ein kondominiales Zusammenwirken von Datenschutzaufsicht und Verbraucherschutz in Betracht gezogen werden. Das schließt nicht aus, dass beide Bereiche zusammenarbeiten. Hierfür gibt es in der Praxis zahlreiche gute Beispiele. Einer gesetzlichen Regelung bedarf es nicht, zumal noch nicht einmal ansatzweise ein Befund festgestellt worden wäre, der für eine solche Regelung sprechen könnte.

- Besonderheiten der Aufsichtspraxis von Datenschutzbehörden

Prägend und wesentlich für die datenschutzrechtliche Aufsichtspraxis sind Beratung der Unternehmen, Empfehlungen, Orientierungshilfen sowie mit Unternehmensverbänden erzielte Verständigungen auf bindende Datenschutzstandards. Ansprechpartner der Wirtschaft sind die Datenschutzbehörden. Im Interesse bundesweit einheitlicher Standards verständigen sich die Behörden im Düsseldorfer Kreis regelmäßig auf die gemeinsame und einheitliche Auslegung des Datenschutzrechts und koordinieren ihre Aufsichtstätigkeit. Sind auf dem Gebiet des Datenschutzes weitere Institutionen - mit anderer Aufgabenstellung und der kollektiven Rechtsbehelfen innewohnenden Breitenwirkung - tätig, wird die Wirtschaft sich nicht oder nicht mehr in dem bisherigen Maße an die Datenschutzbehörden wenden. Mit den Aufsichtsbehörden vereinbarte Standards verlören an Bedeutung. Die Folge wäre der Abbau der Einheitlichkeit der Aufsichtspraxis in Deutschland, ausgerechnet in einer Phase, in der das Zusammenwirken und Bündeln der Datenschutzpraxis in Deutschland unabdingbar

ist für die vorgesehene enge Zusammenarbeit der Datenschutzbehörden in der Europäischen Union.

Eine bedeutsame Errungenschaft des modernen Rechtsstaates liegt gerade darin, dass es diesem gelungen ist, Doppelzuständigkeiten abzubauen und für die Bürgerinnen und Bürger klare Zuständigkeiten der unterschiedlichen Stellen, seien sie öffentlich-rechtlicher oder privatrechtlicher Natur, festzulegen. Wenn neben der Datenschutzaufsicht andere Institutionen regulierend auf Unternehmen mit vergleichbarer Breitenwirkung einwirken, ist aus Sicht der Unternehmen und ebenso der betroffenen Bürgerinnen und Bürger die Rollenverteilung zwischen den "Akteuren" nicht mehr klar. Gerade Klarheit über zuständige Ansprechpartner und die Verlässlichkeit ihrer Aussagen gehören zum Kern des Rechtsstaates.

Zudem ist die rechtsstaatliche Bindung der Datenschutzaufsicht von grundlegender Bedeutung. Der Datenschutzaufsicht werden im Unterschied zum Verbraucherschutz weitgehende Untersuchungsbefugnisse im Rahmen eines förmlich ausgestalteten Verwaltungsverfahrens übertragen. Am Ende kann eine behördliche Anordnung stehen, die von den Verwaltungsgerichten überprüft werden kann. Die Datenschutzaufsicht ist zugleich Verwaltungsbehörde in Ordnungswidrigkeitenverfahren und kann demnach Bußgelder verhängen. Mit Blick auf rechtsstaatliche Anforderungen sind Einwirkungen in den grundrechtlich geschützten eingerichteten und ausgeübten Gewerbebetrieb an starke Verfahrensgarantien gebunden und nur Behörden zugewiesen. Am Ende eines Verwaltungsverfahrens müssen die in rechtlicher und tatsächlicher Hinsicht entscheidungserheblichen Gesichtspunkte zusammengestellt und nachvollziehbar abgewogen sein.

Zwar haben auch Individualklagen vor den Zivilgerichten, für die das alles nicht gilt, eine große Bedeutung für die richterliche Fortentwicklung des Datenschutzes. Kollektiv gestaltete Verbandsrechte führen jedoch zu deutlich anderen und intensiveren Einwirkungen auf Grundrechtsträger als Individualklagen. Sie sind auch systematisch mit ihnen nicht gleichzusetzen. Im Übrigen kann sich jede Bürgerin und jeder Bürger an die Datenschutzbehörden wenden, ohne dass dies mit Kosten oder sonstigen Mühen verbunden wäre. Es stellt sich demnach die Frage, welchen Sinn es dann noch hat, dass die Rechtsordnung auch auf Ebene der EU ein klassisch öffentlich-rechtliches Aufsichtssystem mit Datenschutzbehörden vorsieht, wenn daneben

ebenso sonstige Akteure mit Breitenwirkung ohne vergleichbare Verfahrensbindung und Untersuchungsrechte mit datenschutzrechtlicher Zielsetzung gerichtliche Verfahren in Gang setzen können.

Vorteile, die den Bürgerinnen und Bürgern möglicherweise dadurch entstehen, dass sich weitere Akteure um den Datenschutz kümmern, vermögen die Nachteile nicht auszugleichen.

- EU-Recht

Weder die geltende Datenschutzrichtlinie der EU noch die Entwürfe zur EU-Datenschutzgrundverordnung sehen kollektiv ausgestaltete Rechtsbehelfe vor. Im System des EU-Rechts ist demgegenüber eine starke behördliche Datenschutzaufsicht vorgesehen.

➧ Um den Datenschutz zu verbessern, sollten nicht privatrechtliche Parallelstrukturen geschaffen werden, die überdies zu einer Schwächung des bisherigen Systems führen. Stattdessen gilt es, die Datenschutzbehörden durch eine angemessene Ausstattung zu stärken.

4 Mediendienste

4.1 Smartes Fernsehen nur mit smartem Datenschutz!

Moderne Fernsehgeräte (Smart-TVs) bieten neben dem Empfang des Fernsehsignals unter anderem die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauerinnen und Zuschauern ist es somit möglich, sich simultan zum laufenden TV-Programm zusätzliche Web-Inhalte auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte unterschiedliche Internet-Dienste an. Für die Zuschauerinnen und Zuschauer ist aufgrund dieser Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Die eingesetzte Technik kann zudem eine Nutzungsanalyse erlauben. Anonymes Fernsehen muss aber auch mit einem Smart-TV-Gerät weiter möglich bleiben.

Durch die Online-Verbindung entsteht – anders als beim bisherigen linearen Fernsehen über DVB-C/S/T – ein Rückkanal von Zuschauerin

und Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Meine Analysen der Datenströme, die bei Nutzung von Smart-TV-Geräten mit Online-Verbindung ausgelöst werden, haben bestätigt, dass Daten sowohl an den Hersteller des Gerätes, als auch bei aktivierter HbbTV-Funktion an die Rundfunkanstalten und überdies an Dritte übertragen werden. Teilweise fließen so Daten, ohne dass die Nutzerin oder der Nutzer hierüber, wie vom Gesetz verlangt, hinreichende Informationen erhält oder der Datenübertragung ausdrücklich zugestimmt hätte.

Daher fordere ich alle Hersteller von Smart-TV-Geräten, die Rundfunkanstalten und sonstige Anbieter von Online-Diensten für smarte TV-Geräte auf, die datenschutzrechtlichen Mindestanforderungen zu beachten.

Anonymes Fernsehen – dies ist das zentrale Anliegen – muss auch bei Nutzung eines Smart-TV-Gerätes weiterhin möglich bleiben. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauerinnen und Zuschauer unzulässig.

Daneben gibt das Telemediengesetz für Anbieter einen gesetzlichen Rahmen vor, innerhalb dessen Online-Angebote ausgestalten werden können:

- Nutzerinnen und Nutzer sind insbesondere zu Beginn der Nutzung über Erhebung und Verwendung ihrer Daten zu informieren.
- Pseudonyme Nutzungsprofile dürfen nur erstellt werden, sofern hierüber hinreichend unterrichtet wurde und die Nutzerinnen und Nutzer dem nicht widersprochen haben.
- Das Prinzip "privacy by default" ist zu beachten: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird.

- Smart-TV-Geräte, HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Das Recht auf freien und unbeobachteten Medienzugang darf durch unzulässige Erhebung von Zuschauerdaten nicht gefährdet werden.

Um meiner Forderung Nachdruck zu verleihen, habe ich in einem Beschluss "Smartes Fernsehen nur mit smartem Datenschutz" vom Mai 2014 (Abdruck im Anhang) gemeinsam mit allen Aufsichtsbehörden des Bundes und der Länder sowie den Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten auf die gesetzlichen Vorgaben zu Informationspflichten und Profilbildung im Zusammenhang mit dem Angebot von Online-Diensten hingewiesen. Dieser Position haben sich auch die Landesmedienanstalten angeschlossen.

Daneben habe ich die Hersteller von Smart-TV-Endgeräten in meinem Zuständigkeitsbereich aufgefordert, die internen Datenverarbeitungsprozesse offenzulegen und zu erläutern. Auf der Grundlage der erteilten Auskünfte berate ich derzeit die Hersteller bei der Nachbesserung ihrer Datenschutzhinweise und Registrierungsprozesse.

➧ Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung und Auswertung des Nutzungsverhaltens empfindlich beeinträchtigt. Daher ist es mir ein besonderes Anliegen sicherzustellen, dass die Anbieter und Endgerätehersteller in meinem Zuständigkeitsbereich das Recht der Nutzerinnen und Nutzer auf informationelle Selbstbestimmung beachten.

4.2 Soziale Netzwerke

Für viele Menschen gehören soziale Netzwerke zum Alltag. Sie kommunizieren über alle Altersgruppen hinweg ganz selbst-

verständlich auf diesem Weg und bedienen sich gerne der dadurch gegebenen Möglichkeiten zum Austausch und zum Teilen von Informationen und Fotos – weltweit. Allerdings entsprechen noch immer insbesondere die Angebote ausländischer Anbieter oft nicht den deutschen Anforderungen des Datenschutzes. Es fehlt etwa an Information über die interne Datenverarbeitung und Nutzerdaten werden ohne die erforderliche Einwilligung verarbeitet.

Anfragen und Beschwerden von Bürgerinnen und Bürgern machen deutlich, dass teilweise große Unsicherheiten bei der Nutzung sozialer Netzwerke bestehen. Daher ist es nach wie vor ein wichtiger Bestandteil meiner Beratungstätigkeit, über die Risiken, die mit der Nutzung dieser Dienste verbunden sind, zu informieren und Hinweise und Anleitung zum sicheren Umgang mit sozialen Netzwerke zu geben (auch auf meiner Internetseite unter www.ldi.nrw.de).

Zusätzlich müssen auch die Netzwerkbetreiber auf ihre Verantwortung und den rechtlichen Rahmen ihres Angebotes hingewiesen werden. Die Einhaltung der rechtlichen Vorgaben muss durchgesetzt werden.

So haben die Datenschutzaufsichtsbehörden des Bundes und der Länder nachdrücklich darauf hingewiesen, dass biometrische Gesichtserkennung durch Internetdienste nur nach umfassender Information und wirksamer Einwilligung der Betroffenen rechtmäßig erfolgen kann (Entschließung "Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!" vom 27./28. März 2014; Abdruck im Anhang).

Darüber hinaus haben die Datenschutzaufsichtsbehörden des Bundes und der Länder im Frühjahr 2013 gemeinsam eine Orientierungshilfe "Soziale Netzwerke" erstellt, die die gesetzlichen Anforderungen an die Ausgestaltung des Angebotes sozialer Netzwerkdienste erläutert. Die Orientierungshilfe soll Betreiber sozialer Netzwerke sowie öffentliche und private Stellen, die die Netzwerke nutzen, bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen (siehe www.ldi.nrw.de).

Die Erarbeitung dieser Orientierungshilfe war auch deshalb angezeigt, da die Initiative zur Selbstregulierung sozialer Netzwerke eingestellt wurde. Sie war im Frühjahr 2013 angetreten, um einen ge-

meinsamen Verhaltenskodex der Netzbetreiber zu erarbeiten. Der Dialog zwischen dem Bundesministerium des Innern und der FSM (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V.) mit den großen sozialen Netzwerken, an dem ich mich als Vertreter der Aufsichtsbehörden des Bundes und der Länder ebenfalls beteiligt habe, scheiterte bedauerlicherweise überwiegend an der mangelnden Bereitschaft ausländischer Netzwerkbetreiber.

Trotz dieser Erfahrung halte ich es nach wie vor für sinnvoll, das Gespräch mit den verantwortlichen Stellen zu suchen. Ich unterstütze daher die Initiative der Konferenz der Innenminister und -senatoren, gemeinsam mit den Aufsichtsbehörden erneut Gespräche mit Facebook aufzunehmen, um weitere Informationen über die dortigen technischen Verfahren zu erhalten. Bereits im Frühjahr 2014 wurde Facebook zur Vorbereitung dieser Gespräche ein umfassender Fragenkatalog übermittelt. Die Antworten Facebooks hierauf werden wir Anfang 2015 ausführlich mit dem Unternehmen erörtern.

Die Ministerien des Landes habe ich in den vergangenen Jahren bei den Planungen von eigenen Profilseiten in sozialen Netzwerken beraten. Dabei habe ich mehrfach darauf hingewiesen, dass insbesondere bei den ausländischen Anbietern wesentliche Angaben über die dortigen Datenverarbeitungsprozesse bislang fehlen, so dass den Nutzerinnen und Nutzern nicht die gesetzlich geforderten Informationen zur Verfügung gestellt werden können. Die Landesregierung hat im Sommer 2014 allerdings mitgeteilt, dass ungeachtet dieser bekannten Risiken auch weiterhin Profilseiten öffentlicher Stellen in NRW in ausländischen sozialen Netzwerken angeboten werden sollen. Im Polizeibereich wurde die Nutzung von sozialen Netzwerken für Polizeibehörden per Erlass im Juli 2014 in festgelegten Grenzen zugelassen.

Diese Vorgehensweise irritiert umso mehr, als ich in vielen Gesprächen mit verschiedenen Ressorts sowie in mehreren Schreiben darauf hingewiesen habe, dass insbesondere öffentliche Stellen – ungeachtet der rechtlichen Anforderungen – eine besondere Verantwortung für die Daten der Bürgerinnen und Bürger tragen. Diese vertrauen dem Zugang zur Behörde per Internet und sie dürfen nicht in eine Lage versetzt werden, in der sie den Kontakt zur Behörde ohne ihr Wissen gleichsam mit ihren Daten bezahlen. Andere Landesregierungen, wie etwa in Mecklenburg-Vorpommern, stellen sich konsequent

dieser Verantwortung, indem sie ausdrücklich auf die Nutzung sozialer Netzwerke verzichten.

Um die Risiken von Profilseiten öffentlicher Stellen in sozialen Netzwerken für die Bürgerinnen und Bürger jedoch zumindest so weit wie möglich zu verringern, biete ich den öffentlichen Stellen in NRW gleichwohl weiterhin meine Beratung an. Sofern das Angebot ausländischer sozialer Netzwerke – aus welchen Beweggründen heraus auch immer – entgegen meiner Hinweise genutzt wird, sollten zumindest die folgenden Kriterien beachtet werden:

1. Nutzung von Profilseiten durch öffentliche Stellen ausschließlich für Zwecke der Öffentlichkeitsarbeit
2. Information der Nutzerinnen und Nutzer über prominent platzierte und deutliche eigene Datenschutzhinweise
3. Vollständige Abbildung der eigenen Inhalte von Profilseiten auch auf der eigenen Internetseite
4. Unterbinden jeglicher Kommentar- und sonstiger interaktiver Funktionen der Fanpage
5. Keine direkte Einbindung von Social-Plug-Ins auf der Homepage, allenfalls im Wege der 2-Klick-Lösung
6. Unterbindung der direkten Auffindbarkeit der Profilseite über Suchmaschinen
7. Keine Ausrichtung des Angebotes an Kinder und Jugendliche
8. Beachtung der Impressumspflicht.

➧ Auch in Zukunft werde ich im Rahmen meiner Zuständigkeit auf die Betreiber sozialer Netzwerke einwirken, um die Durchsetzung deutscher Datenschutzstandards voranzutreiben. Solange die Angebote nicht umfassend datenschutzfreundlich gestaltet sind, ist die Nutzung durch private oder öffentliche Stellen weiterhin kritisch zu bewerten. Bürgerinnen und Bürger, die soziale Netzwerke nutzen möchten, sollten sich gut über die Risiken informieren und sich bewusst entscheiden.

4.3 Datenschutzanforderungen an mobile Applikationen ("Apps")

"Smarte" mobile Endgeräte wie Smartphones und Tablets haben in den letzten Jahren enorme Verbreitung gefunden. Mobile Applikationen, die teilweise auf den Endgeräten vorinstalliert sind oder von den Nutzerinnen und Nutzern individuell heruntergeladen werden können, sind kleine Programme, mit denen diese Endgeräte um weitere Funktionen ergänzt werden können. Von der Taschenlampe bis hin zum Navigationssystem bieten sie Zusatzfunktionen für verschiedene Zwecke an.

Verfügbar sind Apps über spezielle Online-Plattformen. Über diesen Weg können Nutzerinnen und Nutzer Apps unkompliziert beziehen und direkt auf dem Endgerät installieren. Verschiedene Plattformen wetteifern um die Gunst der Nutzerinnen und Nutzer. Für Apple-Endgeräte können mobile Apps derzeit ausschließlich über den "App Store" bezogen werden, für Android-Geräte steht unter anderem der "Google Play Store" zur Verfügung – und weitere drängen in den Markt.

Häufig sind Apps Anwendungen, für deren Nutzung eine Online-Verbindung erforderlich ist. Darüber hinaus sind sie oft eng an das jeweilige Endgerät gekoppelt, mit dem sie genutzt werden: Über Programmschnittstellen kann ein Zugriff auf die dort gespeicherten personenbezogenen Daten erfolgen. So nutzen beispielsweise Apps sozialer Netzwerke häufig die Kontakte aus dem Adressbuch des Gerätes oder Apps mit Navigationsfunktion ermitteln den jeweiligen Standort des Endgerätes. Manche Apps greifen auch auf Daten zu, die für ihre Funktion gar nicht erforderlich sind, zum Beispiel auf das Adressbuch, obwohl dies etwa für eine Taschenlampenfunktion nicht gebraucht wird.

Für die Nutzerinnen und Nutzer ist der Prozess des Downloads einer App zunächst sehr einfach gestaltet. Die Datenströme, die anschließend durch die Nutzung einer App ausgelöst werden, sind allerdings oft nicht transparent, da entweder gar keine Datenschutzhinweise durch die App-Anbieter gegeben werden oder diese nur unzureichend sind. Häufig wird die Einwilligung, die für die Nutzung der Daten erforderlich ist, nicht oder nur auf der Basis lückenhafter Informationen

eingeholt. Den Nutzerinnen und Nutzern ist vielfach nicht bewusst, welche ihrer personenbezogenen Daten wie Standort, Endgeräte-Kennung, Mobilfunknummer usw. weitergeleitet und verarbeitet werden. Auch zu welchem Zweck dies geschieht, ist oft unbekannt.

App-Entwickler und Anbieter tragen hier eine besondere Verantwortung und müssen bereits in der Entstehungs- und Entwicklungsphase einer App die datenschutzrechtlichen Vorgaben kennen und beachten. Zu deren Beratung haben die Datenschutzaufsichtsbehörden des Bundes und der Länder daher im Sommer 2014 in einer gemeinsam erarbeiteten Orientierungshilfe die rechtlichen und technischen Datenschutzanforderungen zusammengefasst (abrufbar unter www.ldi.nrw.de). Ziel ist, dass bereits durch datenschutzgerechte Gestaltung ("privacy by design") sowie datenschutzfreundliche Voreinstellungen ("privacy by default") Apps später ohne datenschutzrechtliche Mängel angeboten werden können.

Um zu überprüfen, ob diese Anforderungen von App-Anbietern mit Sitz in NRW – seien es Unternehmen oder Behörden – eingehalten werden, habe ich Ende 2014 ein App-Prüflabor eingerichtet. Dadurch bin ich jetzt in der Lage zu ermitteln, welche Daten der Nutzerinnen und Nutzer über eine App tatsächlich übertragen werden und ob auch die Darstellung in den jeweiligen Nutzungsbedingungen und Datenschutzerklärungen hiermit übereinstimmt.

Das Prüfverfahren sieht wie folgt aus:

Um den Datenaustausch zwischen einem Test-Smartphone meiner Behörde und der über eine App in Anspruch genommenen Dienstleistung im Internet erfassen zu können, wird die WLAN-Schnittstelle des Test-Smartphones genutzt.

Auf dem Weg vom Testgerät in das Internet ist im App-Prüflabor ein Rechner zwischengeschaltet. Der Rechner ermöglicht als technische Zwischeninstanz, den Datenstrom zu Analysezwecken auszuleiten, während die App auf dem Test-Smartphone in üblicher Weise aufgerufen wird.

Somit lässt sich feststellen, mit welchen Internetseiten oder Dienstleistern eine App tatsächlich kommuniziert und welche Datenströme bei Installation, Start, Nutzung und Beenden der App jeweils anfallen. Falls der Datenaustausch nicht verschlüsselt ist, kann ebenso festge-

stellt werden, welche Daten aus dem Test-Smartphone ausgelesen werden.

➧ Applikationen für Smartphones und Tablets bergen nach wie vor Risiken für die Daten der Nutzerinnen und Nutzer, da häufig intransparent bleibt, welche Daten durch die App tatsächlich genutzt und übertragen werden. Vollständige Nutzerinformation über Datenverarbeitungsprozesse ist daher meine Kernforderung an die Anbieter dieser Dienste.

5 Wirtschaft

5.1 Pay As You Drive – Neue Produktentwicklung im Bereich der Kfz-Versicherung

Kfz-Haftpflichtversicherer bemessen Prämien unter anderem nach Zahl der verursachten Schäden, Wohnort, Automarke und Kilometerzahl pro Jahr. Auch wird mit dem Schadensfreiheitsrabatt das unfallfreie Fahren honoriert. Nun – dies ist eine neue Dimension – bietet ein Versicherungsunternehmen mit Sitz in NRW an, das Fahrverhalten mittels einer im Auto fest installierten Box kontinuierlich zu analysieren, um die Beiträge nach dem individuellen Fahrverhalten zu gestalten. Solche Tarifsysteme gibt es bereits in den USA und in einigen europäischen Ländern. Doch Vorsicht ist geboten.

Mit Einverständnis der Versicherungsnehmerin oder des Versicherungsnehmers wird eine Telematik-Box im privat genutzten Fahrzeug montiert. Die Box sendet im Sekundentakt Daten über das Fahrverhalten – zum Beispiel Fahrtstrecke, Zeit, Geschwindigkeit(-sübertretungen), Brems- und Beschleunigungsverhalten – an ein Telekommunikationsunternehmen, das mit einem Unternehmen für Telematik zusammenarbeitet. Die Daten werden auf einem Server in Europa verarbeitet. Aus den Fahrdaten berechnet sich ein Gesamtscore und vier Unterscores (Geschwindigkeit, Fahrweise, Nachtfahrten, Stadtfahrten). Das Telematikunternehmen leitet diese Werte sowie die gefahrenen Gesamtkilometer einmal monatlich sowie als Jahresübersicht an den Versicherer weiter, der den individuellen Tarif ermittelt. Ein Fahrverhalten, das die vorgegebenen Parameter ein-

hält, führt zu einer Beitragsrückerstattung. Die Datenverarbeitung erfolgt nicht mit Klarnamen, sondern mit einer Kunden-Identifikations-Nummer. Versicherungsnehmerinnen und Versicherungsnehmer können Fahrdaten und Scores auf dem Webportal oder mittels einer Smartphone-App einsehen. Bei einem Unfallereignis sendet die Box ein Notrufsignal. Im Fall eines Diebstahls kann das Fahrzeug geortet werden.

Im Rahmen seiner Beratungsanfrage habe ich den Versicherer auf meine grundsätzlichen Bedenken hingewiesen, da die gesammelten Datenmengen für ein Bewegungsprofil missbraucht werden könnten. Wir befinden uns hiermit auf einem gefährlichen Weg: Wer eine Versicherungsleistung zu einem günstigeren Preis haben möchte, bezahlt mit einem Teil seiner Privatsphäre. Mittlerweile denken auch Krankenversicherungen daran, Tarife vom Gesundheitsverhalten ihrer Kundinnen und Kunden abhängig zu machen.

Dem Kfz-Versicherer habe ich unter anderem folgende Anforderungen mitgeteilt:

- Telekommunikationsunternehmen und Telematikunternehmen dürfen Daten über das Fahrverhalten keiner Person zuordnen können. Die Trennung in zwei Datenkreise – komplette Fahrdaten und Scores einerseits, Daten für die Zuordnung zur Person andererseits – muss gewährleistet sein. Der Versicherer kann zwar eine Personenzuordnung vornehmen, erhält aber außer der Gesamtkilometerzahl keine weiteren Fahrdaten sondern nur aggregierte Werte (Scores).
- Daten werden sowohl in der Telematik-Box als auch bei Übertragung und Speicherung nach dem jeweils aktuellen technischen Standard verschlüsselt. Auch ist die Box so zu gestalten, dass Zugriffe und Manipulationen an der Hardware von außen ausgeschlossen sind.
- Bei mehreren Fahrerinnen und Fahrer müssen sich diese individuell vor Fahrtantritt entscheiden können, ob sie eine Aufzeichnung ihres Fahrverhaltens dulden. Mindestens stellt der Versicherer einen Aufkleber zur Verfügung, der – zum Beispiel auf dem Lenkrad angebracht – darauf hinweist, dass eine individuelle Fahrtaufzeichnung stattfindet.

- Die erhobenen Daten werden nur für die Tarifgestaltung verwandt. Eine Nutzung für Schadensregulierung ist auszuschließen.
- Versicherungsnehmerinnen und Versicherungsnehmer werden im Vorfeld umfassend und verständlich über die Datenverarbeitung und die beteiligten Stellen unterrichtet. Sie werden darauf hingewiesen, dass sie der Datenweitergabe an Werkstätten im Falle eines Unfalls widersprechen können.

➧ Die Tendenz der Versicherungswirtschaft zu individualisierten Tarifen ist datenschutzrechtlich kritisch zu begleiten. Neben Datenschutz, Verbraucherschutz und Versicherungsaufsicht ist auch die Politik gefragt. Es ist Zeit für eine gesellschaftliche Debatte darüber, wo insbesondere bei Pflichtversicherungen Grenzen für solche Geschäftsmodelle zu ziehen sind.

5.2 Wearable Computing

Computer und Sensoren, die wie Schmuck, Brillen oder Kleidungsstücke am Körper getragen werden (so genanntes "Wearable Computing") liegen im Trend. Beispiele hierfür sind die Brille "Google Glass", die Armbanduhr "Apple Watch" oder die Fitness-Armbänder verschiedener Hersteller. Auch wenn viele Funktionalitäten derartiger Computer meist von anderen Geräten wie dem Smartphone bekannt sind, kann die Art und Weise der Benutzung von Wearable Computing besondere Gefährdungen für die Privatsphäre der Nutzerinnen und Nutzer sowie Dritter mit sich bringen. Zudem sind neue Geschäftsmodelle auf der Basis von Wearable Computing aufmerksam zu beobachten.

Die Nutzung von Wearable Computing unterliegt denselben rechtlichen Vorgaben zum Datenschutz wie die Nutzung sonstiger Computer, Smartphones oder ähnlicher IT-Systeme. Auch wenn Wearable Computing etwa gegenüber herkömmlichen Smartphones häufig gar keine neuen Funktionalitäten aufweist, ergeben sich durch die Art der Verwendung sowohl hinsichtlich der Quantität als auch der Qualität der Datenverarbeitung neue Gefährdungspotentiale für die Privatsphäre.

Aufgrund der dauernden Verfügbarkeit und der einfachen Nutzung lassen sich zum Beispiel mit der Kamera in "Google Glass" leichter Fotos und Videos von Personen aufnehmen, die unter Umständen dem Intimbereich zuzuordnen sind. Es ist zudem für Betroffene nur schwer erkennbar, ob sie fotografiert worden sind. Dies erschwert im Vorhinein, eine Abbildung zu verhindern, sowie im Nachhinein, Rechte gegen eine unberechtigte Abbildung geltend zu machen. Zwar verbietet Google in seinen Nutzungsbedingungen derzeit die Nutzung von "Google Glass" zum Zweck der Gesichtserkennung sowie der Spracherkennung. Auch hat Google angekündigt, die Testphase des Produkts zu beenden und das Gerät nicht mehr auszuliefern. Doch können Nutzungsbedingungen für die bereits ausgelieferten Modelle von Google in der Zukunft einseitig geändert werden. Außerdem hat das Unternehmen eine Neuentwicklung der Brille angekündigt.

"Apple Watch" soll nach den Berichten zur Vorstellung des Gerätes etwa die Aufzeichnung der Herzfrequenz ermöglichen. Diese Daten ermöglichen es, insbesondere in Verbindung mit weiteren Daten ein umfassendes Abbild des Tagesablaufs der Nutzerinnen und Nutzer zu erstellen und möglicherweise Aussagen über den Gesundheitszustand zu treffen. Fitness-Armbänder mit entsprechenden Sensoren zielen genau hierauf ab.

Für eine rechtlich zulässige Erhebung und Nutzung solcher Daten durch die Anbieter der Geräte bzw. der Dienste ist regelmäßig die Einwilligung der betroffenen Person erforderlich. Dies gilt für ein Foto mit "Google Glass" ebenso wie für die Daten, die mittels "Apple Watch" oder Fitness-Armband aufgezeichnet werden. Die Einwilligung erfordert die bewusste und freiwillige Entscheidung der Nutzerinnen und Nutzer für den Dienst oder das Produkt. Hierzu müssen sie insbesondere umfassend von den Herstellern und Anbietern über Umfang und Zwecke der Datenverarbeitung sowie über die mögliche Weitergabe der Daten an Dritte informiert werden. Des Weiteren sind die Produkte und Dienste vor dem unberechtigten Zugriff durch Dritte abzusichern. Andernfalls könnte sich zum Beispiel ein Angreifer die Kontrolle über das Gerät und alle seine Funktionalitäten verschaffen. Ein solcher Angriff hätte vor dem Hintergrund der potentiell ständigen Verfügbarkeit des Geräts und des möglichen Eingriffs in den Intimbereich der Betroffenen eine besonders gesteigerte Intensität.

Die Verfügbarkeit von großen Datenmengen, die sehr persönliche Analysen ermöglichen, ruft Begehrlichkeiten auch bei Unternehmen hervor. Versicherungsunternehmen planen bereits, Rabatte oder Bonuszahlungen anzubieten, wenn Kundinnen und Kunden ihre Fitness durch Wearable Computing analysieren lassen und die "richtigen" Werte nachweisen. Mit solchen Geschäftsmodellen wird ein finanzieller Druck erzeugt, tiefen Einblick in Lebensgewohnheiten und Gesundheit zu ermöglichen und auch noch die Gesundheitsdaten zu kommerzialisieren (siehe hierzu unter 5.1).

➧ Es geht nicht darum, neue Dienste und Produkte wie Wearable Computing zu verteufeln. Hersteller von Geräten und Anbieter solcher Dienste müssen aber eine bewusste und freiwillige Einwilligung ermöglichen. Die Nutzerinnen und Nutzer sollten sich der Gefahren für die eigene und die Privatsphäre Dritter bewusst sein.

5.3 Scoring – der Mensch als Objekt einer undurchsichtigen Computerentscheidung

Im Wirtschaftsleben hat die Beauskunftung von so genannten Scorewerten durch Wirtschaftsauskunfteien erheblichen Einfluss auf die Entscheidung über Abschluss und Konditionen von Verträgen. Bei diesen Scorewerten handelt es sich um statistisch-mathematisch erstellte Prognosewerte, die angeben sollen, mit welcher Wahrscheinlichkeit jemand seinen Zahlungsverpflichtungen nachkommen wird. Daher ist es für den Einzelnen wichtig, dass die Grundlagen für die Bewertung der Zahlungsfähigkeit und die Berechnung der Scorewerte seriös und transparent sind.

In meinem Bericht 2011 unter 6.1 hatte ich die neuen Regelungen zum Scoring und die erweiterten Auskunftsrechte zu den Scorewerten nach § 34 Abs. 2 und 4 Bundesdatenschutzgesetz (BDSG) erläutert.

Die Frage nach der Transparenz des Scoring ist nach wie vor aktuell, wie eine Entscheidung des Bundesgerichtshofs von Januar 2014 zum Auskunftsanspruch beim Scoring zeigt (BGH, Urteil vom 28. Januar 2014 – VI ZR 156/13). Hintergrund der Klage war ein abgelehnter

Kreditvertrag aufgrund einer falschen Negativauskunft einer Auskunftei. Die Klägerin wollte daraufhin von der Wirtschaftsauskunftei gemäß § 34 BDSG wissen, welche Daten über sie gespeichert sind und wie genau ihr Scorewert berechnet wurde. Die Auskunftei verweigerte ihr die Offenlegung der Gewichtung ihrer einzelnen Merkmale, die zugrunde gelegten Statistiken und die Informationen zu ihrer Vergleichsgruppe. Der BGH hat in seinem Urteil deutlich gemacht, dass der Auskunftsanspruch nach § 34 BDSG die Wirtschaftsauskunfteien verpflichtet, die Betroffenen nachvollziehbar über alle zu ihrer Person gespeicherten Einzeldaten (bloße Datenkategorien reichen nicht), an die für das Scoring angeknüpft wird, zu informieren, damit die Betroffenen deren Richtigkeit überprüfen können.

Der BGH entnahm der Gesetzesbegründung jedoch auch, dass die so genannte Scoreformel als Geschäftsgeheimnis der Auskunfteien geschützt werde und damit den Betroffenen nicht mitzuteilen sei. Somit müsse die Auskunftei keine Auskunft zu der Vergleichsgruppe geben, der die Betroffenen zugeordnet wurden, und auch nicht zur Gewichtung der Faktoren, die in die Scoreberechnung eingeflossen sind. Im Ergebnis erfahren die Betroffenen nur, welche Einzeldaten zu ihrer Person gespeichert sind; sie können aber nicht überprüfen, wie ein bestimmter Scorewert errechnet wird. Die Berechnung des Ergebnisses ist für sie nicht nachprüfbar.

Die Betroffenen müssen im Mindestmaß eine Vorstellung über die Gewichtung der Daten erhalten. Der effektive Rechtsschutz muss sichergestellt sein. Dazu gehört auch, dass die Betroffenen erkennen können, welche Merkmale das Ergebnis maßgeblich geprägt haben. Die Entscheidung zeigt, dass der Gesetzgeber hinsichtlich der Transparenz des Scorings auf halber Strecke stehengeblieben ist. Die Betroffenen sehen, was in die "Blackbox" hineingeht und was wieder herauskommt, in der "Blackbox" selbst tappen sie jedoch weiterhin im Dunkeln. Die Betroffenen bleiben das hilflose Objekt einer undurchsichtigen Computerentscheidung.

➧ Ich bezweifele, dass dem Gesetzgeber mit der derzeitigen Gesetzeslage der verfassungsrechtlich gebotene angemessene Ausgleich der betroffenen Grundrechtspositionen gelungen ist. Hier besteht Nachholbedarf. Um ein transparentes, seriöses und diskriminierungsfreies Scoring sicherzustel-

len, setze ich mich daher insbesondere dafür ein, den Auskunftsanspruch über Scoringverfahren zu erweitern.

5.4 Gewerblicher Handel mit Kfz-Nutzungs- und Unfallhistorien

In der letzten Zeit häufen sich die Ideen von Unternehmen, Nutzungs- und Unfallhistorien von Kraftfahrzeugen zu sammeln und Kaufinteressentinnen und -interessenten von Gebrauchtwagen zur Verfügung zu stellen. Die Abfrage soll dabei über die Fahrzeugidentifikationsnummer (FIN) erfolgen. Die Überlegung, vor einem Gebrauchtwagenkauf valide Informationen zur Verfügung zu stellen, ohne sich auf die Angaben der Verkäuferseite verlassen zu müssen, ist durchaus nachvollziehbar. Allerdings betreffen die Fahrzeughistorien nicht nur die Fahrzeuge, vielmehr sind dadurch auch Rückschlüsse auf das Verhalten der Fahrerinnen und Fahrer möglich.

Nach Ansicht der Unternehmen handelt es sich bei den zu einer FIN gespeicherten Fahrzeugdaten nicht um personenbezogene Daten, sondern lediglich um sachbezogene Daten. Der Schutz des Bundesdatenschutzgesetzes greift nach § 3 Abs. 1 BDSG aber schon dann, wenn die Daten personenbeziehbar sind, ein Personenbezug also ohne unverhältnismäßig großen Aufwand hergestellt werden kann. Dies ist anhand der FIN ohne weiteres möglich.

Datenverarbeitungen und -nutzungen sind nur zulässig, wenn eine Rechtsvorschrift diese erlaubt oder die Betroffenen freiwillig eingewilligt haben (§ 4 Abs. 2 Satz 2 BDSG).

Die Unternehmen beabsichtigen meistens, die Informationen zur Unfallhistorie eines Fahrzeugs von der Versicherungswirtschaft zu beziehen. Die im so genannten Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) – siehe Bericht 2007 unter 7.3 – gespeicherten Daten werden von den Versicherungsunternehmen jedoch nur für die Versicherungswirtschaft übermittelt und dienen versicherungsintern der Betrugsprävention sowie dem Abschätzen von Versicherungsrisiken. Der HIS-Betreiber darf diese Daten daher ausschließlich zu diesem Zweck nutzen: eine Übermittlung der Daten an Unternehmen zu versicherungsfremden Zwecken ist unzulässig.

Als gesetzliche Rechtsgrundlage einer derartigen Auskunftei käme zunächst § 29 BDSG in Betracht. Hiernach dürfen diese Unternehmen die gespeicherten Daten an ihre Kundinnen und Kunden nur übermitteln, wenn diese ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt haben und kein Grund zu der Annahme besteht, dass die Betroffenen ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Selbst wenn ein Informationsinteresse ausreichend glaubhaft dargelegt werden kann (zum Beispiel unter Hinweis auf konkrete Kaufverhandlungen), stehen jedenfalls gewichtige schutzwürdige Interessen der früheren Fahrerinnen und Fahrer entgegen. Denn mittels einer einfachen Halterabfrage kann die Identität der früheren Fahrzeughalterinnen und -halter ermittelt und so unter anderem festgestellt werden, wo und wann das Fahrzeug in einen Unfall verwickelt war. Diese Informationen erlauben Rückschlüsse auf das Fahrverhalten oder Aufenthaltsorte zu einem bestimmten Zeitpunkt. Damit besteht die nicht unerhebliche Gefahr der Entstehung von Bewegungs- und Fahrverhaltensprofilen. Ein derartiges Portal kann daher nicht auf der gesetzlichen Grundlage des § 29 BDSG betrieben werden, so dass nur noch eine Einwilligung der Betroffenen als Rechtsgrundlage in Betracht käme.

Aber auch eine Einwilligung scheitert an der in § 4a Abs. 1 BDSG geforderten Freiwilligkeit. Es ist davon auszugehen, dass künftig Fahrzeugkäufe ohne Offenlegung der personenbezogenen Daten kaum mehr möglich sein werden und demnach ein faktischer Zwang, in die Übermittlung einzuwilligen, entsteht.

➡ Geschäftsmodelle, die den gewerblichen Handel mit Nutzungs- und Unfallhistorien von Gebrauchtwagen über die FIN ermöglichen, sind nach derzeitiger Rechtslage unzulässig. Auch in diesen Fällen werde ich weiterhin darauf achten, dass die Selbstbestimmung über die eigenen Daten erhalten bleibt.

5.5 Was dürfen Vermieterinnen und Vermieter fragen?

Für die Entscheidung, an wen Wohnraum vermietet wird, erheben Vermieterinnen und Vermieter teils umfänglich personenbezogene Daten von Mietinteressentinnen und Mietinteressenten, insbesondere um Zahlungsausfällen vorzubeugen.

Im Januar 2014 haben die Aufsichtsbehörden gemeinsam eine Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressenten" erstellt, die ein datenschutzgerechtes Vorgehen aufzeigt.

Bei der Einholung von Selbstauskünften durch Vermieterinnen und Vermieter handelt es sich um ein seit Jahren stets aktuelles Thema (siehe Bericht 2011 unter 5.2 und Bericht 2007 unter 7.6).

Einerseits haben Vermieterinnen und Vermieter ein Interesse daran, Zahlungsausfälle zu vermeiden und die Zuverlässigkeit potentieller Mieterinnen und Mieter abzuschätzen. Anderseits ist das Recht auf informationelle Selbstbestimmung der Mietinteressentin und des Mietinteressenten sowie etwaiger Personen, die mit diesem eine Wohnung beziehen wollen, zu wahren.

Sollen Auskünfte eingeholt werden, ist daher stets eine Abwägung dieser widerstreitenden Interessen vorzunehmen. Die genaue Grenzziehung bereitet im Alltag jedoch Probleme.

Die gemeinsame Orientierungshilfe der Datenschutzaufsichtsbehörden zeigt auf, welche personenbezogenen Daten je nach Stadium der Vertragsverhandlung (vorvertragliches Anbahnungsverhältnis bzw. konkreter Vertragsschluss) erhoben werden dürfen. Für die Praxis habe ich ein darauf aufbauendes Formular entwickelt. Orientierungshilfe und Formular finden Sie unter www.ldi.nrw.de.

➧ Mit der Orientierungshilfe geben die Datenschutzaufsichtsbehörden Vermieterinnen und Vermietern eine wichtige Praxishilfe an die Hand. Sie ermöglicht ein datenschutzgerechtes Einholen von Auskünften. Die Interessen der Vermieterinnen und Vermieter werden dabei ebenso berücksichtigt wie die Belange der Mieterinnen und Mieter. Die Interessenverbände sollten ihre Mitglieder auf die Orientierungshilfe aufmerksam machen, damit auf Unkenntnis beruhende Datenschutzverstöße bereits präventiv verhindert werden und ein aufsichtsbehördliches Einschreiten der Datenschutzaufsichtsbehörden nicht länger erforderlich ist.

5.6 Bargeld- und kontaktloses Bezahlen mit NFC-Technik – schneller, leichter, aber auch sicher?

Die Deutsche Kreditwirtschaft hat in den vergangenen zwei Jahren nach und nach die Möglichkeit entwickelt, mit Geldkarten, Girokarten und Kreditkarten Kleinbeträge zahlen zu können, ohne die Karte in ein Lesegerät einführen und eine PIN eingeben zu müssen. Dieses zunächst verbraucherfreundlich wirkende Verfahren stellt jedoch besondere Anforderungen an die Datensicherheit.

Mit der NFC-Technik (Near Field Communication) halten Geldkarten, Girokarten und Kreditkarten Einzug, die einen kontaktlosen Einsatz der Karten ermöglichen. Die Karten sind hierfür mit einem Funkchip ausgestattet. Die Daten, die für die Durchführung eines Bezahlvorgangs auf dem NFC-Chip gespeichert sind, können mittels eines Lesegeräts in einem Abstand von bis zu 10 cm ausgelesen werden. Die Karten aus der Hand zu geben ist somit nicht mehr nötig. Das Einführen in ein Lesegerät zum Auslesen der bislang auf Magnetstreifen oder herkömmlichen Chips gespeicherten Daten entfällt. Dadurch sollen Bezahlvorgänge, insbesondere bei Massengeschäften, beschleunigt werden.

Zur NFC-Technik bei Geldkarten habe ich bereits im September 2012 gemeinsam mit den anderen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich mehr Transparenz und Sicherheit gefordert (siehe Bericht 2013 Beschluss des Düsseldorfer Kreises "Near Field Communication (NFC) bei Geldkarten" vom 18./19. September 2012, Seite 156).

Die Deutsche Kreditwirtschaft und die Kreditkartenorganisationen legten daraufhin Datenschutzfolgeabschätzungen, auch Privacy Impact Assessments (PIA) genannt, vor. Hiermit werden Risiken, die mit neuen Verfahren und Technologien verbunden sind, beurteilt und Gegenmaßnahmen aufgezeigt. Nach Prüfung durch die Aufsichtsbehörden müssen folgende wesentliche Anforderungen erfüllt sein:

- Die Karten ausgebenden Institute stellen, zumindest auf Verlangen der Kundinnen und Kunden, eine Schutzhülle zur Verfügung, die das heimliche Auslesen des NFC-Chip – zum Beispiel mittels eines handelsüblichen Smartphones – verhin-

dert. Die Hülle sollte kostenfrei zur Verfügung gestellt werden.

- Sämtliche Kundinnen und Kunden werden über die Datenverarbeitungsprozesse und über die Möglichkeit, Schutzhüllen verlangen zu können, informiert.
- Die technische Möglichkeit, die NFC-Funktion auf Wunsch der Karteninhaberin und des Karteninhabers abzuschalten, müssen die Unternehmen schnellstmöglich umsetzen.
- Vorkehrungen der Karten ausgebenden Institute, die zu einem höheren Maß an Sicherheit führen (wie zum Beispiel Verschlüsselung der Kartennummer), sollen weiterentwickelt werden.

Aktuell befinden sich die Datenschutzaufsichtsbehörden mit der Deutschen Kreditwirtschaft in Beratungen, in welcher Weise die NFC-Funktion einer Geldkarte in Verbindung mit einer Smartphone-Bezahl-App genutzt werden kann.

➡ Schnelles Einkaufen ohne lange Warteschlangen an den Kassen ist für Verbraucherinnen und Verbraucher durchaus attraktiv. Es ist nicht nur wichtig, dass die Anforderungen erfüllt werden. Mir ist auch daran gelegen, dass die Kreditwirtschaft vor Einführung neuer Verfahren die erforderlichen Sicherungsmaßnahmen bereits in Gänze zur Verfügung stellt.

5.7 Vorsicht bei der Verwendung des Personalausweises

Gerne wird von verschiedensten Unternehmen wie Kreditinstituten, Versicherungen, Wirtschaftsauskunfteien oder Hotels eine Kopie des Personalausweises der Kundinnen und Kunden angefertigt und aufbewahrt. Da das Ausweisdokument jedoch zahlreiche personenbezogene Daten enthält, ist Vorsicht geboten. Grundsätzlich besteht keine Verpflichtung, eine Kopie des Personalausweises vorzulegen oder anderen zu überlassen oder den Personalausweis gar einscannen zu lassen.

Zahlreiche Anfragen von Bürgerinnen und Bürgern, ob und in welchem Umfang Unternehmen die Vorlage oder eine Kopie des Perso-

nalausweises verlangen können, etwa "Darf ein Hotel beim Einchecken den Personalausweis kopieren?" oder "Warum verlangt die Bank beim Abschluss eines Girovertrages den Personalausweis?", habe ich zum Anlass genommen, die wesentlichen Anforderungen in unseren Hinweisen "Personalausweis und Datenschutz" zusammenzufassen (abrufbar unter www.ldi.nrw.de).

Teilweise können sich Unternehmen auf eine gesetzliche Regelung stützen, wie Kredit- und Finanzdienstleistungsinstitute zum Beispiel auf das Geldwäschegesetz. Danach müssen die Institute unter anderem für die Begründung einer Geschäftsbeziehung ihre Vertragspartner identifizieren. Hierfür sind bei einer natürlichen Person folgende Angaben zu erheben und aufzuzeichnen:

- Vor- und Nachname
- Geburtsort
- Geburtsdatum
- Staatsangehörigkeit
- Anschrift
- die Art, die Nummer und die ausstellende Behörde des zur Überprüfung der Identität vorgelegten Dokuments (wie etwa des Personalausweises)

Die Wahlmöglichkeit, ob eine Kopie des Personalausweises gefertigt wird oder die erforderlichen Daten aus dem Ausweis notiert werden, liegt bei dem jeweiligen Institut. Allerdings können und sollen die Daten, die für die Identifizierung nicht erforderlich sind, geschwärzt werden.

In anderen Fällen mag das Vorzeigen des Ausweises zur Identifizierung der Person zwar erforderlich sein, jedoch nicht die Anfertigung einer Kopie oder das Einscannen. So haben zum Beispiel Veranstalter und Gewerbetreibende nach dem Jugendschutzgesetz nur in Zweifelsfällen das Alter einer Person zu überprüfen.

➧ Die Hinweise enthalten viele praxisnahe Beispiele und die strengen Voraussetzungen, unter denen Ausweiskopien in Einzelfällen erstellt werden können. Weitere Informationen zum Hinterlegungsverbot, zur Möglichkeit der Online-Identifizierung sowie zur grafischen Darstellung des Personalausweises runden die Hinweise ab.

5.8 Verarbeitung von Daten für Werbezwecke einschließlich Adresshandel

Nach wie vor gehen Beschwerden und Eingaben wegen der Verarbeitung von Daten für Werbezwecke in hoher Zahl bei mir ein. Das Bundesdatenschutzgesetz (BDSG) verlangt zwar grundsätzlich eine Einwilligung für die Nutzung von Daten für Werbung und Adresshandel. Von dieser Regel gibt es aber viele Ausnahmen, die in erheblichem Umfang Fragen zur Gesetzesanwendung aufwerfen und Veranlassung zu verschiedenen Interpretationen geben. Der Bundesgesetzgeber hat es leider versäumt, für klare und verständliche Regelungen zu sorgen.

Daher habe ich gemeinsam mit den Aufsichtsbehörden des Bundes und der Länder in einer Arbeitsgruppe des Düsseldorfer Kreises Anwendungshinweise für die Auslegung erarbeitet. Unternehmen sowie Bürgerinnen und Bürger erhalten somit eine Übersicht über das bundesweit einheitliche Verständnis der Aufsichtsbehörden.

Über die Homepage können die Anwendungshinweise abgerufen werden (www.ldi.nrw.de).

- Telefonwerbung

Immer noch richten sich Beschwerden in hoher Zahl gegen Telefonwerbung (siehe Bericht 2013 unter 5.3).

Adresshändler und Werbetreibende müssen bereits im Zeitpunkt des Ankaufs bzw. der Erhebung von personenbezogenen Daten die Zwecke konkret festlegen, für die diese Daten später verarbeitet bzw. genutzt werden sollen. Sollen Telefonnummern für Werbeanrufe genutzt werden, bedeutet dies, dass bereits in diesem frühen Stadium eine ausdrückliche Einwilligung der Betroffenen in die Verarbeitung und Nutzung ihrer Daten zu Werbezwecken vorliegen muss. Für den Adresshandel sieht § 29 BDSG eine eigene Rechtsgrundlage vor. Zulässig ist danach auch das geschäftsmäßige Erheben, Speichern und Nutzen von Daten zum Zwecke der Übermittlung, die aus allgemein zugänglichen Quellen, wie zum Beispiel Telefonbüchern, entnommen werden können. Allerdings ist zu prüfen, ob ein schutzwürdiges, offensichtlich überwiegendes Interesse der Betroffenen diesem

geschäftsmäßigen Handeln entgegensteht. Das ist bei Telefonwerbung der Fall.

So erwarb ein Adresshändler geschäftsmäßig personenbezogene Daten, wie Namen, Adressen und die Zugehörigkeit zu einer Gruppe (Alter, Beruf, Kunde oder Versicherungsnehmer bei einem Unternehmen, etc.), um diese an Dritte, insbesondere zum Zwecke der Werbung oder des Adresshandels, zu übermitteln. Der Adresshändler vertrat die unzutreffende Auffassung, nicht er müsse sich mit der Frage befassen, ob die Betroffenen ein sogenanntes Opt-In in die werbliche Ansprache per Telefon erteilt hätten, sondern die jeweilige Käuferin oder der jeweilige Käufer der Datensätze.

Dem Adresshändler musste ich im Wege einer Anordnung nach § 38 Abs. 5 BDSG auferlegen, zukünftig beweiskräftige Nachweise über Einwilligungserklärungen vorzuhalten und mir auf Verlangen vorzulegen. Für den Fall der Zuwiderhandlung habe ich ein Zwangsgeld angedroht. Ebenso wurde in dem Fall eines Werbetreibenden verfahren, der gleichfalls keine Opt-In Erklärungen von Betroffenen nachweisen konnte. Beide Anordnungen sind bestandskräftig.

Vergleichbare Anforderungen gelten auch für Telefonwerbung durch Organisationen, die für Spenden werben. Das BDSG sieht für die Nutzung von personenbezogenen Grunddaten, wie Namen, Adresse, Berufsbezeichnung oder Zugehörigkeit zu einer Personengruppe (zum Beispiel Spender der Aktion XY, Tierschützer), für Zwecke der Spendenwerbung in § 28 Abs. 3 Satz 2 Nr. 3 BDSG eine eigene Zulässigkeitsregelung vor. Voraussetzung ist, dass es sich um gemeinnützige und damit steuerbegünstigte Zwecke handelt.

Die Nutzung von Telefondaten für Spendenanrufe ist hingegen nicht privilegiert, sondern nur mit ausdrücklicher Einwilligung der Spenderin oder des Spenders zulässig. Daran ändert auch der häufige Einwand von Spendenorganisationen nichts, ihr Handeln sei nicht "gewerblich".

- Widerspruchsrecht

Des Weiteren können Betroffene der Verarbeitung und Nutzung ihrer Daten zu Werbezwecken sowie zu Zwecken der Markt- und Meinungsforschung widersprechen. Werbetreibende sind gemäß § 28 Abs. 4 Satz 2 BDSG verpflichtet, in ihren Werbeschreiben über das

Widerspruchsrecht und die verantwortliche Stelle zu unterrichten, die die Daten erhoben und verarbeitet hat. In einem Fall, in dem es mehrfach zu Verstößen gekommen ist, musste ich ein Unternehmen mit einer Anordnung und Androhung bzw. Festsetzung eines Zwangsgelds für jede Zuwiderhandlung belegen. Seitdem ist das Unternehmen nicht mehr durch solche Verstöße aufgefallen.

- Sanktionen durch weitere Stellen

Auch die Justiz nimmt Verstöße gegen das BDSG ins Visier. In einem Fall, in dem ein Adresshändler in hoher Zahl Datensätze einer Personengruppe mit Angaben über Namen, Anschriften und Bankkontodaten unbefugt verarbeitet hatte, kam es auf Antrag der Staatsanwaltschaft zu einem Strafbefehl mit einer empfindlichen Geldstrafe.

➡ Vor dem Hintergrund der äußerst kompliziert gestalteten Vorschriften im BDSG kommt den Bemühungen der Aufsichtsbehörden um Klarheit große Bedeutung zu.

➡ Die Anwendungshinweise mögen den Unternehmen verdeutlichen, dass nunmehr auch bundesweit die Aufsichtsbehörden von einem einheitlich hohen Datenschutzniveau ausgehen. Ich begrüße, dass ebenso mit strafrechtlichen Sanktionen eine generalpräventive Wirkung im Sinne einer Stärkung des Rechts auf informationelle Selbstbestimmung erzielt werden kann. Meine Behörde wird Werbetreibende weiterhin mit Nachdruck dazu anhalten, ihren Verpflichtungen nachzukommen.

➡ Zu meinem Bedauern muss ich allerdings feststellen, dass die zur Zeit diskutierten Entwürfe zur Europäischen Datenschutz-Grundverordnung dem Einwilligungsprinzip bei der Verarbeitung von Daten zu Werbezwecken eine Abfuhr erteilen, indem den Betroffenen lediglich ein Widerspruchsrecht zugestanden werden soll. Gerade die Verarbeitung von personenbezogenen Daten zu Werbezwecken macht die Betroffenen zu Objekten von Konsumentenprofilen (siehe hierzu unter 3.5).

5.9 Kundendaten sind kein Einstandsgeschenk für den neuen Arbeitgeber

Ein Mitarbeiter eines Sanitätshauses nahm bei einem Wechsel seines Arbeitgebers ohne dessen Wissen etwa 200 Adressdaten nebst Telefonnummern der vormals von ihm betreuten Kundinnen und Kunden mit. Er warb unter dem Kopfbogen des neuen Arbeitgebers damit, seine Beratungstätigkeit fortzusetzen.

Bei den Adressdaten handelt es sich um besonders schützenswerte Gesundheitsdaten, für deren Übermittlung die engen Voraussetzungen des § 28 Abs. 6 bis 9 BDSG gelten. Eine Datenübermittlung ist danach unter anderem nur zulässig, soweit die betroffene Person eingewilligt hat. Da eine Einwilligung erkennbar nicht eingeholt worden war, handelte es sich bei der Mitnahme der Kundendaten um eine unbefugte Datenverarbeitung. Dem Geschäftsführer der neuen Firma war das Handeln des Mitarbeiters nach § 30 Ordnungswidrigkeitengesetz zuzurechnen. Deshalb wurden sowohl gegen den Mitarbeiter als auch gegen den neuen Arbeitgeber Ordnungswidrigkeitenverfahren eingeleitet, die mit der Verhängung von Bußgeldern endeten.

➧ Die Mitnahme von Kundendaten beim Arbeitgeberwechsel ist kein "Kavaliersdelikt".

5.10 Mithören von Telefongesprächen in Call-Centern und bei Markt- und Meinungsumfragen

"Zu Trainingszwecken können einzelne Gespräche mitgehört oder aufgezeichnet werden." Fast jeder, der mit einem Call-Center telefoniert, kennt diesen Satz. Ist dies auch mit dem Datenschutz vereinbar?

Während das unbefugte Aufzeichnen von Telefonaten gemäß § 201 Abs. 1 Strafgesetzbuch wegen der Verletzung der Vertraulichkeit des Wortes eine Straftat ist, besteht eine Strafbarkeit bei einem unbefugten Mithören von Telefonaten nur, wenn es sich um ein Abhören mittels einer verbotenen technischen Einrichtung (etwa Richtmikrofon, Minispione) handelt. Herkömmliche Telefonapparate fallen nicht hierunter.

Mitunter halten Call-Center sowie Markt- und Meinungsforschungsinstitute in Bezug auf das Mithören von Telefongesprächen eine vorherige Information an ihre Beschäftigten und die ausdrückliche Einwilligung der Gesprächsteilnehmerinnen und -teilnehmer für entbehrlich. Zum Teil beruft man sich auf sogenannte berufsständische Verhaltensregeln. Danach sollen Beschäftigte nur zu Beginn ihrer Tätigkeit über das Mithören informiert werden, um die Telefonate unbefangen zu führen. Die Befragten, so die Argumentation, hätten bereits durch ihre Einwilligung in das Interview zu erkennen gegeben, dass sie mit der Auswertung ihrer Angaben einverstanden seien.

In meinen Stellungnahmen und Empfehlungen weise ich regelmäßig darauf hin, dass das Bewusstsein über das jederzeitige Mithören der geführten Telefonate bei den Beschäftigten einen permanenten Kontrolldruck erzeugen kann. Dieser stellt – auch nach der Rechtsprechung des Bundesarbeitsgerichts – stets eine Verletzung des allgemeinen Persönlichkeitsrechts der Beschäftigten dar. Im Hinblick auf die Gesprächsteilnehmerinnen und -teilnehmer ist außer einer Einwilligung eine Rechtsgrundlage nicht gegeben, die ein heimliches Mithören solcher Telefongespräche erlaubt.

- Sowohl im Telefonmarketing als auch bei telefonischen Befragungen durch Markt- und Meinungsforschungsinstitute bedarf es der ausdrücklichen Einwilligung der externen Gesprächsteilnehmerinnen und Gesprächsteilnehmer in das Mithören von Telefongesprächen vor ihrer Aufzeichnung. Beschäftigte sind einige Tage vor dem Mithören auf Beginn und Dauer hinzuweisen, um einen permanenten Kontrolldruck zu vermeiden.

5.11 Insolvenzbekanntmachungen im Internet durch Private

Durch mehrere Eingaben bin ich darauf aufmerksam gemacht worden, dass auch private Anbieter auf ihren Homepages unter Verwendung der Bekanntmachungen der Insolvenzgerichte über Insolvenz-Eröffnungen informieren. Mit Hilfe des Namens, Sitzes, des Eröffnungsdatums oder Aktenzeichens kann herausgefunden werden, ob gegen eine Person (oder Firma) ein Insolvenzverfahren eröffnet wurde. Dies ist nur unter bestimmten Bedingungen zulässig.

Als Rechtsgrundlage für die Datenverarbeitung kommt § 29 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) in Betracht. Danach ist das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte. Es sei denn, das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung überwiegt offensichtlich.

Nach § 9 Abs. 1 Insolvenzordnung (InsO) sind Insolvenzverfahren durch die Amtsgerichte als Insolvenzgerichte öffentlich bekannt zu machen. Dies erfolgt über die von der Justiz betriebene Homepage www.insolvenzbekanntmachungen.de. Demnach handelt es sich bei dieser um eine allgemein zugängliche Quelle im Sinne des § 29 Abs. 1 Satz 2 BDSG. Darüber hinaus ist weder der InsO noch der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (InsoBekV) zu entnehmen, dass Bekanntmachungen über Insolvenzverfahren ausschließlich über Amtsgerichte als Insolvenzgerichte erfolgen dürfen.

Auch ein offensichtlich überwiegendes schutzwürdiges Interesse des Betroffenen ist zunächst nicht zu erkennen. Durch die verpflichtende öffentliche Bekanntmachung soll die Allgemeinheit darüber in Kenntnis gesetzt werden, dass das Insolvenzverfahren über den Betroffenen eröffnet wurde. Die öffentliche Bekanntmachung hat die Aufgabe, der Entscheidung nach außen hin Geltung zu verschaffen und die Publizitätswirkung auch gegenüber solchen Personen eintreten zu lassen, an die eine Einzelzustellung nicht möglich ist. Sie entfaltet zudem eine Signalwirkung gegenüber potentiellen Geschäftspartnern des Betroffenen. Daher ist eine Veröffentlichung von Insolvenzbekanntmachungen durch private Dritte aufgrund des § 29 Abs. 1 Satz 2 BDSG grundsätzlich möglich.

Die Ausgestaltung der Veröffentlichung durch private Dritte begegnet allerdings datenschutzrechtlichen Bedenken. Die Veröffentlichung auf privaten Homepages darf nicht über die öffentliche Bekanntmachung durch die Insolvenzgerichte hinausgehen. Es ist sicherzustellen, dass die Veröffentlichungen vollständig und aktuell bleiben sowie jederzeit ihrem Ursprung nach zugeordnet werden können. Darüber hinaus darf die Veröffentlichung nur die personenbezogenen Daten enthal-

ten, die nach der InsO oder nach anderen Gesetzen, die eine öffentliche Bekanntmachung in Insolvenzverfahren vorsehen, bekannt zu machen sind. Da die Insolvenzbekanntmachungen selbst nur innerhalb der ersten zwei Wochen sowie täglich aktualisiert auf der Homepage www.insolvenzbekanntmachungen.de abrufbar sind, dürfen die Daten auch auf privaten Homepages nur für den Zeitraum von zwei Wochen nach dem ersten Tag der Veröffentlichung abrufbar sein. Danach sind die Daten zu löschen. Darüber hinaus dürfen die Daten nicht ungeschützt im Internet bereitgestellt werden, insbesondere sind sie sicher vor Suchmaschinen einzustellen sowie ständig zu aktualisieren.

- Private Anbieter dürfen Insolvenzdaten nur in engen Grenzen und unter Beachtung der genannten Anforderungen veröffentlichen. Überhaupt stellt sich die Frage nach dem Bedarf für Veröffentlichungen durch Private, wenn bereits ein amtliches Informationsangebot besteht.

6 Videoüberwachung

6.1 "Sehen und gesehen werden"…

…lautet nicht nur das altbekannte Motto auf der Düsseldorfer Königsallee, sondern heißt es auch überall dort, wo Videokameras zu Überwachungszwecken eingesetzt werden: Während die einen mittels Kamera ihre Mitmenschen beobachten und/oder die Bilder aufzeichnen, sehen sich die anderen dieser Überwachung unweigerlich ausgesetzt. Jetzt gibt es unter diesem Titel eine neue Orientierungshilfe meiner Behörde zum Thema Videoüberwachung.

Der Einsatz von Überwachungskameras durch Privatpersonen und private Unternehmen nimmt stetig zu: In großen Geschäften, in Banken, an Tankstellen und im Bereich des Öffentlichen Personennahverkehrs haben wir uns schon fast an den Anblick gewöhnt. Plötzlich haben aber nicht nur der Supermarkt und die Sparkasse, sondern auch die kleine Bäckerei an der Ecke und der Kiosk nebenan den Einsatz von Videotechnik für sich entdeckt. Damit aber noch lange nicht genug: Spitzenreiter unter allen Eingaben und Anfragen, die mich zum Thema Videoüberwachung erreichen, ist mit weitem Ab-

stand der Wohnbereich und dabei insbesondere Nachbarschaftsstreitigkeiten, die immer häufiger in einer gegenseitigen Videoüberwachung eskalieren. Auch im Übrigen unterliegt der Freizeitbereich, der typischerweise der Erholung und Entspannung dienen sollte, schon längst keinem generellen Überwachungstabu mehr: Sowohl im gehobenen Restaurant als auch in einem Schnellimbiss und sogar im Wald sind gelegentlich Videokameras installiert. In Schwimmbädern, Saunen und Fitnessstudios ist es für die meisten Menschen besonders unangenehm, sich leicht oder gar nicht bekleidet einer Videoüberwachung ausgesetzt zu sehen; trotzdem hat auch hier die Videotechnik Einzug gehalten. Und dies sind nur einige von vielen Beispielen. Betroffen sind – je nach Sphäre der Überwachung – Kundinnen und Kunden ebenso wie vor allem auch Beschäftigte, die sich der Videoüberwachung oftmals gar nicht entziehen können, im Wohnumfeld insbesondere Bewohnerinnen und Bewohner, nicht selten aber auch unbeteiligte Dritte, die sich auf Gehwegen, öffentlichen Plätzen oder Straßen aufhalten.

Dabei hat jeder Mensch grundsätzlich das Recht, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung zu werden (siehe auch Bericht 2013 unter 6.1). Dieses (Grund-)Recht ist, wenn es in die eine Schale einer Waage gelegt wird, von besonderem Gewicht. In der anderen Waagschale sind – je nach Einzelfall – andere geschützte Rechtsgüter und -positionen zu berücksichtigen, von denen vor allem das Leben, die körperliche Unversehrtheit, das Eigentumsrecht bzw. das Recht am eingerichteten und ausgeübten Gewerbebetrieb sowie die Berufsausübungsfreiheit besonders schwer wiegen. Ein differenziertes Austarieren der Waage verspricht nur dann Erfolg, wenn weitere Kriterien (wie zum Beispiel Zweck, Erforderlichkeit und Verhältnismäßigkeit der in Rede stehenden Videoüberwachung) berücksichtigt werden. Diesem Ziel, einen angemessenen Ausgleich zwischen den unterschiedlichen Interessen der verantwortlichen sowie der betroffenen Personen zu gewährleisten, dient die Regelung des § 6b Bundesdatenschutzgesetz.

Doch die Rechtsvorschrift ist das eine, ihre Anwendung und Umsetzung in der Praxis dagegen etwas ganz anderes. Meiner Erfahrung nach sind die Voraussetzungen und Grenzen, unter bzw. in denen eine Videoüberwachung durch Privatpersonen und private Unterneh-

men zulässig ist, noch vielfach unbekannt. Manchmal fehlt überdies sogar das Bewusstsein, mit einer Videoüberwachung in die Rechte anderer Menschen einzugreifen.

Deshalb habe ich nunmehr die Orientierungshilfe "Sehen und gesehen werden – Videoüberwachung durch Private in NRW" herausgegeben, die kostenlos in der Druckfassung bestellt oder unter www.ldi.nrw.de abgerufen werden kann. Auf über 100 Seiten werden die gesetzlichen Voraussetzungen und Anforderungen anhand von vielen praktischen Fallbeispielen erläutert. Ziel der Broschüre ist es, den für die Videoüberwachung Verantwortlichen konkrete Hinweise für ihre eigenverantwortliche Prüfung zu geben. Zugleich wird der Rahmen umschrieben, in dem Betroffene eine Videoüberwachung hinnehmen müssen und außerhalb dessen sie sich wehren können. Leider kann ich nicht allen Beschwerden und Beratungsersuchen im Detail nachgehen. Umso wichtiger ist es, die Sensibilität der verantwortlichen Personen hinsichtlich des datenschutzgerechten Einsatzes von Videotechnik zu erhöhen und das Bewusstsein ihrer Eigenverantwortung zu stärken. Hierzu soll die neue Orientierungshilfe beitragen.

Um eine flächenbrandähnliche Verbreitung unzulässiger Kameras zu verhindern, setzen darüber hinaus die Datenschutzaufsichtsbehörden in Deutschland ihre Bestrebungen fort, sich bundesweit zu einzelnen Aspekten der Videoüberwachung abzustimmen. Neue Themen erfordern dabei rasches Handeln. So fasste der Düsseldorfer Kreis als Reaktion auf die in jüngster Zeit zunehmend diskutierte Frage, ob mit in Kraftfahrzeugen installierten Kameras der öffentliche Verkehrsbereich erfasst und aufgezeichnet werden darf, am 25./26. Februar 2014 den Beschluss "Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)". Inzwischen sind bereits erste Gerichtsentscheidungen im Sinne dieses Beschlusses ergangen. Schon ein Jahr zuvor hatte das Gremium am 26./27. Februar 2013 – ebenfalls aus aktuellem Anlass – den Beschluss "Videoüberwachung in und an Taxis" gefasst. Beide Beschlüsse sind im Anhang abgedruckt. Wegen der anhaltend großen Bedeutung der Fragen rund um den Einsatz von Videotechnik wurde zudem die ursprüngliche "Ad-hoc-AG Videoüberwachung" inzwischen zu einer ständigen "Arbeitsgemeinschaft" des Düsseldorfer Kreises.

➧ Dem ausufernden und unzulässigen Einsatz von Videotechnik muss wirksam begegnet werden. Dieses Ziel lässt sich nur dann erreichen, wenn sich die Personen und Stellen, die diese Technik nutzen, ihrer Verantwortung bewusst sind und dieser umfassend Rechnung tragen. Meine Orientierungshilfe soll hierzu einen Beitrag leisten.

6.2 Keine Videoüberwachung öffentlicher Plätze durch Kommunen

Kommunen haben keine Befugnis, ihre Wege, Straßen und öffentlichen Plätze mittels Videokameras zu überwachen.

Städte und Gemeinden sind häufig mit Beschädigungen ihres Eigentums (etwa durch Graffitis) konfrontiert. Zur Verhinderung und Aufklärung solcher Vorkommnisse plante eine Stadt, ihre öffentlichen Plätze mit Videokameras zu überwachen. Das Datenschutzgesetz NRW (DSG NRW) enthält jedoch aus gutem Grunde keine Vorschrift, die Kommunen eine solche Überwachung erlaubt.

Nach § 29b DSG NRW kann die Überwachung öffentlich zugänglicher Bereiche mit so genannten optisch-elektronischen Einrichtungen nur auf den Zweck der Wahrnehmung des Hausrechts gestützt werden. Auch wenn in dieser Vorschrift nicht von "Räumen", sondern allgemein von öffentlich zugänglichen "Bereichen" die Rede ist, muss es sich hierbei um ein hausrechtsfähiges "befriedetes Besitztum" handeln. Ein solches liegt vor, wenn Grundstücke von Berechtigten in äußerlich erkennbarer Weise mittels zusammenhängender Schutzwehren gegen das beliebige Betreten durch andere gesichert sind. Eine Videoüberwachung kann – bei Erfüllung weiterer Voraussetzungen – beispielsweise den für den Publikumsverkehr zugänglichen Parkplatz einer Behörde betreffen. Die an ein Dienstgebäude angrenzenden öffentlichen Verkehrsflächen dürfen jedoch grundsätzlich nicht erfasst werden, da sie nicht zum befriedeten Besitztum zählen. Nur wenn es für den Überwachungszweck lage- oder situationsbedingt unvermeidbar ist, diese Verkehrsflächen mit in die Überwachung einzubeziehen, kann dies im Ausnahmefall gerechtfertigt sein (etwa zum Schutz der Fassade eines Dienstgebäudes vor Sachbeschädigungen). In diesem Fall ist jedoch der Erfassungsbereich der

Kameras auf das zwingend erforderliche Maß (Erfassung maximal eines Meters des öffentlichen Verkehrsraums) zu beschränken.

Eine räumlich darüber hinausgehende Videoüberwachung von öffentlichen Wegen, Straßen und Plätzen durch öffentliche Stellen des Landes NRW kann hingegen nicht auf § 29b DSG NRW gestützt werden. Zum einen unterliegen diese Flächen – wie bereits ausgeführt – gar nicht dem Hausrecht der Kommune. Zum anderen würden durch eine Videoüberwachung dieser Bereiche, die gerade auch zur Entfaltung sozialer Kommunikation dienen, zahlreiche Bürgerinnen und Bürger in den Wirkungsbereich einer solchen Maßnahme einbezogen und damit unter einen Generalverdacht gestellt, obwohl sie in keiner Beziehung zu einem etwaigen Fehlverhalten Einzelner stehen.

➧ Es muss auch weiterhin sichergestellt bleiben, dass sich Bürgerinnen und Bürger im öffentlichen Raum frei und ungezwungen bewegen können, ohne befürchten zu müssen, zum Gegenstand einer behördlichen Videoüberwachung gemacht zu werden.

6.3 Videoüberwachung in Fußballstadien

Auch wenn die meisten Sportveranstaltungen friedlich ablaufen, kommt es in Einzelfällen immer wieder zu teilweise sehr gewalttätigen Auseinandersetzungen zwischen den so genannten Fans. Deshalb werden seit längerem in großen Stadien Videokameras eingesetzt, um Besucherinnen und Besucher zu schützen und die Stadien vor Beschädigungen zu bewahren.

Bei sportlichen Großveranstaltungen kann es nachvollziehbare Gründe für den Einsatz von Videoüberwachungsanlagen in den Veranstaltungsstätten geben. Die Videoüberwachung wird dort von Veranstalterinnen und Veranstaltern sowohl zur Beobachtung und Steuerung der Besuchermassen (so genanntes Crowd-Management) als auch zur Verhinderung und Aufklärung von konkreten Hausrechtsverstößen einzelner Personen eingesetzt. Parallel dazu nutzt häufig die Polizei diese Anlagen zum Zwecke der Gefahrenabwehr. Um hier zu datenschutzgerechten Lösungen zu kommen, müssen die Verantwortlichkeiten der handelnden Stellen klar voneinander abgegrenzt und

die Maßnahmen nach den jeweils für sie geltenden Befugnisnormen ausgestaltet werden.

Die Veranstalterinnen und Veranstalter als private Stellen können die Videoüberwachung gemäß § 6b Bundesdatenschutzgesetz auf die Wahrnehmung des Hausrechts oder ihrer berechtigten Interessen stützen. Dabei müssen allerdings neben dem Kriterium der Erforderlichkeit der Videoüberwachung insbesondere auch die schutzwürdigen Interessen der betroffenen Personen angemessen berücksichtigt werden.

Es ist somit stets zu prüfen, ob reine Übersichtsaufnahmen ohne Personenbezug zur Erreichung des Überwachungszwecks (zum Beispiel zum reinen Crowd-Management) genügen. Soweit dies der Fall ist, muss mangels Erforderlichkeit auf eine personenscharfe Videobeobachtung verzichtet werden.

Im Rahmen der vorzunehmenden Interessenabwägung ist vor allem zu berücksichtigen, dass die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung der Betroffenen in den Lebensbereichen besonders hoch ist, in denen die freie Entfaltung der Persönlichkeit im Vordergrund steht. Dies ist insbesondere bei Fußballspielen, Konzerten etc. der Fall. Eine anlasslose Videoüberwachung, die ohne einen konkreten Verdacht auf einen Rechtsverstoß eine Vielzahl von unbescholtenen Personen erfasst, weist eine stärkere Eingriffsintensität auf als eine Überwachung, die erst im Bedarfsfall aktiviert wird.

Auch aus diesem Grund sind Veranstalterinnen und Veranstalter grundsätzlich allenfalls dazu befugt, Übersichtsaufnahmen in den Stadien zu erstellen. Sofern sich jedoch bei Veranstaltungen konkrete Anhaltspunkte für erhebliche Hausrechtsverstöße ergeben, können anlassbezogen durch den Einsatz der Zoomfunktion personenscharfe Aufnahmen gefertigt und gespeichert werden.

Neben der Veranstalterin oder dem Veranstalter nutzt aber häufig auch die Polizei die installierten Videoüberwachungsanlagen. Sie kann selbständig auf die auf den Monitoren angezeigten Bilder zugreifen und bei Bedarf die Erfassungsbereiche der Kameras durch die Betätigung der Zoomfunktion beeinflussen. In diesen Fällen ist auch die Polizei als datenschutzrechtlich verantwortliche Stelle tätig und benö-

tigt für die Videoüberwachung eine eigene bereichsspezifische Befugnisnorm.

Nach § 15 Polizeigesetz NRW kann sie bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, personenbezogene Daten auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmenden erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten oder Ordnungswidrigkeiten begangen werden.

Somit darf auch die Polizei bei Veranstaltungen in Stadien im Regelfall nur Übersichtsaufnahmen einsehen. Soweit sich allerdings im Verlauf einer Veranstaltung konkrete Anhaltspunkte für Rechtsverstöße ergeben, darf sie anlassbezogen personenscharfe Aufnahmen anfertigen.

Als verantwortliche Stellen haben sowohl die Veranstalterinnen und Veranstalter als auch die Polizei gemäß der für sie jeweils geltenden Rechtsvorschriften aufeinander abgestimmte Datenschutzkonzepte für ihre Videoüberwachungsmaßnahmen zu erstellen.

➧ Eine Videoüberwachung in Fußballstadien lässt sich bei Beachtung der Verantwortlichkeiten der handelnden Stellen und unter angemessener Berücksichtigung der schutzwürdigen Interessen der davon betroffenen Personen datenschutzgerecht ausgestalten.

6.4 Kennzeichenerfassungssysteme im Bereich von Parkflächen

In Parkhäusern und auf Parkplätzen werden zunehmend Kennzeichenerkennungssysteme eingesetzt. Kann es aber zulässig sein, zum Zweck des Parkraum-Managements die Kennzeichen aller dort parkenden Fahrzeuge zu erfassen und zu speichern?

Im Bereich der Parkraumbewirtschaftung durch private Stellen halten zunehmend Kennzeichenerfassungssysteme Einzug. Bei diesen Systemen erfasst eine Kamera das Kennzeichen eines jeden einfahrenden Fahrzeugs. Bei so genannten Kurzzeitparkenden verknüpft und

speichert eine Systemsoftware die Bilddatei des Kennzeichens, die Einfahrtszeit und die ausgegebene Ticketnummer zu einem Datensatz über den Parkvorgang. Bei der Ausfahrt eines Fahrzeugs erfolgt dann ein Abgleich mit dem hinterlegten Kennzeichen. Durch dieses Verfahren soll insbesondere verhindert werden, dass sich Kundinnen und Kunden betrügerisch die Zahlung eines geringen Parkentgelts in der Weise erschleichen, dass sie ihr Fahrzeug für einen langen Zeitraum abstellen, später aber behaupten, sie hätten ihr Parkticket verloren und so nur das geringere Entgelt für die Ausstellung eines Ersatztickets zahlen. Bei Kundinnen und Kunden, die Dauerpark-Verträge haben (so genannte Dauerparkende) soll durch die Kennzeichenerfassung insbesondere die Zufahrtsberechtigung ohne das Mitführen einer Parkkarte ermöglicht werden.

Kfz-Kennzeichen sind personenbezogene Daten (vgl. hierzu auch § 45 Satz 2 Straßenverkehrsgesetz). Die Erhebung, Verarbeitung und Nutzung dieser Daten ist daher gemäß § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Da es sich bei Kfz-Kennzeichen um halterbezogene Daten handelt, müsste die Einwilligung durch die jeweiligen Kraftfahrzeughalterinnen bzw. -halter abgegeben werden. Häufig ist jedoch die fahrzeugführende Person nicht mit der Halterin bzw. dem Halter des Kraftfahrzeugs identisch, so dass dann bereits aus diesem Grund von den Kurzzeitparkenden keine wirksame Einwilligung bei der Einfahrt in den Parkbereich abgegeben werden kann. Im Übrigen genügt der teilweise im Einfahrtsbereich anzutreffende Hinweis auf die Kennzeichenerfassung durch ein Schild mit der Aufschrift "Videoüberwachung", "Kennzeichenerfassung" oder die Abbildung eines Kamerasymbols der nach § 4a Absatz 1 BDSG erforderlichen Informationspflicht der verantwortlichen Stelle nicht. Durch diese Maßnahmen erhalten die Betroffenen nämlich nicht alle Informationen, die notwendig sind, um Anlass, Ziel und Folgen der Datenverarbeitung abschätzen zu können.

Bei Dauerparkenden kann allerdings eine Einwilligungslösung im Rahmen des jeweiligen Vertragsverhältnisses in Betracht kommen. Die Betreiberinnen und Betreiber der Parkflächen können mit den Fahrzeughalterinnen und -haltern unter Beachtung der Voraussetzungen des § 4a BDSG vertraglich vereinbaren, dass die Kennzei-

chenerfassung zum Zwecke der Zufahrtskontrolle und ggf. auch zur Abrechnung des Parkentgelts erfolgt. Insbesondere die umfassende Informationspflicht sowie das Schriftformerfordernis können so gewahrt werden. Um eine "freie Entscheidung" der Fahrzeughalterinnen und -haltern zu ermöglichen, müssten neben der Kennzeichenerfassung jedoch auch alternative Möglichkeiten zur Zufahrtskontrolle und Abrechnung des Parkentgelts angeboten werden.

Dagegen kann eine Kennzeichenerfassung mit optisch-elektronischen Einrichtungen bei Kurzzeitparkenden nur unter den Voraussetzungen des § 6b BDSG in Betracht kommen.

Parkentgelt einnehmen zu können stellt ein berechtigtes wirtschaftliches Interesse der parkraumbewirtschaftenden privaten Stellen dar.

Eine Kennzeichenerfassung müsste zu diesem Zweck allerdings auch "erforderlich" sein. Dies kann nur dann der Fall sein, wenn belegbare Vorkommnisse in der Vergangenheit die Annahme rechtfertigen, dass auch künftig schwerwiegende Beeinträchtigungen der geschützten Interessen drohen. Betreiberinnen und Betreiber von Parkflächen bzw. Parkhäusern haben daher vor dem Einsatz von Kennzeichenerfassungssystemen zunächst betriebswirtschaftlich zu ermitteln und darzulegen, ob bzw. in welcher Höhe in der Vergangenheit Einnahmeverluste durch das Erschleichen von Parkentgelten eingetreten sind. Falls derartige Schäden festgestellt werden, müssen diese im Verhältnis zum jeweiligen Gesamtumsatz eine nicht nur unerhebliche Höhe aufweisen.

Die Erforderlichkeit des Einsatzes dieser Systeme kann zudem nur dann bejaht werden, wenn es kein anderes gleich wirksames Mittel gibt, das weniger stark in das Recht auf informationelle Selbstbestimmung der Fahrzeughalterinnen und -haltern eingreift. In diesem Sinne könnte etwa die deutliche Erhöhung des Entgelts für die Ausstellung eines Ersatztickets als geeignete Maßnahme in Betracht kommen, diesen Zweck ebenfalls wirksam zu erreichen. Ein Entgelt, das sich an der jeweiligen durchschnittlichen Parkdauer und der Stunden- bzw. Tagessatzhöhe orientiert, könnte den finanziellen Anreiz ausschließen bzw. mindern, sich durch die Ausstellung eines (kostengünstigen) Ersatztickets die Dienstleistung für ein (kostenintensives) Parken über einen längeren Zeitraum zu erschleichen.

Sofern in begründbaren Einzelfällen die Verwendung eines Kennzeichenerkennungssystems als ultima ratio zur Sicherung der Einnahmen in Erwägung gezogen werden kann, müssen bei der Ausgestaltung der Maßnahme die schutzwürdigen Interessen der betroffenen Kraftfahrzeughalterinnen und -halter angemessen berücksichtigt werden. Um den Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen möglichst gering zu halten, müssten die Kennzeichendaten daher in diesen Fällen sofort nach der Entrichtung des Parkentgelts und dem Verlassen der jeweiligen Parkfläche gelöscht werden.

- Der Betrieb von Kennzeichenerfassungssystemen als Teil des Parkraum-Managements kann – bezogen auf Kurzzeitparkende – nur dann in Betracht kommen, wenn zuvor alle Maßnahmen zur Sicherung der Einnahmen erfolglos ausgeschöpft worden sind, die weniger in das Recht auf informationelle Selbstbestimmung der Fahrzeughalterinnen und -halter eingreifen.

6.5 Einzelfälle der Videoüberwachung in Handel und Gewerbe

Im Berichtszeitraum wurden weiterhin zahlreiche unzulässige Videoüberwachungen von Beschäftigten durch Arbeitgeber im Handel und im Gewerbe festgestellt. Häufig kommen die verantwortlich handelnden Personen in den Unternehmen dabei fahrlässig ihrer Pflicht nicht oder nicht ausreichend nach, sich rechtzeitig über die gesetzlichen Anforderungen zu informieren, die an eine zulässige Videoüberwachung geknüpft sind. Vielfach fehlt beim Einsatz von Videokameras auch die notwendige Sensibilität und das Augenmaß, weil der Schutz eigener Geschäftsinteressen in der Regel einseitig zu Lasten der durch eine Videoüberwachung beeinträchtigten Persönlichkeitsrechte von Beschäftigten an ihrem Arbeitsplatz höher bewertet wird.

Dass es auch anders geht, zeigen Gespräche mit einem Unternehmen, dessen bundesweit verbreitete Bäckereien und Backstuben überwiegend von Franchise-Partnern geführt werden. Die Firmenverantwortlichen und der betriebliche Datenschutzbeauftragte entwickel-

ten dabei mit meiner Unterstützung eine Richtlinie für die Franchisenehmer mit datenschutzrechtlichen Standards für den Einsatz von Videoüberwachungskameras. Zudem soll mit vertragsrechtlichen Maßnahmen sichergestellt werden, dass die Datenschutzanforderungen bei Videoüberwachungen in den Franchise-Betrieben umgesetzt und durch den betrieblichen Datenschutzbeauftragten des Unternehmens kontrolliert werden.

In deutlichem Kontrast zu diesem Positivbeispiel stand eine erhebliche Anzahl unzulässiger Videoüberwachungen, bei denen Beschäftigte von Videokameras an ihrem ständigen Arbeitsplatz erfasst wurden. In zwei Fällen waren die Verstöße so gravierend, dass sie mit Bußgeldern geahndet werden mussten:

In den saisonal betriebenen Verkaufsständen einer Bäckerei kontrollierten Videokameras nicht nur die Warenpräsentationen, sondern auch die Beschäftigten an ihrem Arbeitsplatz. Trotz einer von mir bereits vor längerer Zeit ausgesprochenen Aufforderung, künftig auf die unzulässige Videokameraüberwachung der Beschäftigten zu verzichten, wurden solche Kameras erneut installiert. Diese konnten in der Firmenzentrale jederzeit bei Bedarf durch die Geschäftsleitung eingesehen werden. Zwar wurde die Videoüberwachung nach einem Vor-Ort-Termin in der Firmenzentrale unverzüglich eingestellt. Wegen der wiederholten Verstöße musste jedoch ein Bußgeld in empfindlicher Höhe verhängt werden.

In einem anderen Fall führte ein Betreiber von Tankstellen- und Waschanlagen mit bundesweiten Niederlassungen auf dem jeweiligen Betriebsgelände sowie in den Servicebereichen umfangreiche Videoüberwachungen durch. Die Videokameras erfassten Kundinnen und Kunden sowie Beschäftigte. Videobildaufnahmen von einigen Niederlassungen des Unternehmens waren zudem im Internet durch Eingabe der jeweiligen Webadresse zugänglich. Einen betrieblichen Datenschutzbeauftragten bestellte das Unternehmen erst am Tag vor meinem Informations- und Kontrollbesuch. Das Unternehmen zeigte sich im Rahmen meiner datenschutzrechtlichen Überprüfung zwar kooperativ, indem Empfehlungen zur Verbesserung des Datenschutzes zeitnah umgesetzt wurden. Ferner wurden unter anderem zahlreiche Kameras entfernt, bei den verbliebenen Kameras die Ausrichtung verändert sowie erfasste Nachbargrundstücke oder öffentliche Verkehrsflächen verpixelt. Dennoch waren die festgestellten unzulässi-

gen Eingriffe in die Persönlichkeitsrechte der erfassten Personen derart schwerwiegend, dass ich ein Bußgeld in Höhe von 54.000 Euro festgesetzt habe.

Wäre rechtzeitig ein betrieblicher Datenschutzbeauftragter bestellt und mit einer Vorabkontrolle beauftragt worden, die im Übrigen bei einer derartigen Videoüberwachung vorgeschrieben ist, hätten die Datenschutzverstöße vermieden werden können. Auch unter diesem Gesichtspunkt habe ich die unterlassene Bestellung eines betrieblichen Datenschutzbeauftragten mit einem Bußgeld in Höhe von weiteren 10.000 Euro geahndet.

- Unternehmensverantwortlichen ist dringend anzuraten, sich vor Durchführung einer Videoüberwachung zu vergewissern, welche gesetzlichen Anforderungen an einen Einsatz von Videokameras am Arbeitsplatz ihrer Beschäftigten und in Kundenbereichen zu stellen und umzusetzen sind. Ist ein Betriebsrat vorhanden, muss er beteiligt werden. Der Einsatz von Videokameras sollte stets in einer Betriebsvereinbarung geregelt werden. Bei Verstößen werde ich weiterhin konsequent von meinen aufsichtsrechtlichen Befugnissen Gebrauch machen.

6.2 Videoüberwachung in Arztpraxen

Dürfen in einer ärztlichen Praxis Videokameras angebracht werden, um den Empfangstresen, den Eingangs- oder den Wartebereich zu überwachen? Kann eine Videokamera in einem Aufwachraum eingesetzt werden, um Patientinnen und Patienten nach einer ärztlichen Behandlung zu beobachten?

Videoüberwachung findet einerseits in den öffentlich zugänglichen Bereichen wie Eingangs- und Empfangszonen sowie in Wartezimmern statt. Vereinzelt kommen sie zudem in Behandlungs-, Therapie- und Aufwachräumen zum Einsatz.

Begründet werden die Videoüberwachungsmaßnahmen etwa mit dem Schutz der Praxis vor Einbruch und unbefugtem Betreten sowie mit dem Schutz der Patientinnen und Patienten vor Diebstahl oder Übergriffen. Allerdings können diese Straftaten bereits durch herkömmli-

che Sicherungsmaßnahmen, etwa Türöffnungssysteme, die erst auf individuelle Freigabe nach Anforderung öffnen, abschließbare Garderobenfächer oder gesicherte Bargeldaufbewahrungen im Empfangsbereich, erschwert oder verhindert werden. Daher ist eine Videoüberwachung zu diesen Zwecken jedenfalls während der Praxiszeiten nicht erforderlich.

Auch eine bessere Beobachtung von Patientinnen und Patienten in bestimmten Behandlungssituationen wird als Grund angeführt. Der Einsatz von Videoüberwachungstechnik zur Kontrolle von Verfahrensabläufen oder zur Erleichterung der Therapiedurchführung mag zur Kosteneinsparung auf den ersten Blick hilfreich und geeignet erscheinen. Zu bedenken ist allerdings, dass jedenfalls bei dem Risiko schwerwiegender Komplikationen Videoüberwachung die Anwesenheit von medizinisch geschultem Personal, das sofort reagieren kann, nicht zu ersetzen vermag.

Es ist von einem überwiegenden Interesse der Patientinnen und Patienten auszugehen, in einer Arztpraxis nicht videoüberwacht zu werden. Bereits der Umstand, dass eine Person eine Arztpraxis aufsucht, stellt ein Gesundheitsdatum dar, das mit besonderer Sensibilität zu behandeln ist, zumal viele Menschen beim Besuch einer Ärztin oder eines Arztes in erkennbar schlechter gesundheitlicher Verfassung sind.

➡ Videoüberwachung gehört nicht in eine Arztpraxis.

7 Verkehr

7.1 Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Ein Auto verfügt über zahlreiche Steuergeräte, in denen eine große Menge an Daten gespeichert wird. Diese Datenspeicher sind unter anderem notwendig für verschiedene Assistenzsysteme. Die Entwicklung in der Automobilindustrie geht jedoch in großen Schritten weiter. So kann das Fahrzeug etwa mit Hilfe des Smartphones mit dem Internet verbunden werden, um Zusatzdienste nutzen zu können. Auch testen einige Hersteller- und Internetfirmen schon das autonom – also ohne Fahrerin oder Fahrer – fahrende Auto. Je mehr Daten im Auto

verarbeitet werden und je mehr Beteiligte (Automobilhersteller, Händler, Werkstätten, Kommunikations- und Teledienstanbieter) auf diese Daten zugreifen können, desto stärker wird das informationelle Selbstbestimmungsrecht berührt. Auch werden Begehrlichkeiten bei Versicherern, Arbeitgebern und staatlichen Stellen geweckt.

Folgende Datenkategorien stehen hierbei im Vordergrund:

- Fahrzeugdatenspeicher

Daten, die in den Speichermedien der elektronischen Steuerungseinheiten gesammelt werden (so genannte Betriebsdaten) – zum Beispiel Geschwindigkeit, Bremsbetätigung, Beschleunigung, Füllstände und vieles mehr – dienen letztlich dazu, eine störungsfreie Nutzung des Fahrzeuges zu ermöglichen und eine etwaige Wartung oder Reparatur zu erleichtern.

- Europäischer Notruf (eCall)

Die Europäische Union führt ein EU-weites Notrufsystem mit dem Namen "eCall" verbindlich ein. Spätestens ab dem Jahr 2018 sollen in allen neuen Personenkraftwagen und leichten Nutzfahrzeugen serienmäßig Notrufgeräte installiert werden, die bei schweren Autounfällen automatisch per Mobilfunkverbindung über die europaweite Notrufnummer 112 die Rettungsdienste benachrichtigen und eine Kommunikation zur Fahrerin oder zum Fahrer aufbauen. Die Rettungsdienste erhalten auf diesem Weg in einem Minimaldatensatz Angaben zum Standort, zur Fahrtrichtung, zum Unfallzeitpunkt, zur Anzahl der Insassen und zum Fahrzeugtyp, um so schnell und effizient Hilfe zu leisten. Der eCall-Notruf kann auch von der Fahrerin oder dem Fahrer manuell ausgelöst werden. Er darf jedoch nicht als Pannenruf oder als Auskunftsplattform missbraucht werden, sondern ist nur für echte Notfälle gedacht. Der eCall ist im Normalzustand abgeschaltet und wird erst bei einem Unfall – automatisch oder manuell – aktiviert. Die Datenverarbeitung für den reinen eCall ist auf die Rettungsleitstelle und ihre Hilfsmaßnahmen beschränkt. Eine Ortung findet nur im Notfall statt.

- Mehrwertdienste

Während gegen den auf Notfälle und Rettungsmaßnahmen bezogenen eCall datenschutzrechtlich im Grundsatz Bedenken nicht erhoben

werden, sind die kommerziellen Mehrwertdienste parallel zum eCall kritisch zu sehen. Beispiele für Mehrwertdienste sind besondere Dienstleistungsangebote der Fahrzeughersteller mit auf die Automarke zugeschnittenem Pannenruf, Dienste der Versicherungen bei Unfällen und Beschädigungen, sowie internetbasierte Angebote (zum Beispiel Hotel- oder Restaurantsuche). Der Markt der Mehrwertdienste wird von den Automobilherstellern und ihren Vertragswerkstätten, von den Versicherern, den Mobilfunkanbietern und den Automobilclubs sowie von zahlreichen Internetfirmen stark umworben, denn diese Dienste sind in der Regel kostenpflichtig und bedürfen einer permanenten Mobilfunkanbindung.

Auf Initiative des Düsseldorfer Kreises hat die Datenschutzkonferenz am 8./9. Oktober 2014 eine Entschließung zum Datenschutz im Kraftfahrzeug getroffen (Abdruck im Anhang). Danach sind Automobilhersteller, Händler, Werkstätten sowie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten. Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrerinnen und Fahrer sowie Halterinnen und Halter von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken über-

mittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzerinnen und Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrerinnen und Fahrer sowie Halterinnen und Halter technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

➧ Gemeinsam mit den anderen Aufsichtsbehörden befinde ich mich bereits in intensiven Verhandlungen mit der Automobilindustrie mit dem Ziel, das informelle Selbstbestimmungsrecht beim Autofahren zu wahren. Darüber hinaus wecken in großer Menge und mit hohem Auswertungspotenzial im Kfz erfasste Daten Begehrlichkeiten bei Anbietern von Telekommunikations- und Online-Diensten, Versicherungen, Arbeitgebern und sonstigen Stellen. Autofahren darf nicht ein "gläsernes" Vergnügen mit erheblichen Risiken für die Freiheit sein.

7.2 Stauwarnung durch Bluetooth-Technik

Im Stau steht niemand gerne! Aber müssen Verkehrsteilnehmende für eine Stauwarnung ihre personenbezogenen Daten preisgeben?

Im Bereich der Verkehrsplanung gibt es eine neue Idee: Für die Einrichtung von Stauwarnsystemen wollen Städte auf die Daten der in den Kraftfahrzeugen der Verkehrsteilnehmerinnen und -teilnehmern vorhandenen Bluetooth-Geräte (wie beispielsweise Handys, Freisprech- oder Navigationseinrichtungen) Zugriff nehmen, um damit

die für die Verkehrsanalyse benötigten Reisezeiten der Fahrzeuge zu ermitteln.

Bei diesen Systemen sollen die Bluetooth-Geräte-Adressen (so genannte MAC-Adressen) an mehreren Messstellen im Stadtgebiet beim Vorbeifahren der Kraftfahrzeuge durch Sensoren erfasst und zur weiteren Auswertung an einen kommunalen Verkehrsrechner übermittelt werden. Aus dem Vergleich der Zeitpunkte der Erfassung der MAC-Adresse eines Gerätes an unterschiedlichen Messstellen im Stadtgebiet soll dann die Reisezeit des jeweiligen Fahrzeugs, in dem sich ein solches Gerät befindet, ermittelt werden. Durch das Zusammenführen einer Vielzahl der auf diese Weise erhobenen Datensätze können dann die aktuelle Verkehrslage ermittelt und bei Bedarf entsprechende Stauwarnungen veröffentlicht werden.

Die Erfassung und Verarbeitung von Bluetooth-Geräte-Adressen hat jedoch eine datenschutzrechtliche Dimension, der bei diesen Anwendungen häufig nicht bzw. nicht ausreichend Rechnung getragen wird.

Die MAC-Adresse eines Bluetooth-Gerätes ist eindeutig und grundsätzlich für die gesamte Lebensdauer des Gerätes diesem fest zugeordnet. Die Adresse beinhaltet den Hersteller, den Gerätetyp und eine eindeutige Gerätenummer. Da diese Geräte meist ständig von einer Person mitgeführt werden oder fest in einem Fahrzeug installiert sind, könnte beispielsweise bei einer Personen- oder Verkehrskontrolle die MAC-Adresse eines Gerätes einer bestimmten Person zugeordnet werden. Bei einer Speicherung von MAC-Adressen in einer Datenbank könnten zudem durch entsprechende Auswertungen umfassende und langfristige Bewegungsprofile erstellt werden. Bezüglich derartiger Profile kann nicht ausgeschlossen werden, dass durch die Verknüpfung mit weiteren Datenbeständen oder sonstigen Zusatzinformationen eine Identifizierung des oder der jeweiligen Gerätebesitzenden möglich ist (zum Beispiel durch die Anmeldung in Web-Portalen des Herstellers oder Händlers des Gerätes). Bei MAC-Adressen von Bluetooth-Geräten handelt es sich daher meines Erachtens um personenbezogene Daten. Ihre Erhebung, Verarbeitung und Nutzung unterliegt deshalb den geltenden datenschutzrechtlichen Bestimmungen.

Öffentliche Stellen des Landes NRW sind zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten jedoch nur befugt, wenn eine

Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat (vgl. § 4 Abs. 1 Datenschutzgesetz NRW – DSG NRW). Eine Einwilligung der betroffenen Verkehrsteilnehmenden ist bereits aus rein praktischen Gründen nicht möglich, und eine bereichsspezifische Vorschrift für die Verwendung dieser Systeme gibt es im Straßenverkehrsrecht nicht. Maßnahmen dieser Art könnten daher allenfalls auf § 12 DSG NRW gestützt werden. Vor dem Hintergrund des verfassungsrechtlichen Gebots der Normenklarheit habe ich jedoch erhebliche Zweifel, dass diese allgemeine Datenschutzvorschrift als Rechtsgrundlage für so weitreichende Datenverarbeitungsprozesse ausreichen kann. Allenfalls in Einzelfällen kann dies in Betracht kommen, wenn es sich um zeitlich befristete Maßnahmen handelt.

Auf jeden Fall muss mit technisch-organisatorischen Maßnahmen sichergestellt werden, dass keine Sammlung von Datenbeständen erfolgt, die eine Rückführung auf die jeweiligen Gerätenutzerinnen und -nutzer ermöglicht. Um Bewegungsprofile auszuschließen, müssen die MAC-Adressen sofort nach ihrer Erfassung in Hashwerte umgewandelt werden. Auch diese Hashwerte dürfen nicht dauerhaft gespeichert werden, sondern sind nach ihrer Zusammenführung und Berechnung der Reisezeit – spätestens jedoch nach einem Tag – zu löschen.

- Soweit Kommunen den Betrieb von bluetoothbasierten Stauwarnsystemen überhaupt auf eine Befugnisnorm stützen können, muss beim Einsatz solcher Systeme auf jeden Fall durch geeignete technisch-organisatorische Maßnahmen sichergestellt werden, dass eine Bildung von Bewegungsprofilen und eine Identifizierung der Gerätenutzerinnen und -nutzer ausgeschlossen sind.

7.3 Daten her oder Ihr Bus-Abo ist weg!

Viele Inhaberinnen und Inhaber eines Nahverkehrsabonnements staunten nicht schlecht, als ihnen im Herbst 2013 Post ins Haus flatterte: Entweder sie unterschrieben eine datenschutzrechtliche Einwilligung zur Speicherung von Bewegungsdaten, oder sie seien Anfang 2014 ihr Abo los.

Hintergrund war, dass das Unternehmen für die Abokarten elektronische Tickets einführen wollte, die bei jedem Einstieg in ein Fahrzeug mit Hilfe eines Lesegeräts auf ihre Gültigkeit überprüft werden. Sofern das Lesegerät lediglich den menschlichen Kontrolleur ersetzt und keine personenbezogenen Daten gespeichert werden, verstößt dies nicht gegen datenschutzrechtliche Vorgaben (siehe Bericht 2013 unter 5.2).

Das Unternehmen plante jedoch, den Einstiegsort und -zeitpunkt für sechs Wochen zu speichern, obwohl dies bei Abonnements, die zu beliebig vielen Fahrten im Gültigkeitsbereich berechtigen, nicht erforderlich ist.

Auch kann eine Einwilligung in die Datenerhebung bei Teilnahme am Öffentlichen Personennahverkehr nicht freiwillig sein. Wegen der Monopolstellung der Nahverkehrsunternehmen gibt es keine Wahlmöglichkeit. Hinzu kommt, dass zu jedem Fahrgast personenbezogen Bewegungsprofile gebildet werden könnten.

Aufgrund meiner Hinweise änderte das Unternehmen seine Vorgehensweise noch vor Einführung der elektronischen Abotickets. Die Kundinnen und Kunden erhielten ein zweites Schreiben des Unternehmens, mit dem die neue Vorgehensweise erläutert wurde. Eine Einwilligung wird nicht mehr verlangt.

➧ Wieder einmal gilt: Nur erforderliche Daten dürfen erhoben und verwendet werden. Das Unternehmen hätte seinen Kundinnen und Kunden Aufregung ersparen können, wenn es sich frühzeitig an meine Behörde gewandt hätte.

8 Gesundheit und Soziales

8.1 Der E-Postbrief im Gesundheitswesen

Darf eine Ärztin oder ein Arzt Patientenrechnungen als E-Postbrief verschicken? Berufsgeheimnisträger unterliegen der Schweigepflicht. Wenn sie für Briefe, die die Patientin oder den Patienten betreffen, das E-Postbrief-Verfahren nutzen möchten, ist Vorsicht geboten.

Steigender Kostendruck und Organisationsaufwand veranlassen auch Verantwortliche im Gesundheitswesen immer häufiger zu Einsparungen. Hierbei darf der Schutz der Patientendaten jedoch nicht vernachlässigt werden. Ein Beratungsersuchen zum E-Postbrief-Verfahren zeigt, wo Fallstricke lauern können.

Wer am E-Postbrief-Verfahren teilnehmen will, muss sich bei der Deutsche Post AG registrieren lassen. Dabei gibt es zwei vom Umfang der Registrierung abhängige Versandwege:

Beim vollelektronischen Versand wird der von der Absenderseite verfasste Brief als E-Postbrief unmittelbar an die Empfängerseite versandt. Eine Datenübermittlung begegnet keinen datenschutzrechtlichen Bedenken, soweit eine Ende-zu-Ende-Verschlüsselung gewährleistet, das heißt der elektronische Kommunikationsweg von der Sender- bis zur Empfängerseite vollständig verschlüsselt ist

Falls die Empfängerseite kein E-Postfach hat, erfolgt der Versand mit einem so genannten Hybridbrief. Dabei wird der von der Absenderseite elektronisch erstellte und elektronisch an die Deutsche Post AG versandte Brief von dieser oder durch ein von ihr beauftragtes Druckzentrum ausgedruckt, kuvertiert und dem Empfänger auf dem normalen Postweg zugestellt.

Bei Zustellung mittels des Hybridbriefes nehmen Beschäftigte der Deutsche Post AG sowie der ggf. mit dem Ausdruck der E-Postbriefe beauftragten Subunternehmen vom Inhalt der Daten zwar grundsätzlich keine Kenntnis. Dies kann aber im Rahmen von erforderlichen Qualitätsprüfungen vorkommen. Daher besteht die Möglichkeit, dass Gesundheitsdaten auch von unbefugten Dritten eingesehen werden.

Ärztinnen oder Ärzte laufen damit Gefahr, gegen ihre Schweigepflicht zu verstoßen und sich strafbar zu machen. Um die Dienstleistung dennoch nutzen zu können, muss die betroffene Patientin oder der betroffene Patient in diese Versandmethode schriftlich einwilligen und dabei zuvor auf die Möglichkeit der Offenbarung der Daten hingewiesen werden. Die Deutsche Post AG macht in ihren Allgemeinen Geschäftsbedingungen auf diese Problematik ausdrücklich aufmerksam.

- Ärztinnen und Ärzte sind insbesondere auch bei der elektronischen Kommunikation für die Wahrung des Patientengeheimnisses verantwortlich.

Bei der Inanspruchnahme von Dienstleistungen Dritter wie dem E-Postbriefverfahren müssen sie auch das Kleingedruckte beachten, um Datenschutzverstöße zu vermeiden.

8.2 Beauftragung privater Gutachter durch Versicherungen

Für die Prüfung einer Leistungspflicht der privaten Krankenversicherung kann es notwendig sein, medizinische Gutachterinnen oder Gutachter einzuschalten. In der Praxis erfolgt deren Auswahl teilweise durch zwischengeschaltete Begutachtungsinstitute.

Einige Versicherungen übermitteln die zu begutachtenden Fälle an ein Institut nur nach Entbindung von der Schweigepflicht. Auch dann sollten Klardaten der Versicherten nach Möglichkeit geschwärzt werden, zumal sich die Versicherungen in den "Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft" (siehe Bericht 2013 unter 5.1) dem Grundsatz der Erforderlichkeit verpflichtet haben.

Andere Krankenversicherungen sehen aufgrund der Schwärzung personenbezogener Angaben von einer Schweigepflichtentbindung und Unterrichtung der Versicherten gänzlich ab. Sie nutzen jedoch weiterhin die Versicherungsnummer als Zuordnungsmerkmal.

Von einer Schweigepflichtentbindung kann jedoch nur abgesehen werden, wenn nach sicherer Verschlüsselung das Begutachtungsinstitut Daten keiner Person zuordnen kann. Dies setzt den Verzicht auf die Versicherungsnummer, den Namen und die Anschrift der versicherten Person sowie mögliche weitere Identifikationsmerkmale zwingend voraus.

Eine Krankenversicherung hat zugesagt, zukünftig automatisch per EDV eine Pseudonymisierungsnummer zu erstellen und den Gutachtenauftrag mit einem Code zu versehen. Zudem werde durch weitere technisch-organisatorische Maßnahmen die Schwärzung personenbezogener Daten sicher gewährleistet. Dies ist zu begrüßen.

➧ Nach Mitteilung des Verbands der Privaten Krankenversicherung e. V. prüfen derzeit weitere

Krankenversicherungen eine derartige Verfahrensumstellung.

8.3 Viele Fragen zur Datenverarbeitung in Sozialbehörden

Zahlreiche Anliegen von Bürgerinnen und Bürgern betreffen weiterhin den datenschutzgerechten Umgang mit Sozialdaten.

Die Eingaben zeigen, dass Rat suchende Betroffene vermehrt ein sensibles Gespür für den Umgang mit ihren Daten haben.

Zu häufig gestellten Fragen wie etwa zum Recht auf Akteneinsicht oder zum Umfang von Mitwirkungspflichten (zum Beispiel zur Vorlage von Kontoauszügen) finden sich ausführliche Erläuterungen unter www.ldi.nrw.de. Bereits diese Hinweise sind in vielen Fällen geeignet, datenschutzrechtliche Probleme mit Hilfe von behördlichen Datenschutzbeauftragten vor Ort zu lösen. Viele an mich gerichtete Eingaben ließen sich vermeiden, wenn die Ämter sich eingehender mit den Anliegen der Bürgerinnen und Bürger auseinandersetzen würden.

Gegenstand zahlreicher Anfragen ist aktuell das Bemühen von Sozialleistungserbringern, die Wirksamkeit ihrer Maßnahmen zu prüfen. Die Nachsteuerung von Prozessabläufen ist sinnvoll und möglich. Soweit eine telefonische Zufriedenheitsumfrage durch eine beauftragte nicht-öffentliche Stelle erfolgen soll, ist bei der Umsetzung das Sozialgeheimnis zu wahren. Daher dürfen Daten von Leistungsberechtigten (etwa Name, Vorname und Bezeichnung der Maßnahme) auch für erforderliche Planungen im Sozialleistungsbereich nicht ohne weiteres an Dritte übermittelt werden. Die Übermittlung solcher Daten an eine nicht-öffentliche Stelle zur Durchführung einer Befragung setzt als zweckändernde Nutzung grundsätzlich die Einwilligung der Betroffenen voraus (vgl. §§ 67c Abs. 2 Nr. 3, 75 Abs. 1 Sozialgesetzbuch Zehntes Buch).

➡ Gerade in sozialdatenschutzrechtlichen Angelegenheiten, die für die Betroffenen von besonderer Sensitivität sind, sollten bereits unter den Beteiligten vor Ort alle Möglichkeiten ausgeschöpft werden, berechtigte Anliegen zu berücksichtigen.

9 Innere Sicherheit und Justiz

9.1 Änderung des Polizeigesetzes

Da das Bundesverfassungsgericht weitere Anforderungen an den Abruf von Daten gestellt hatte, die Behörden bei Anbietern von Telekommunikationsdiensten erfragen, war das Polizeigesetz zu ändern. Zugleich musste entschieden werden, ob die Regelung zur Videoüberwachung öffentlich zugänglicher Orte durch die Polizei verlängert wird.

In seinem Beschluss vom 24. Januar 2012 zur Bestandsdatenauskunft (1 BvR 1299/05) hatte das Bundesverfassungsgericht festgestellt, dass die in den §§ 112 und 113 TKG geregelten Auskunftsbefugnisse und -pflichten der Diensteanbieter nicht zugleich auch den Abruf von Daten durch Behörden erlauben. Das Bundesverfassungsgericht sprach in diesem Zusammenhang bildlich vom Erfordernis einer Doppeltür: Der Gesetzgeber muss auf der einen Seite nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auf der anderen Seite auch die Tür zur Abfrage dieser Daten. Ferner stellte das Bundesverfassungsgericht hohe Hürden für den Zugriff auf dynamische IP-Adressen und Zugangssicherungscodes (wie Passwörter, PIN oder PUK) auf. Die bisherige Praxis ließ das Bundesverfassungsgericht zwar vorübergehend ohne ausreichende Rechtsgrundlagen zu, längstens jedoch bis zum 30. Juni 2013. Dabei wies das Gericht auf die Verantwortung des Gesetzgebers für die rechtsstaatliche Ausgestaltung der Datenerhebungsvorschriften hin.

Wie alle Länder und auch der Bund war daher der nordrhein-westfälische Gesetzgeber aufgerufen, hinreichend bestimmte und normenklare Rechtsgrundlagen zu schaffen, die es den Polizeibehörden weiterhin ermöglichen, zur Gefahrenabwehr Telekommunikations- und Telemediendaten bei den Diensteanbietern zu erheben.

Behördliche Datenerhebungen, die Rückschlüsse auf das Kommunikationsverhalten betroffener Personen ermöglichen können, stellen gravierende Grundrechtseingriffe dar. Deshalb habe ich mich für einen Richtervorbehalt ausgesprochen, soweit Telekommunikations- und Telemediendaten erhoben oder mit so genannten IMSI-Catchern die Position eines Mobilfunkgerätes ermittelt werden sollen. Insbesondere dann, wenn die Maßnahmen ohne Wissen der Betroffenen

durchgeführt werden, kann das Erfordernis einer richterlichen Anordnung ein Mindestmaß an vorbeugendem Grundrechtsschutz gewährleisten.

Trotz der von mir und anderen Sachverständigen vorgetragenen Argumente für einen Richtervorbehalt verlangt der neue § 20a Polizeigesetz NRW lediglich, dass Abfragen von Bestands-, Verkehrs- und Nutzungsdaten von der Behördenleitung anzuordnen sind. Beim Einsatz von so genannten IMSI-Catchern nach § 20b Polizeigesetz NRW ist nicht einmal ein Behördenleitervorbehalt vorgesehen. Eine eingehende Kontrolle durch eine unabhängige Stelle ist somit bei diesen Maßnahmen allenfalls nachträglich möglich.

Daneben war über die Verlängerung der Möglichkeit zur Videobeobachtung öffentlich zugänglicher Orte durch die Polizei zu entscheiden, da die hierfür einschlägige Rechtsgrundlage (§ 15a Polizeigesetz NRW) bis zum 31. Juli 2013 befristet war.

Im Rahmen des Gesetzgebungsverfahrens zur Änderung des Polizeigesetzes NRW habe ich darauf hingewiesen, dass die Wirksamkeit der polizeilichen Videobeobachtung bisher nicht wissenschaftlich belegt werden konnte. Der vom Ministerium für Inneres und Kommunales hierzu vorgelegte Evaluierungsbericht wurde weder von einer unabhängigen Stelle erstellt noch genügt er wissenschaftlichen Standards.

§ 15a Polizeigesetz NRW ist schließlich dahingehend ergänzt worden, dass die Auswirkungen dieser Vorschrift und die praktische Anwendung durch die Landesregierung unter Mitwirkung einer oder eines unabhängigen wissenschaftlichen Sachverständigen geprüft werden.

➧ Sowohl für die Videobeobachtung als auch für die Erhebung von Telekommunikations- und Telemediendaten ist gesetzlich die Evaluierung unter Mitwirkung von unabhängigen wissenschaftlichen Sachverständigen vorgesehen. Ich werde die polizeiliche Praxis weiterhin beobachten und die vorzulegenden Evaluierungsberichte kritisch auswerten.

9.2 Informationspflichten der Sicherheitsbehörden bei technischen Ermittlungsmaßnahmen

Sicherheits- und Strafverfolgungsbehörden haben in den letzten Jahren zusätzliche Ermittlungsbefugnisse erhalten, die zu gravierenden Grundrechtseingriffen führen können. Beim Einsatz verdeckter Ermittlungsmethoden ist es wichtig, dass die betroffenen Personen zumindest nachträglich unterrichtet werden. Um die Dimensionen und Auswirkungen der Ermittlungsmaßnahmen aber auch in ihrer Gesamtheit abschätzen und bewerten zu können, sind zudem Informationspflichten gegenüber Kontrollinstanzen und der Öffentlichkeit unerlässlich.

Im Bereich der elektronischen Telekommunikation stehen den Behörden besondere Ermittlungsmethoden wie die Funkzellenabfrage, die "stille SMS" oder der "IMSI-Catcher" zur Verfügung, die unter anderem die Erhebung von Bestands- und Verkehrsdaten ermöglichen.

Der Benachrichtigung der Betroffenen kommt dabei große Bedeutung zu. Soweit die gesetzlichen Regelungen den Behörden ein Beurteilungsermessen einräumen, besteht allerdings die Gefahr, dass Benachrichtigungen dort, wo sie angebracht wären, unterbleiben. Andererseits darf ein Verfahren zur Benachrichtigung nicht dazu führen, dass zusätzlich noch weitere Daten zu den Betroffenen erhoben werden müssen. Die offenen Fragen konnten im Berichtszeitraum mit dem Ministerium für Inneres und Kommunales und dem Justizministerium des Landes noch nicht abschließend geklärt werden.

Überdies ermöglicht die derzeit bestehende Berichtspraxis der Behörden im Lande keine verlässliche Beurteilung über das Ausmaß der Überwachung und die Anzahl der Betroffenen. Die wehrhafte Demokratie ist auch auf heimliche Ermittlungsmethoden angewiesen, um ihre Bürgerinnen und Bürger vor Gefahren zu schützen und um Straftaten aufzuklären. In einem Rechtsstaat muss die Allgemeinheit aber erfahren können, in welchem Umfang die Behörden verdeckte Ermittlungsmaßnahmen einsetzen, damit das konkrete Ausmaß der Betroffenheit erkennbar wird. Nur dann ist eine sinnvolle gesellschaftliche Diskussion über das Spannungsverhältnis zwischen Freiheit und Sicherheit möglich.

Auch eine effektive Kontrolle der Ermittlungsbehörden und der Nachrichtendienste durch parlamentarische Gremien und unabhängige Datenschutzbeauftragte setzt voraus, dass diesen Stellen aussagekräftige Informationen über den Einsatz heimlicher Überwachungsmethoden an die Hand gegeben werden. In der Konferenz der Informationsfreiheitsbeauftragten habe ich mich daher für mehr Transparenz eingesetzt. Siehe Entschließung "Mehr Transparenz bei technischen Ermittlungsmethoden – Vertrauen in den Rechtsstaat stärken!" vom 9. Dezember 2014 (Abdruck im Anhang).

➧ Sowohl aus Sicht des Datenschutzes der einzelnen betroffenen Bürgerinnen und Bürger als auch mit Blick auf die Informationsfreiheit sind sowohl der Gesetzgeber als auch die Behörden des Landes gefragt, für mehr Transparenz zu sorgen.

9.3 Novellierung des Verfassungsschutzgesetzes

Die Novellierung des Verfassungsschutzgesetzes NRW (VSG NRW) verfolgt das begrüßenswerte Ziel, unter anderem Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (Az.: 1 BvR 370/07) zur so genannten "Online-Durchsuchung" umzusetzen. Zu dem Vorhaben, das sich durch besondere Komplexität auszeichnet, habe ich umfänglich im Rahmen einer Anhörung am 2. Mai 2013 im Landtag NRW Stellung genommen. Leider sind meine Bedenken, die hauptsächlich die Bestimmtheit und die Anforderungen an das Verfahren betreffen, kaum aufgegriffen worden.

Auf zwei Punkte, die mir besonders wichtig sind und im Zusammenhang stehen, möchte ich eingehen:

- Zugriff auf zugangsgesicherte Telekommunikationsinhalte und sonstige Informations- und Kommunikationsinhalte im Internet

In der Anhörung des Landtags hatte ich empfohlen, die neu geschaffene Eingriffsbefugnis in § 5 Abs. 2 Nr. 11 VSG NRW zum "Zugriff auf zugangsgesicherte Telekommunikationsinhalte und sonstige Informations- und Kommunikationsinhalte im Internet" zu präzisieren, die, wie Gesetzeswortlaut und Begründung erkennen lassen, die Überwachung von Daten unter anderem aus Telekommunikationsvorgängen

ermöglichen soll. Schließlich war die Vorgängerregelung auch an den Bestimmtheitsanforderungen des Bundesverfassungsgerichts gescheitert. Wenn der in Folge überarbeitete Gesetzeswortlaut nunmehr vorsieht, Zugriffe des Verfassungsschutzes auf Inhalte "im Internet" technisch lediglich auf dem für jede Nutzerin und jeden Nutzer vorgesehenen Weg zu ermöglichen, können Bürgerinnen und Bürger – was aber schon mit Unwägbarkeiten verbunden ist – allenfalls vermuten, dass eine Ausspähung von Daten beispielsweise mittels einer Infiltrationssoftware nicht erlaubt sein soll. Denn diese Art des Zugriffs entspricht wohl kaum dem, was technisch für jede Nutzerin und jeden Nutzer "vorgesehen" ist. Ein derartiges Verständnis setzt aber voraus, als "technisch vorgesehen" nur solche Vorgehensweisen einzuordnen, die Nutzerinnen und Nutzern gesetzlich erlaubt sind. Wird dem Begriffspaar ("technisch vorgesehen") hingegen ein Verständnis etwa in dem Sinne zugrunde gelegt, dass der Zugangsmodus sich nach Vorgaben von Dienste- oder Geräteanbietern richtet oder sich gar nach dem technisch Möglichen bestimmt, steht die für eine Eingriffsnorm erforderliche Bestimmtheit nicht zweifelsfrei fest.

Das Gesetz geht – offenbar in der Absicht, vollständig für Klarheit zu sorgen – weiter und schließt eine "Online-Durchsuchung" ausdrücklich aus. Damit ist die über eine laufende Telekommunikationsüberwachung hinausgehende Ausspähung aller auf einem Speichersystem verfügbaren Daten mittels einer besonderen Software gemeint. Sollte der Zugang nur auf dem vorgesehenen Weg im Sinne des oben dargelegten Verständnisses zugelassen sein ("technisch vorgesehen" im Sinne von gesetzlich erlaubt), müsste nicht noch ausdrücklich der Zugang mittels einer Software ausgeschlossen werden, wie sie bei einer "Online-Durchsuchung" Anwendung findet. Allerdings schließt der Gesetzeswortlaut lediglich die "Online-Durchsuchung" aus. Im Umkehrschluss stellt sich dann die Frage, ob nicht doch die weniger weitreichende, aber gleichwohl eingriffsintensive so genannte "Quellen-Telekommunikationsüberwachung" dem Wortlaut nach möglich sein könnte, bei der zur Erfassung "lediglich" der laufenden Telekommunikation an dem Zielsystem ebenfalls eine Infiltrationssoftware aufgespielt wird. Demgegenüber führt als Beispiel für die geplante Art des Zugriffs leider nur die Gesetzesbegründung den Zugang etwa über Zugangscodes oder Passworte an. Hier vermisse ich klare, jegliches Missverständnis ausschließende Regelungen im Ge-

setzestext, die für die Bürgerinnen und Bürger aus sich heraus verständlich sind.

Zu bedenken ist auch die Reichweite einer solchen Maßnahme, soweit sie ebenso Daten erfasst, die nach Abschluss von Kommunikationsvorgängen in einem Speichermedium abgelegt sind.

- Zugangssicherungsdaten

In § 5 Abs. 2 Nr. 15 VSG NRW wird unter anderem die Erhebung der Zugangssicherungsdaten (PIN, PUK) bei Telekommunikationsanbietern geregelt. Hat sich der Verfassungsschutz solche Daten wo und wie auch immer beschafft, ist ihm der Zugang zu Informationen auf einem Speichermedium nunmehr unabhängig von der Mitwirkung anderer Stellen nahezu unbegrenzt eröffnet. Wegen der besonderen Eingriffsintensität ist es jedoch geboten, bereits die Beschaffung von Zugangssicherungsdaten einer unabhängigen Kontrollstelle vorzulegen. Auch hier bleibt der Gesetzentwurf hinter meinen Erwartungen zurück.

➡ Wegen der hohen Eingriffsintensität von Maßnahmen des Verfassungsschutzes bedarf es klarer Vorgaben. Angesichts der weit gefassten Eingriffstatbestände und der Komplexität von Verweisungen ist zu befürchten, dass nur wenige Fachleute in der Lage sind, den Gesetzestext zu durchdringen. Unter rechtsstaatlichen Gesichtspunkten erscheint es bedenklich, wenn die Bürgerinnen und Bürger aus eigener Anschauung kaum noch in der Lage sind, das Ausmaß ihrer Betroffenheit durch staatliches Handeln zu überblicken. Die Anwendung des Gesetzes in der Praxis wird weiterhin kritisch zu begleiten sein.

9.4 Novellierung des Strafvollzugsrechts

Seit der Föderalismusreform obliegt den Ländern die Zuständigkeit für den Strafvollzug. Im Jahre 2014 verabschiedete der Landtag ein Gesetz zur Regelung des Erwachsenenstrafvollzugs (StVollzG NRW). Von mir im Rahmen des Gesetzgebungsverfahrens eingebrachte Änderungsvorschläge wurden leider nur zum Teil übernommen.

Besonders hervorheben möchte ich folgende Themen:

- Offenbarungspflicht von Ärztinnen und Ärzten

Ärztinnen und Ärzten sowie Psychologinnen und Psychologen wird durch § 112 Abs. 2 Satz 2 und Abs. 4 des Gesetzes eine Pflicht zur Offenbarung von Gesundheitsdaten gegenüber der Anstaltsleitung auferlegt. Zwar soll die Verpflichtung nur bestehen, soweit dies auch unter Berücksichtigung der Interessen der Gefangenen an der Geheimhaltung der personenbezogenen Daten erforderlich ist. Dies könnte zur Verhinderung von Selbstverletzungen, zur Abwehr von erheblichen Gefahren für Leib oder Leben anderer Gefangener oder Dritter oder zur Abwehr der Gefahr erheblicher Straftaten im Einzelfall geboten sein. Eine Offenbarung von besonders geschützten Daten ist in Notstandssituationen jedoch zulässig – unabhängig von einer Verpflichtung der Berufsgeheimnisträger. Die Frage, ob und ggf. welche konkreten Anhaltspunkte den Gesetzgeber veranlassen, die ärztliche Entscheidungsfindung einzugrenzen und das Offenbarungsrecht nunmehr in eine Offenbarungspflicht umzuwandeln, ist unbeantwortet geblieben.

- Versorgung durch nebenamtliche oder vertraglich verpflichtete Ärztinnen und Ärzte

Daneben soll nach § 99 Abs. 1 Satz 2 des Gesetzes die ärztliche Versorgung aus "besonderen Gründen" nebenamtlichen oder vertraglich verpflichteten Ärztinnen oder Ärzten übertragen werden. Die Regelung ist zu unbestimmt, da die "besonderen Gründe" nicht konkret benannt werden. Weiterhin fehlt eine Regelung hinsichtlich der notwendigen Schweigepflichtentbindungserklärung bei einer Datenübermittlung zwischen hauptamtlichen und nebenamtlich/vertraglich verpflichteten Ärztinnen und Ärzten.

- Seelsorge

Nicht nachvollziehbar ist, weshalb nach § 69 des Gesetzes die regelmäßige Überwachung von Gesprächen mit Seelsorgerinnen und Seelsorgern nur auf deren Verlangen ausgesetzt werden können soll. Es ist davon auszugehen, dass sich die Gefangenen aufgrund ihrer Situation oftmals in extremen seelischen Nöten befinden und Seelsorgerinnen und Seelsorger unter Umständen die einzigen Personen sind, denen sie sich bedingungslos anvertrauen können. Daher ist eine

nicht überwachte Seelsorge auch auf Wunsch der Gefangenen zu gewährleisten. Etwaigen Sicherheitsbedenken kann durch geeignete Maßnahmen begegnet werden.

- Auskunft und Akteneinsicht

Das in § 116 angelegte Recht der Gefangenen auf Akteneinsicht in die eigene Personalakte besteht nicht vollumfänglich. Sie erhalten Akteneinsicht nur, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht und sie dafür auf die Einsichtnahme angewiesen sind. Ein nachvollziehbarer Grund für diese Einschränkung ist nicht ersichtlich. Das Grundrecht auf informationelle Selbstbestimmung umfasst das Recht des Einzelnen zu erfahren, wer welche Daten zu welchem Zweck über ihn gespeichert hat – und dies unabhängig von weiteren Bedingungen.

- Telefonüberwachung

Das Gesetz sieht vor, der Justizvollzugsbehörde zu ermöglichen, Telefonate sporadisch zu überwachen und damit personenbezogene Daten zu erheben. Nach meinem Verständnis soll die Überwachung zwar mit Einwilligung der Betroffenen, aber unangekündigt – also ohne Wissen der Betroffenen – erfolgen. Daher habe ich angeregt, im Gesetzestext statt einer "unregelmäßigen" eine "unangekündigte" Überwachung vorzusehen. Darüber hinaus lässt sich dieser Regelung nicht entnehmen, was konkret unter "Überwachung" zu verstehen ist – das bloße Mithören der Gespräche oder die Aufzeichnung von Gesprächen bzw. von Gesprächsteilen?

➡ Leider ist mit dem Gesetz die Chance vertan worden, sich von den herkömmlichen Standards zu lösen und den Datenschutz im Strafvollzug weiter zu entwickeln.

10 Kommunales und Archivwesen

10.1 Bürgeranträge nach § 24 Gemeindeordnung NRW sind nicht anonym möglich

Durch eine Bürgereingabe wurde ich mit der Frage befasst, ob die Weitergabe personenbezogener Daten der Einsenderinnen und Einsender von Bürgeranträgen nach § 24 Gemeindeord-

nung NRW (GO NRW) an den Rat der Gemeinde mit den Regelungen des Datenschutzgesetzes NRW (DSG NRW) in Einklang steht.

Nicht selten wenden sich Bürgerinnen und Bürger schriftlich an ihre Kommune, sei es im Rahmen dort laufender Verwaltungs- oder Antragsverfahren, sei es im Rahmen von Anregungen oder Beschwerden. Soweit sie ihr individuelles Anliegen an den Bürgermeister oder die Verwaltung der Kommune richten, unterliegt die weitere Bearbeitung ihres Anliegens sowie die damit einhergehende Verarbeitung ihrer personenbezogenen Daten den Regelungen des DSG NRW. Die Kommune darf unter Beachtung der Grundsätze der Erforderlichkeit sowie der Datensparsamkeit nur solche Daten verarbeiten, die für ihre Aufgabenerfüllung zwingend erforderlich sind. In den Fällen, in denen eine Beschlussfassung durch den Rat angezeigt ist, hat die Verwaltung der Kommune in jedem Einzelfall zu prüfen, ob entweder eine bereichsspezifische Rechtsgrundlage die Weitergabe der personenbezogenen Daten der Einsenderin oder des Einsenders erlaubt oder ob dem Rat eine Entscheidung auch ohne konkreten Personenbezug und damit ohne Kenntnis der personenbezogenen Daten der Einsenderin oder des Einsenders möglich ist.

Auch nach Auffassung des Ministeriums für Inneres und Kommunales NRW ist eine hiervon abweichende Verfahrensweise indes angezeigt, wenn eine Bürgerin oder ein Bürger von dem ihr bzw. ihm eingeräumten Recht nach § 24 GO NRW Gebrauch macht und sich mit einer Einwendung oder einer Beschwerde im Rahmen eines Bürgerantrags direkt an den Rat wendet bzw. aus dem Antrag erkennbar ist, dass eine Befassung des Rates als bürgerschaftliche Vertretung der Kommune gewünscht wird. Diese Vorschrift in der Gemeindeordnung ist Artikel 17 des Grundgesetzes (GG), dem Petitionsrecht, nachgebildet und über Artikel 4 Abs. 1 auch in der Landesverfassung NRW verankert. Nach Artikel 17 GG hat jedermann das Recht sich einzeln oder in Gemeinschaft mit anderen schriftlich mit Bitten oder Beschwerden an die zuständigen Stellen und an die Volksvertretung zu wenden. Für die kommunale Ebene bedeutet dies, dass Bürgeranträge in Angelegenheiten der Gemeinde nach § 24 GO NRW ebenfalls schriftlich beim Rat einzureichen sind. Was unter schriftlich zu verstehen ist, wird in § 126 des Bürgerlichen Gesetzbuches definiert. Dort heißt es: "Ist durch Gesetz schriftliche Form vorgeschrieben, so

muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden." Dabei kommt der Unterschrift unter anderem die Funktion zu, die Identität des Aus- bzw. Antragstellers erkennbar zu machen. Bürgeranträge nach § 24 GO NRW müssen daher den Namen der Einsenderin oder des Einsenders erkennen lassen.

Auch eine ggf. geäußerte Bitte der Einsenderin oder des Einsenders eines Bürgerantrags nach § 24 GO NRW, den Antrag anonym zu behandeln, lässt unter Berücksichtigung des bestehenden Schriftformerfordernisses keine andere Sichtweise zu.

➧ Die Weitergabe personenbezogener Daten der Einsenderinnen und Einsendern von Bürgeranträgen nach § 24 GO NRW an den Rat der jeweiligen Kommune ist wegen der einschlägigen und insoweit vorrangigen kommunalverfassungsrechtlichen Regelungen zulässig.

10.2 Erhebungen für Zwecke der Hundesteuer

Kommunen sind ebenso wie staatliche Finanzbehörden zu einer gesetzmäßigen und gleichmäßigen Besteuerung der Bürgerinnen und Bürger verpflichtet. Dazu gehört nach § 85 der Abgabenordnung auch die Aufdeckung und Ermittlung unbekannter Steuerfälle. Um die Besteuerung der Hundehaltung durchführen zu können, erheben die Kommunen regelmäßig den Hundebestand im Gemeindegebiet.

Zur Erhebung des Hundebestands besuchen Beschäftigte beauftragter Unternehmen in regelmäßigen Abständen alle Haushalte und Betriebe im Gemeindegebiet persönlich und stellen durch Befragung fest, ob dort Hunde gehalten werden. Dabei sollen in Listen, die vom kommunalen Steueramt mit Straßenbezeichnung und Hausnummer versehen sind, der Name der Hundehalterin oder des Hundehalters und die Anzahl der Hunde eingetragen werden. Nach Abschluss der Befragung sollen die ausgefüllten Listen an das Steueramt der Gemeinde für eine etwaige Hundesteuererhebung zurückgegeben werden. Die Mitwirkung angetroffener Bürgerinnen und Bürger an der Befragung ist stets freiwillig.

Eine gemeinsam mit dem Städte- und Gemeindebund NRW herausgegebene Informationsschrift "Hundebestandsaufnahme durch private Unternehmen" erläutert, welche Befugnisse privaten Dritten bei der Hundebestandsaufnahme zustehen (www.ldi.nrw.de).

➡ Steuerpflichtige sollten ebenso wie Kommunen wissen, unter welchen datenschutzrechtlichen Voraussetzungen derartige Datenerhebungen durchführbar sind.

10.3 Daten in und aus Archiven

Das Thema "Datenschutz in Archiven" gerät nur selten ins Rampenlicht. Dies kann sich in Einzelfällen jedoch schnell ändern, wenn etwa in großem Stil Daten aus den Archivbeständen veröffentlicht werden oder im Rahmen einer Novellierung des Archivgesetzes NRW (ArchivG NRW) auch datenschutzrechtliche Anforderungen zu berücksichtigen sind.

In diesem Sinne gab es in den letzten beiden Jahren für mich zwei besonders wichtige Anlässe, den Blick auf die Verarbeitung von Daten in und aus Archiven zu richten:

- Internetveröffentlichung "Städtische Jüdinnen und Juden"

Das Archiv einer Kommune – nennen wir sie "X-Stadt" – hatte schon damit begonnen, unter der Überschrift "X-städter Juden" Daten im Internet zu veröffentlichen, als ich von Betroffenen auf diese Datenbank aufmerksam gemacht wurde. Hierzu fand sich auf der Internetseite folgende Erläuterung: "Diese Datenbank befindet sich noch im Aufbau. Langfristig soll sie alle Personen jüdischen Glaubens enthalten, die im 19. oder 20. Jahrhundert in [X-Stadt] geboren wurden, hier heirateten, starben und/oder begraben wurden, hier dauerhaft oder auch nur kurzzeitig lebten, hier arbeiteten, vor Gericht standen und/oder in Haft saßen; kurz alle, die in [X-Stadt] amtlich registriert wurden. Ferner soll die Datenbank auch die Eltern, Ehegatten, Kinder und Geschwister des oben genannten Personenkreises umfassen. Die Angaben stammen aus verschiedenen, im Kommunalarchiv [X-Stadt] und anderen Archiven verwahrten Unterlagen. Die Datenbank soll stetig erweitert und verbessert werden. Das Kommunalarchiv [X-Stadt] ist daher für alle Informationen und Ergänzungen, die einzelne [X-städter] Juden oder deren Familienangehörige betreffen, dank-

bar." Welchem Zweck diese Veröffentlichung dienen sollte, wurde seinerzeit nicht erläutert.

Zum Zeitpunkt meiner ersten Einsichtnahme waren bereits Namen, Fotos und sonstige Angaben zu Personen in diese Datenbank eingestellt, die nach verschiedenen Kriterien recherchiert werden konnten. Es gab Hinweise darauf, dass ein Teil der Daten lebende Personen betraf; andere Angaben bezogen sich auf Verstorbene. Die Datenbank unterlag keiner Zugriffsbeschränkung, so dass die in ihr enthaltenen Informationen weltweit von jeder Internetnutzerin und jedem -nutzer abrufbar und zu unbestimmten Zwecken weiterverwendbar waren. Vor dem Hintergrund antisemitischer Ressentiments bis hin zu kriminellen Übergriffen war daher eine zweckwidrige Verwendung nicht auszuschließen.

Eine Rechtsvorschrift, die die Veröffentlichung von Daten lebender Personen im Internet ohne wirksame vorherige Einwilligung lag nicht vor. Dabei war insbesondere zu beachten, dass es sich bei den in Rede stehenden Angaben um besondere Daten handelte, für die § 4 Abs. 3 Datenschutzgesetz NRW (DSG NRW) einen erhöhten Schutzbedarf vorsieht. Einwilligungen für die Veröffentlichung dieser Daten waren jedoch nicht eingeholt worden, was einen eklatanten Verstoß gegen das Recht der Betroffenen auf informationelle Selbstbestimmung darstellt.

Dieses Recht umfasst in der Regel nur den Schutz der Daten lebender Personen. Unter einem Gesichtspunkt war meine Zuständigkeit jedoch auch in Bezug auf die Angaben zu verstorbenen Personen gegeben: In einigen bereichsspezifischen Vorschriften finden sich Ausnahmen, in denen Daten von Verstorbenen ebenfalls geschützt werden (siehe Bericht 2003 unter 11.5). So sieht das ArchivG NRW besondere, über den Tod der betroffenen Person hinausgehende Schutzfristen für personenbezogenes Archivgut vor. Diese können unter bestimmten Voraussetzungen und zu bestimmten Zwecken verkürzt werden; in anderen Fällen ist die Nutzung des Archivguts allerdings auch ganz oder zum Teil zu versagen.

Nach §§ 8 Satz 1, 10 Abs. 5 ArchivG NRW ist ein Kommunalarchiv berechtigt, Archivgut sowie die dazugehörigen Findmittel unter Wahrung der schutzwürdigen Belange Betroffener zu veröffentlichen, wobei gemäß § 8 Satz 2 ArchivG NRW ggf. weitere Einschränkungen

zu beachten sind. Für die Veröffentlichung des in Rede stehenden personenbezogenen Archivguts in der Internetdatenbank waren die Voraussetzungen dieser Rechtsvorschrift indes nicht erfüllt:

Es war insbesondere nicht zu erkennen, dass bei der Veröffentlichung die "schutzwürdigen Belangen der Betroffenen" berücksichtigt oder gar gewahrt worden waren. Die Angehörigen, die sich wegen dieser Veröffentlichungen an mich gewandt hatten, äußerten sich vielmehr tief betroffen. Waren ihre Vorfahren, Familienangehörigen und ggf. auch sie selbst in der Zeit des Nationalsozialismus gänzlich recht- und schutzlos gewesen, empfanden sie die weltweite Bekanntgabe der ihre Familien betreffenden Daten unter der Überschrift "X-städter Juden" nunmehr als erneute öffentliche Ausgrenzung und Anprangerung, diesmal allerdings mit den modernen Mitteln der Informationstechnik. Auch wenn ein solcher Effekt nicht beabsichtigt war, ist zu bedauern, dass die Sensitivität des personenbezogenen Archivguts bei der Entscheidung über die Veröffentlichung nicht hinreichend berücksichtigt wurde.

Zudem könnten die Daten der Verstorbenen auch einen Bezug zu lebenden Personen haben, und dies ist ein weiterer gewichtiger Aspekt, der im Rahmen der "Wahrung schutzwürdiger Belange" zu beachten gewesen wäre. Ziel der Internetseite war es unter anderem, Stammbäume von Familien zu veröffentlichen. Selbst wenn dabei ausschließlich Namen und andere Daten von verstorbenen Personen genannt werden, ist nicht auszuschließen, dass sich jedenfalls in Einzelfällen Rückschlüsse auf lebende Personen ziehen lassen, etwa bei Namensidentität zwischen Vorfahren und Abkömmlingen oder bei selten vorkommenden Namen. In derartigen Fällen würde es sich bei den veröffentlichten Informationen zugleich um personenbeziehbare Angaben zu lebenden Personen handeln. Bei Eingabe dieser Namen in eine Internet-Suchfunktion ist damit zu rechnen, dass stets auch die Datenbank "X-städter Juden" als Treffer angezeigt würde. Damit schließt sich zugleich auch der Kreis zu den obigen Ausführungen zur Veröffentlichung von Daten lebender Personen.

Angesichts dieser Rechtslage habe ich der Stadt X empfohlen, die Datenbank unverzüglich von der Internetseite zu entfernen. Dieser Empfehlung ist die Kommune nachgekommen.

- Novellierung des ArchivG NRW

Die Evaluation des ArchivG NRW, die im Jahr 2014 anstand, ist dagegen ein gelungenes Beispiel für die rechtzeitige und umfassende Berücksichtigung datenschutzrechtlicher Belange. Nachdem das Kulturministerium NRW in seiner Vorprüfung festgestellt hatte, dass die geplanten Änderungen möglicherweise den Datenschutz berühren könnten, wurde ich frühzeitig beteiligt und um Stellungnahme gebeten. Erfreulicherweise wurden meine Ausführungen (abzurufen unter www.ldi.nrw.de) im Weiteren berücksichtigt, so dass die Novellierung des ArchivG NRW letztlich zu keinen Einschränkungen des Datenschutzes führte.

➧ Auch bei der Verarbeitung von Archivdaten ist sorgfältig darauf zu achten, ob Datenschutzbelange betroffener Personen berührt sein könnten. Je frühzeitiger derartige Überlegungen im Rahmen eines Projekts berücksichtigt werden, desto besser.

11 Datensicherheit

Querschnittserhebung zur Datensicherheit

Sicherheitskonzepte bedürfen einer regelmäßigen Überprüfung. Das bekannt gewordene Vorgehen US-amerikanischer Geheimdienste und die weltweit zunehmende Zahl von Angriffen auf IT-Systeme habe ich zum Anlass genommen, zunächst bei den Kommunen des Landes eine flächendeckende Querschnittserhebung zur Datensicherheit durchzuführen.

Die Querschnittserhebung dient dazu, Anhaltspunkte zu gewinnen, ob und inwieweit weitere Überprüfungen zur Datensicherheit erforderlich sind.

Die Erhebung konzentrierte sich auf konzeptionelle Kernanforderungen der Datensicherheit, beispielsweise ob ein Schutzstufenkonzept sowie ein Sicherheitskonzept vorhanden sind, ob diese einem etablierten Standard entsprechen und Sicherheitsmaßnahmen im Rahmen eines strukturierten Prozesses mit einer oder einem Prozessverantwortlichen ergriffen werden. Ferner wurde nach konkreten Maßnahmen zur IT-Sicherheit gefragt, zum Beispiel nach Penetrationstests oder nach Verschlüsselung von Daten mit hohem Schutzbedarf.

Das Verfahren gestaltete sich übersichtlich und konnte ohne großen Aufwand bei den befragten Kommunen bearbeitet werden. Die Fragen waren bis auf eine Ausnahme zur vereinfachten Beantwortung als Ja/Nein-Optionen formuliert. Der per E-Mail versandte Fragebogen ließ sich sowohl in elektronischer als auch in konventioneller Papierform beantworten.

Umso enttäuschender war zunächst eine Rücklaufquote von nur 44,8%. Erst nach Erinnerung und – in immerhin 21% der Fälle – nachfolgender förmlicher Beanstandung gemäß § 24 Abs. 2 Datenschutzgesetz NRW (DSG NRW) liegen mir nunmehr Antworten sämtlicher Kommunen vor.

Nach Auswertung der Umfrageergebnisse deutet sich im Wesentlichen folgendes Bild an:

- Sicherheitskonzept

Ein Sicherheitskonzept ist unabdingbar, um strukturiert die für die jeweilige Datenverarbeitung zu treffenden technischen und organisatorischen Sicherheitsmaßnahmen ermitteln zu können und bildet damit die Grundlage für das weitere Vorgehen im IT-Sicherheitsprozess.

Ein Drittel der Kommunen (33%) hat nach eigenen Angaben kein Sicherheitskonzept erstellt und hält sich damit nicht an die Vorgaben des § 10 Abs. 3 DSG NRW. Diese Zahl ist auffallend hoch, zumal die Verpflichtung zur Erstellung eines Sicherheitskonzeptes bereits seit der Novellierung des Datenschutzgesetzes im Jahre 2000 besteht.

- Schutzstufenkonzept

Schutzstufenkonzepte dienen der Ermittlung des Schutzbedarfs und sind Grundlage für den weiteren IT-Sicherheitsprozess. Ergibt eine Schutzbedarfsermittlung, dass Daten mit hohem oder sehr hohem Schutzbedarf verarbeitet werden, reicht ein katalogmäßig herstellbarer Basisschutz meist nicht aus, sondern es ist auf der Grundlage einer Risiko- und Bedrohungsanalyse von jeder Kommune in eigener Verantwortung jeweils zu ermitteln, ob darüber hinausgehende, spezifische Maßnahmen zu treffen sind.

43% der Kommunen geben an, ein solches Konzept erstellt zu haben. Die kreisfreien Städte liegen hier mit 65% über dem Durchschnitt.

Die kreisangehörigen Gemeinden sind mit 41% unterdurchschnittlich repräsentiert. Es wird daher zu prüfen sein, ob die kreisangehörigen Gemeinden unabhängig vom jeweiligen Schutzbedarf Standarddienstleistungen von kommunalen Rechenzentren auf der Grundlage eines einheitlichen Schutzniveaus in Anspruch nehmen.

- Aktualisierung von Sicherheitskonzepten

Sicherheitskonzepte müssen regelmäßig überprüft werden. Von den Kommunen mit Sicherheitskonzept geben 91% an, dieses regelmäßig zu tun und einer veränderten Sicherheitslage anzupassen. Bei diesen Kommunen kann nach den Angaben davon ausgegangen werden, dass IT-Sicherheit dort insoweit "gelebt" wird.

- Penetrationstests

Ein Penetrationstest ist ein umfangreicher Sicherheitstest von IT-Systemen mit Mitteln und Methoden, die ein Angreifer anwenden würde.

43% der Kommunen geben an, solche Tests durchzuführen. Hier deutet sich ein positives Bild an; die Zahl sollte aber noch erhöht werden.

Sorge bereitet mir allerdings, dass etwa ein Viertel (26%) der Kommunen weder ein Sicherheitskonzept erstellt hat noch Penetrationstest durchführt bzw. durchführen lässt. In diesen Fällen sind in eigener Regie also weder konzeptionelle Sicherheitsüberlegungen noch praktische Sicherheitsüberprüfungen durchgeführt worden.

Hinzu kommt, dass 25% der Kommunen die Frage, ob zum Schutz besonders sensitiver Daten (zum Beispiel Gesundheits- oder Sozialdaten) Verschlüsselungsverfahren eingesetzt werden, verneinen.

➧ Aus der Umfrage ergeben sich Anzeichen dafür, dass die IT-Sicherheit zumindest bei einem Drittel der Kommunen verbesserungsbedürftig sein dürfte. In Zeiten, in denen die Bedrohungslage kontinuierlich zunimmt, muss das Thema IT-Sicherheit ernst genommen und nach Lösungen gesucht werden. Der Auswertung werden weitere Prüfungen folgen.

12 Informationsfreiheit

12.1 Quo vadis Open Data?!

Wie geht es weiter mit den Strategien zur proaktiven Veröffentlichung von amtlichen Informationen im Internet, wann werden aus Strategien endlich Taten und vor allem: Was wird aus der erforderlichen gesetzlichen Verpflichtung zur antragsunabhängigen Bereitstellung dieser Informationen im Netz? Die OpenData-Initiative in NRW, die vor einigen Jahren mit einem Sturmesbrausen begann, droht inzwischen, sich in einem lauen Lüftchen zu verlieren.

Noch im letzten Bericht hatte ich Anlass, die Landtagsinitiative "Open Government Strategie für Nordrhein-Westfalen vorantreiben" ausdrücklich zu begrüßen (siehe Bericht 2013 unter 15.1). Die damaligen Pläne klangen verheißungsvoll: So war etwa von der Notwendigkeit des Wandels von der Holschuld der Bürgerinnen und Bürger zur Bringschuld der Verwaltung die Rede gewesen. Dem Aufgabenfeld Open Data und dem Aufbau einer entsprechenden Internetplattform sei eine hohe Priorität einzuräumen. Überdies sei eine Verankerung dieses Veröffentlichungsanspruchs im Informationsfreiheitsgesetz NRW (IFG NRW) sowie die Weiterentwicklung dieses Gesetzes zu einem Transparenzgesetz erforderlich (vgl. LT-Drs. 16/811).

Doch was ist aus dieser Initiative geworden? Im Mai 2013 gab es eine Veranstaltung "#opennrw" im Landtag, die sich eines großen Zuspruchs erfreute, doch seitdem ist es zu meinem Bedauern rund um das Thema "Open Data" stiller geworden. Der Entwurf "Gesetz zur Verwirklichung von Transparenz und Informationsfreiheit im Land Nordrhein-Westfalen" (LT-Drs. 16/3248), den eine Fraktion vorgelegt hatte, fachte – immerhin – im Dezember 2013 noch einmal kurzzeitig die Diskussion an; er erwies sich letztlich jedoch als nicht tragfähig. Es gab einige Anfragen und Anträge, die das Thema streiften – und ansonsten?

Bereits im Dezember 2011 war eine interministerielle Projektgruppe zur Erarbeitung der "Open.NRW-Strategie" eingesetzt worden, die schließlich im März 2014 einen umfangreichen Bericht vorgelegt hat. Die von ihr entwickelte und in dem Papier dargestellte Strategie ist im Mai 2014 vom Kabinett unverändert verabschiedet worden. Zu

hohe Erwartungen werden in dem Bericht selbst jedoch schnell durch die Betonung gemindert, dass sich die Strategie zunächst nur auf die unmittelbare Landesverwaltung (nicht etwa auf alle öffentlichen Stellen in NRW) beziehe und es sich nach wie vor ausschließlich um strategische Überlegungen (im Gegensatz zu konkreten Plänen für eine zeitnahe Umsetzung) handele. Für die Umsetzung, für die es offenbar noch keine konkreten Vorstellungen, aber eine Geschäftsstelle beim Beauftragten der Landesregierung für Informationstechnik (CIO) gibt, ist ein dehnbarer und unbestimmt umschriebener Stufenplan von einigen Jahren vorgesehen.

Auch bei genauerer Durchsicht enthält das Strategiepapier zum Thema "offene Verwaltungsdaten" neben wenigen hoffnungsvollen Ansätzen vor allem Enttäuschungen. Zu begrüßen sind zwar die ausdrücklich aufgeführten "zehn OpenData-Prinzipien für Open.NRW": Vollständigkeit, Primärquelle, zeitnahe Bereitstellung, leichter Zugang, Maschineninterpretierbarkeit, Diskriminierungsfreiheit, Verwendung offener Standards, Lizensierung (ohne Nutzungsbeschränkungen), Dauerhaftigkeit und Kostenfreiheit. Schon das Prinzip der "Vollständigkeit der veröffentlichten Daten" wird jedoch bis auf weiteres nicht zu verwirklichen sein, weil es – und das ist der Kernpunkt meiner Kritik – keinerlei Verpflichtungen zur Veröffentlichung von Daten geben soll. So heißt es vielmehr ausdrücklich: "Für die Open.NRW-Strategie als freiwilliges und proaktives Leistungsangebot der Exekutive ist es nicht erforderlich, das (…) IFG NRW anzupassen. Der individuelle und antragsbedingte Informationsanspruch des IFG NRW steht unbeeinträchtigt neben dem Transparenzangebot der Open.NRW-Strategie. Die Open.NRW-Strategie steht auch in keinem unmittelbaren Zusammenhang mit der Weiterentwicklung des IFG NRW hin zu einem Transparenzgesetz, so wie es der Koalitionsvertrag 2012-2017 zwischen NRWSPD und Bündnis 90 / Die Grünen NRW vorsieht" (Open-NRW-Strategie Teil I, S. 8). Aber wann, wenn nicht jetzt und im Rahmen der "Open.NRW-Strategie", sollen die erforderlichen Veröffentlichungspflichten geschaffen werden?

Bereits in der Vergangenheit – so auch im letzten Bericht unter 15.1 – habe ich wiederholt nachdrücklich darauf hingewiesen, dass die Weiterentwicklung des IFG NRW im Bereich Open Data zum einen notwendig ist, um die Veröffentlichung bestimmter Verwaltungsdatenbestände unabhängig vom Behördenwillen festzuschreiben. Damit

den Bürgerinnen und Bürgern möglichst viele und umfassende Informationsbestände zur Verfügung gestellt werden, darf diese Entscheidung nicht der Disposition der jeweiligen öffentlichen Stellen überlassen bleiben. Ansonsten wäre zu besorgen, dass interessante Informationen gar nicht erst veröffentlicht werden. Zum anderen ist die Weiterentwicklung des IFG NRW erforderlich, soweit durch die Veröffentlichung von Daten in besonders geschützte Belange eingegriffen wird und dies nur auf der Grundlage eines Gesetzes zulässig ist. Mit geeigneten Veröffentlichungspflichten müssen deshalb zugleich korrespondierende gesetzliche Veröffentlichungsbefugnisse einhergehen.

Mit diesen Forderungen befinde ich mich im Einklang mit den Informationsfreiheitsbeauftragten des Bundes und der anderen Länder. So hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland im Jahr 2013 das Positionspapier "Informationsfreiheit und Open Data" verabschiedet und dieses zusammen mit der Entschließung "Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft" veröffentlicht. Aus diesem Jahr stammen auch die Entschließungen "Transparenz bei Sicherheitsbehörden" sowie "Forderung für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!". 2014 folgten die gemeinsamen Entschließungen "Informationsfreiheit nicht Privaten überlassen!" sowie "Open Data muss in Deutschland Standard werden!"(jeweils Abdruck im Anhang). Alle genannten Resolutionen thematisieren Aspekte der Transparenz staatlichen Handelns sowie vor allem auch die Forderung nach Schaffung von gesetzlichen Veröffentlichungspflichten für amtliche Informationen. Letzteres gehört zu den notwendigen Kernbedingungen von "Open Data", und zwar sowohl nach dem nationalen wie auch nach dem internationalen Verständnis dieses Begriffs.

Transparenzregelungen wie beispielsweise § 71a Hochschulgesetz NRW in der neuen Fassung entsprechen noch nicht den Anforderungen an die Schaffung verbindlicher und möglichst konkreter Veröffentlichungspflichten. Nach dieser Vorschrift informiert das Rektorat die Öffentlichkeit in geeigneter Weise über abgeschlossene Vorhaben der Forschung mit Mitteln Dritter. Zwar ist diese Vorschrift grundsätzlich zu begrüßen, soweit sie gegenwärtig eine Verpflichtung zur Information der Öffentlichkeit schafft, die über die bisherige Regelung des IFG NRW hinausgeht. Allerdings gewährt sie dem Rektorat einen großen Entscheidungsspielraum im Hinblick auf die Art und den

Umfang der veröffentlichten Information. Diese Vorschrift bleibt noch deutlich hinter meinen Empfehlungen zurück, klare Veröffentlichungspflichten zu schaffen sowohl für Gutachten und Forschungsergebnisse, die von öffentlichen Stellen in Auftrag gegeben und mit öffentlichen Geldern finanziert worden sind, als auch für Verträge, die öffentliche Stellen mit privaten Unternehmen oder Personen schließen (siehe etwa Bericht 2013 unter 15.1). Derartige Regelungen sollten nach Möglichkeit zudem aus Gründen der Übersichtlichkeit im IFG NRW selbst getroffen werden.

➧ Nicht alles, was auf den ersten Blick glänzt, ist Gold. In diesem Sinne wird die "Open.NRW-Strategie" erst noch beweisen müssen, dass der immense Aufwand ihrer Entwicklung durch eine zeitnahe und gelungene Umsetzung der Ideen in die Praxis gerechtfertigt ist. Dabei darf jedoch auf keinen Fall darauf verzichtet werden, endlich die erforderlichen gesetzlichen Veröffentlichungspflichten zu schaffen.

12.2 Das "1 x 1 des IFG-Antrags"

Das Antragsverfahren nach dem Informationsfreiheitsgesetz NRW (IFG NRW) ist einfach und niederschwellig ausgestaltet. Insbesondere enthält es keine gesetzlichen Formvorschriften, die von informationssuchenden Personen zu beachten wären. Dennoch kommt es bei der Antragstellung immer wieder zu Problemen und Enttäuschungen, die sich mit wenig Aufwand leicht vermeiden lassen.

Bürger B. ärgert sich, weil er bereits vor mehr als einem Monat per E-Mail einen Antrag auf Informationszugang bei seiner Gemeinde gestellt hat. Er wartet dringend darauf, die von ihm beantragten Informationen endlich zu erhalten, denn er ist politisch interessiert und engagiert. Auf seinen Antrag hat er nach Ablauf eines Monats noch keine Antwort erhalten. Empört ruft er nun bei der Gemeinde an und muss feststellen, dass sein Antrag dort überhaupt nicht vorliegt.

Bürgerinnen und Bürger wie Herr B. wenden sich häufig an meine Behörde, weil sie von der öffentlichen Stelle überhaupt keine Reaktion erhalten haben. In einer Vielzahl dieser Fälle werden die Anträge

– wie nach dem IFG NRW ausdrücklich zulässig – elektronisch gestellt. Die Absenderin oder der Absender sollte daher immer stutzig werden, wenn die öffentliche Stelle auf die E-Mail noch nicht einmal eine Eingangsbestätigung versendet, und nachfragen, ob der elektronisch gestellte Antrag die Stelle überhaupt erreicht hat. Fehlerquellen können hierbei etwa veraltete E-Mail-Adressen, Schreibfehler oder SPAM-Ordner der öffentlichen Stelle sein.

Nach dem Telefonat mit der Gemeinde überprüft Herr B. die Angaben in seiner ursprünglichen E-Mail und stellt fest, dass er eine veraltete E-Mail-Anschrift der Gemeinde verwendet hatte. Er übersendet den Antrag noch einmal an die richtige E-Mail-Adresse und erhält diesmal sogleich eine Eingangsbestätigung. Die Sachbearbeiterin S. der Gemeinde wundert sich indes, weshalb die nunmehr eingegangene E-Mail des Herrn B. solch "merkwürdige" Fragen enthält. So möchte er beispielsweise wissen, warum die Gemeinde bestimmte Entscheidungen (die ihn und sein Lebensumfeld gar nicht unmittelbar berühren) getroffen hat, welche Kosten diese Entscheidungen verursacht haben und aus welchen Gründen dieses Geld nicht besser für ein anderes Vorhaben aufgewendet wurde. In der Vergangenheit hatte Frau S. einen Herrn B. betreffenden Vorgang doch zu seiner vollsten Zufriedenheit bearbeitet – was will er also noch? Pflichtbewusst und ein wenig pikiert verweist Frau S. in ihrem Antwortschreiben lapidar auf ihre rechtlich zutreffende Sachentscheidung in der damaligen Angelegenheit und sieht im Übrigen keinerlei Veranlassung, auf seine Fragen einzugehen.

Das IFG NRW ist nicht allen Beschäftigten öffentlicher Stellen stets gegenwärtig; viele haben – wie Frau S. – nur selten oder nie einen IFG-Antrag zu bearbeiten. Für einen erfolgreichen Informationszugang empfehle ich daher vorsorglich, den Antrag unter ausdrücklichem Hinweis auf das IFG NRW zu stellen.

Als Herr B. die Antwort von Frau S. erhält, ist für ihn das Maß voll: Er wiederholt seinen Antrag ein weiteres Mal und verweist nun ausdrücklich auf das IFG NRW. Weil er einmal dabei und ohnehin in Rage ist, begründet er seinen Antrag zudem in einem fünfseitigen Schreiben, in dem er zugleich seine politischen Auffassungen und Forderungen zum Ausdruck bringt. Den Abschluss dieses Schriftsatzes bildet eine Dienstaufsichtsbeschwerde gegen Frau S., die seine demokratischen Rechte missachtet habe. Frau S. versteht inzwischen

die Welt nicht mehr und ist mit ihren Nerven am Ende, als sie bei ihrer Vorgesetzten in dieser Angelegenheit eine Rücksprache hat. Es gelingt den beiden nach längerer intensiver Durchsicht des inzwischen umfangreichen Schriftverkehrs, das informationsfreiheitsrechtliche Begehren des Herrn B. zu ermitteln. Diesem wird sodann im Anschluss an die Rücksprache auch prompt Rechnung getragen: Herr B wird – wie beantragt – über die Kosten der von ihm angesprochenen Entscheidungen informiert. Im Übrigen wird sein Antrag abgelehnt, weil es sich nicht um Informationen im Sinne des IFG NRW handelt.

Für öffentliche Stellen ist es oftmals schwierig, wenn IFG-Anträge umfangreiche Erläuterungen oder politischen Forderungen enthalten, die zur Bearbeitung des Anliegens weder erforderlich noch dienlich sind. Das eigentliche Informationsbegehren tritt so manchmal in den Hintergrund, und es entsteht das Risiko, dass berechtigte Anträge bei der Bearbeitung schlichtweg verkannt werden. Die Anträge auf Informationszugang sollten daher klar, eindeutig und auf das für die Bearbeitung Wesentliche beschränkt formuliert werden. Nur so kann der Informationszugang nach Maßgabe des IFG NRW ohne unnötigen Reibungsverlust erfolgen.

Auch wenn Herr B. zufrieden ist, dass er endlich eine inhaltliche Antwort auf seine IFG-Anträge erhalten hat, und seine Dienstaufsichtsbeschwerde bereits ein wenig bereut, hält das Schreiben der Frau S. gleichwohl eine kleine Enttäuschung für ihn bereit: Schließlich bleiben die Fragen, warum bestimmte Entscheidungen getroffen wurden, ausdrücklich unbeantwortet, und der Bürgermeister gibt zu den Ausführungen des Herrn B. auch kein politisches Statement ab. Derartige Erklärungen kann Herr B. allerdings nach Maßgabe des IFG NRW auch nicht beanspruchen: Das Gesetz eröffnet ausschließlich einen Anspruch auf die bei einer öffentlichen Stelle vorhandenen amtlichen Informationen sowie auf eine nachvollziehbare Begründung für den Fall der Ablehnung eines IFG-Antrags. Im Übrigen sind die öffentlichen Stellen jedoch weder dazu verpflichtet, Erläuterungen zu den herausgegebenen Informationen oder sonstige Stellungnahmen abzugeben, noch haben sie zu prüfen, ob die herausgegebenen Informationen inhaltlich richtig sind.

➧ Bürgerinnen und Bürger können selbst dazu beitragen, dass Anträge nach dem IFG NRW von den

Behörden als solche erkannt und zügig bearbeitet werden können. Klar formulierte Informationsbegehren können auch klar beschieden werden. Nur so kann es in der Praxis gelingen, dass das IFG NRW seinen Beitrag zur behördlichen Transparenz leistet.

12.3 Überfragt zu "fragdenstaat"?!

Gelegentlich werden Anträge nach dem Informationsfreiheitsgesetz NRW (IFG NRW) mittels der Internetplattform "fragdenstaat.de" gestellt. So manche öffentliche Stelle ist verunsichert.

Die Internetplattform "fragdenstaat.de" versteht sich als Unterstützungsangebot für informationssuchende Bürgerinnen und Bürger. Durch sie soll den Informationssuchenden die Stellung eines IFG-Antrags erleichtert und eine etwaige "Schwellenangst" genommen werden. So sollen letztlich mehr Personen zur Antragstellung ermutigt werden. Nicht immer gestaltet sich die Bearbeitung dadurch schneller. Manche Behörde meint – im Gegenteil – neue Zugangshindernisse auszumachen.

- Die informationssuchende Person ist nicht sicher identifizierbar

Über die Internetplattform "fragdenstaat.de" ist es möglich, anonyme oder pseudonyme Anträge auf Informationszugang zu stellen. Viele öffentliche Stellen lehnen die Bearbeitung solcher Anträge ab, solange keine postalische bzw. zustellungsfähige Adresse mitgeteilt wird. Dieses Vorgehen ist unzulässig: Da der freie Zugang zu Informationen als wesentlicher Bestandteil des Demokratie- und Rechtsstaatsprinzips gesehen wird und die Kontrollmöglichkeiten der Bürgerinnen und Bürger gegenüber dem Staat gestärkt werden sollen, hat der Gesetzgeber bewusst geringe Anforderungen an die Antragstellung nach dem IFG NRW gestellt. Gesetzlich sind sowohl mündliche als auch elektronische Anträge vorgesehen. Der Gesetzgeber hat demnach gezielt und gewollt zwei Antragsarten zugelassen, bei denen eine sichere Identifizierung der oder des Antragstellenden zunächst ausgeschlossen ist. Grundsätzlich ist die Möglichkeit anonymer oder pseudonymer Anträge im Übrigen auch deshalb sinnvoll und wichtig,

um eventuellen negativen Folgen für die Antragstellenden vorzubeugen.

Entscheidend ist jedoch Folgendes: Aus Gründen des Datenschutzes darf die verantwortliche Stelle die Postanschrift der Antragstellerinnen und -steller nur dann ermitteln, wenn es zu ihrer Aufgabenerfüllung erforderlich ist. Dass zum Beispiel die Erteilung eines förmlichen Ablehnungsbescheides die Angabe einer Postanschrift erfordert, stellt kein durchgreifendes Argument dafür dar, bereits die Zulässigkeit eines Antrags von der Angabe einer zustellungsfähigen Adresse abhängig zu machen. Ob ein Informationsanspruch ganz oder teilweise abgelehnt werden muss, dürfte regelmäßig bei Antragstellung noch nicht feststehen, so dass diese Erwägung kein Grund für eine Identifizierung sein kann. Ist dem Antrag stattzugeben, kann die gewünschte Information in der Regel erteilt werden, ohne dass es hierzu der Angabe einer Postanschrift bedarf. In diesen Fällen ist die Feststellung der Identität der Antragstellenden für die Aufgabenerfüllung der öffentlichen Stelle nicht erforderlich und somit unzulässig.

Etwas anderes gilt, wenn die Gewährung eines Informationszugangs einen Gebührentatbestand nach der Verwaltungsgebührenordnung zum IFG NRW auslöst. Ein Gebührenbescheid wird erst wirksam, wenn er der Person, für die er bestimmt ist, bekanntgegeben wird. Damit der Gebührenbescheid im Zweifel auch vollstreckt werden kann muss nachweisbar sein, dass der Bescheid ordnungsgemäß bekanntgegeben wurde, er folglich seine Adressatin oder seinen Adressaten erreicht hat. Auch eine eventuelle Vollstreckung der Gebührenforderung ist nur bei Kenntnis des Namens und der Anschrift der informationssuchenden Person möglich. In diesem Fall ist es für die Aufgabenerfüllung der öffentlichen Stelle daher erforderlich, den Namen und die Adresse der oder des Informationssuchenden zu erfahren.

Demgegenüber kann die Ablehnung eines Antrags der informationssuchenden Person zunächst per E-Mail mitgeteilt werden. Soweit letztere in diesem Zusammenhang auf Nachfrage die Mitteilung einer postalischen Anschrift zur Erteilung eines förmlichen Ablehnungsbescheids verweigert, kann ihr ein solcher eben nicht zugestellt werden und ihr stehen damit keine weiteren Rechtsschutzmöglichkeiten zur Verfügung, worauf sie von der verantwortlichen Stelle hingewiesen werden sollte.

Auf materieller Ebene kann die Identifizierbarkeit des Informationssuchenden in Ausnahmefällen erforderlich sein. Gemäß § 9 Abs. 1 Buchstaben a) und e) IFG NRW können grundsätzlich zu schützende personenbezogene Daten offenbart werden, wenn die betroffene Person entweder in die Offenlegung eingewilligt hat oder die Antragstellerin oder der Antragsteller ein rechtliches Interesse an der begehrten Information geltend macht und überwiegende schutzwürdige Belange der betroffenen Person der Offenbarung nicht entgegenstehen. Eine Einwilligung kann nur dann wirksam erteilt werden, wenn der betroffenen Person alle maßgeblichen Aspekte der Offenlegung bekannt sind; dazu gehört grundsätzlich auch, welche Person die Offenlegung begehrt, es sei denn, die betroffene Person erklärt sich allgemein mit der Offenlegung der sie konkret betreffenden personenbezogenen Daten einverstanden. Im Rahmen des § 9 Abs. 1 Buchstabe e) IFG NRW hat die öffentliche Stelle unter anderem zu prüfen, ob die antragstellende Person ein rechtliches Interesse an der Kenntnis der begehrten Information geltend machen kann. Auch hier ist die Identität der oder des Informationssuchenden maßgeblich. Soweit es hingegen auf die Verweigerungsgründe des § 9 IFG NRW nicht ankommt, kann die fehlende Identifizierbarkeit oder die fehlende Postanschrift nicht zur Ablehnung des Antrags führen.

- Veröffentlichung der Information auf der Internetplattform wird untersagt

Vielfach weisen öffentliche Stellen darauf hin, dass sie einer Veröffentlichung der Informationen im Internet widersprechen. Dies läuft jedoch den Intentionen des Gesetzgebers zuwider, einen möglichst weitreichenden und (fast) voraussetzungslosen Informationsanspruch zum Zwecke der Informationsweitergabe um ihrer selbst willen zu schaffen. Wurde einem Informationsantrag entsprochen, steht es den Antragstellerinnen und Antragstellern grundsätzlich frei, wie sie mit diesen Informationen weiter verfahren. Eine Weitergabe im privaten Rahmen ist dabei ebenso zulässig wie die Einstellung der Informationen ins Internet. In diesem Sinne hat auch das OVG NRW bereits mit Beschluss vom 19. Juni 2002 (Az. 21 B 589/02) ausgeführt, es sei ausgeschlossen, dass der Gesetzgeber die nahe liegende Möglichkeit der Verwendung erlangter Informationen – sei es zum rechtlichen oder wirtschaftlichen Vorteil der oder des Informationssuchenden, sei es zum rechtlichen oder wirtschaftlichen Nachteil der öffentlichen

Stelle oder einer bzw. eines Dritten – nicht gesehen habe. Dies habe er jedoch nicht zum Anlass genommen, einen entsprechenden allgemeinen Ablehnungsgrund in das Gesetz aufzunehmen. Eine solche Untersagung ist somit unzulässig.

➧ Bei Angeboten wie "fragdenstaat.de" handelt es sich im Kern um "alten Wein in neuen Schläuchen". Viele Fragestellungen lassen sich mit den grundsätzlichen Erwägungen zu Datenschutz und Informationsfreiheit lösen.

12.4 Informationsfreiheitsgesetz und Einsichtsrechte nach anderen Normen

Meine Behörde wird immer wieder mit Fallgestaltungen befasst, in denen ein Informationszugang mit Blick auf Spezialregelungen verweigert wird.

So beantragte ein Mitglied der Vertreterversammlung einer Kassenzahnärztlichen Vereinigung (KZV) bei deren Vorstand Einsicht in einen Geschäftsvorgang. Dieser lehnte den Antrag mit dem Argument ab, die Einsichtsregelung des § 79 Abs. 3 Satz 2 Sozialgesetzbuch – Fünftes Buch (SGB V) erlaube die Einsicht in Geschäftsvorgänge nur "der Vertreterversammlung", nicht jedoch einem einzelnen Mitglied. Es handele sich um eine das Informationsfreiheitsgesetz NRW (IFG NRW) ausschließende besondere Rechtsvorschrift im Sinne des § 4 Abs. 2 IFG NRW.

Meine Behörde wies darauf hin, dass dies nicht der Fall ist: § 79 Abs. 3 Satz 2 SGB V sieht vor, dass die Vertreterversammlung sämtliche Geschäfts- und Verwaltungsunterlagen einsehen und prüfen kann. Die Akteneinsichtsregelung begünstigt somit spezifische Personen bzw. eine Personenmehrheit. In einem solchen Fall ist zu prüfen, ob daneben auch für andere Personen ein Anspruch nach dem IFG NRW in Betracht kommt. Dies wäre – wie auch das OVG NRW in ständiger Rechtsprechung ausführt – nur dann nicht der Fall, wenn ein umfassender Informationsanspruch dem Schutzzweck des Spezialgesetzes zuwider laufen würde. Das lässt sich hier jedoch nicht feststellen: Sinn und Zweck der vorgenannten Regelung ist es, die Vertreterversammlung mit allen notwendigen Kenntnissen auszustatten, welche für die Wahrnehmung und Ausübung der Rechte und

Pflichten der Vertreterversammlung notwendig sind. Es ist nicht ersichtlich, dass es diesem Schutzzweck zuwider liefe, wenn einzelne Personen darüber hinaus ein Einsichtsrecht erhalten. Vielmehr dient eine weitergehende Information einzelner Mitglieder der Vertreterversammlung oder aber auch unbeteiligter Dritter gerade dazu, die Rechtmäßigkeit der Vorstandstätigkeit prüfen zu können. Schließlich lässt sich der Vorschrift nicht entnehmen, dass ein allgemeiner Informationsanspruch auf der Grundlage des IFG NRW ausgeschlossen sein soll.

Die KZV hielt jedoch an ihrer Rechtsauffassung fest und trug auch keine anderen nachvollziehbaren Verweigerungsgründe vor, so dass das Verhalten der Organisation zu beanstanden war.

➡ Vielfach werden Zugangsanträge nach dem IFG NRW wegen anderer, vermeintlich verdrängender Normen abgelehnt, obwohl die Anforderungen an eine besondere Rechtsvorschrift im Sinne des § 4 Abs. 2 IFG NRW selten erfüllt sind.

12.5 Verbandsempfehlungen zur Höhe von Vorstandsgehältern müssen offengelegt werden

Wegen des vermeintlichen "Schutzes der Persönlichkeitsrechte der Vorstandsmitglieder" wurde einem Antragsteller der Zugang zu den Verbandsempfehlungen zur Höhe der Vorstandsgehälter durch einen Sparkassenverband vorenthalten.

Meine Prüfung ergab, dass die Verbandsempfehlungen offenzulegen sind, da diese keine schutzwürdigen personenbezogenen Daten enthalten (siehe Bericht 2013 unter 15.3). Trotz Empfehlung und Beanstandung wurden die Informationen nicht offengelegt.

Nunmehr hat das Verwaltungsgericht Düsseldorf mit rechtskräftigem Urteil meine Auffassung bestätigt und den Sparkassenverband zur Offenlegung der Vergütungsempfehlungen verpflichtet (Urteil vom 23. November 2012 – 26 K 1846/12 –). Auch das Gericht sah keine personenbezogenen Daten betroffen, da sich aus den allgemeinen Empfehlungen nicht ergebe, welcher Vorstand tatsächlich welches Gehalt bezöge, selbst wenn man davon ausginge, dass den Empfehlungen regelmäßig entsprochen würde.

➧ Die Ablehnung des Zugangsantrags war sachlich nicht begründet. Der Antragsteller konnte seinen Anspruch auf dem Rechtsweg durchsetzen.

12.6 Informationszugang auch bei privatrechtlichem Handeln einer Behörde

Eine Stadt verweigert die Einsicht in privatrechtliche Verträge mit dem Argument, es handele sich nicht um Verwaltungstätigkeit. Erstaunlich – ist diese Problematik doch schon seit nunmehr über zwölf Jahren obergerichtlich geklärt.

Ein Antragsteller beantragte bei einer Stadt die Einsicht in Pachtverträge von Sportlerheimen. Die Stadt lehnte diesen Antrag ab und trug vor, bei den privatrechtlich abgeschlossenen Verträgen handele es sich nicht um Verwaltungstätigkeit der Stadt, so dass kein Anspruch nach dem Informationsfreiheitsgesetz NRW (IFG NRW) bestünde. Zur Begründung berief sie sich auch auf Anwendungshinweise des Innenministeriums NRW.

Meine Behörde hat die Stadt mehrfach darauf hingewiesen, dass die Handlungsform der öffentlichen Stelle – sei sie nun privatrechtlich oder öffentlich-rechtlich – für die Frage des Vorliegens von "Verwaltungstätigkeit" irrelevant ist. Das IFG NRW definiert als Behörde im Sinne des Gesetzes "jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt". Es stellt nicht auf die Rechtsform der Tätigkeit ab, sondern allein darauf, dass die Tätigkeit sich als Wahrnehmung einer im öffentlichen Recht wurzelnden Verwaltungsaufgabe – im Gegensatz zu Rechtsprechung und Rechtsetzung – darstellt. In welcher Rechtsform die Verwaltungsaufgabe erfüllt wird, ist unerheblich. Bereits im Jahre 2002 wurde dies vom Oberverwaltungsgericht NRW entschieden. Auch die von der Stadt benannten Anwendungshinweise des Innenministeriums NRW stützen die Behauptung der Stadt keineswegs.

Trotz der Hinweise meiner Behörde setzte sich die Stadt mit dieser eindeutigen Rechtslage nicht weiter auseinander, sondern verwies den Antragsteller lediglich auf sein Klagerecht. Auch die notwendige Prüfung der Verweigerungsgründe "ersparte" sich die Stadt so. Dies stellt einen klaren Verstoß gegen das IFG NRW dar und musste beanstandet werden.

- Manche öffentlichen Stellen lehnen Informationszugangsanträge ohne ausreichende Begründung ab und verweisen die Antragstellerinnen und Antragsteller stattdessen auf ihr Klagerecht. Dieses Verhalten stellt eine Missachtung der Auskunftsrechte der Bürgerinnen und Bürger nach dem IFG NRW dar.

12.7 "Vorgeschobene" Antragstellerin?

Eine Stadt verweigert einer Antragstellerin den Zugang zu Informationen. Als Grund gibt sie an, die Detailkenntnis des Antrags spreche dafür, dass eigentlich der - bei einer anderen Kommune beschäftigte – Ehemann der Antragstellerin hinter dem Antrag stehe und der Antrag letztlich im Interesse der anderen Kommune gestellt sei.

Die Antragstellerin begehrt Auskünfte zu einer Kooperation der Stadt mit einer Bäderbetriebsgesellschaft. Da ihr Ehemann in gleicher Thematik bei einer anderen Kommune beschäftigt ist und die Fragen eine umfangreiche Sachkenntnis erkennen ließen, unterstellt die Stadt, die Antragstellerin sei von ihrem Ehemann "vorgeschoben" worden, um ihm Informationen für die andere Kommune oder die dort tätige Bäderbetriebsgesellschaft zu verschaffen. Der Antrag wurde deshalb mit dem Argument abgelehnt, bei der Antragstellerin handele es sich nicht um eine natürliche, sondern um eine juristische Person, so dass ihr die Antragsberechtigung fehle.

Die Stadt habe ich darüber unterrichtet, dass diese Ablehnungsbegründung nicht trägt: Die Antragstellerin hat den Antrag im eigenen Namen gestellt. Selbst wenn der mit dem Thema beruflich befasste Ehemann die Fragen für Zwecke der anderen Kommune formuliert haben sollte, wäre dies nach dem Sinn und Zweck des Informationsfreiheitsgesetzes NRW (IFG NRW) unerheblich, weil das IFG NRW einen sich auf ein "Vorschieben" beziehenden Ablehnungsgrund nicht kennt. Auch enthält das Gesetz keinerlei Einschränkung hinsichtlich der Verwendung zugänglicher Informationen. Inwieweit eine informationssuchende natürliche Person eine Information für eine juristische Person verwenden könnte, spielt somit prinzipiell keine Rolle. Das Gesetz gewährt vielmehr einen voraussetzungslosen, von einem – wie auch immer gearteten – Informationsinteresse unabhängigen

Zugangsanspruch. Es ist daher grundsätzlich ohne Belang, wozu die Antragstellerin oder der Antragsteller die Information benötigt. Insofern ist eine Antragstellung durch eine natürliche Person auch dann nicht als rechtsmissbräuchlich anzusehen, wenn sie mutmaßlich im überwiegenden oder gar alleinigen Interesse einer juristischen Person erfolgt. Einer Antragstellerin kann das durch § 4 Abs. 1 IFG NRW gewährte allgemeine Bürgerrecht auf Information nicht schon deshalb genommen werden, weil ihr Ehemann für eine juristische Person tätig ist, die mit dem Informationsgegenstand in irgendeiner Weise in Beziehung steht.

Trotz Empfehlung und Beanstandung meinerseits zeigt die Stadt jedoch kein Einsehen und verweigert den beanspruchten Informationszugang bis heute.

➧ Die Stadt mag ihre Gründe haben, die gewünschten Informationen nicht herauszugeben. Rechtlich zu begründen und zu rechtfertigen ist diese Ablehnung jedoch nicht. Trotz meiner Beanstandung verbleibt die Stadt hartnäckig bei ihrer Rechtsauffassung und verstößt damit fortgesetzt gegen die Regelungen des IFG NRW.

12.8 Ungebührliche Gebühren?

Eine Kreisverwaltung macht die Übersendung von internen Arbeitsanweisungen an einen Arbeitslosengeld-II-Bezieher von der Vorauszahlung einer Gebühr in Höhe von 100 Euro anhängig.

Ein Antragsteller beanspruchte von seinem Jobcenter interne Arbeitsanweisungen zu den Kosten der Unterkunft und Heizung. Auf Weisung des Kreises sollte das Jobcenter nicht selbst über den Antrag entscheiden, sondern musste diesen der Kreisverwaltung zur Beantwortung vorlegen. Letztere stellte die Übersendung der beantragten Unterlagen in Aussicht, sobald eine Gebührenvorauszahlung in Höhe von 100 Euro entrichtet sei – sehr viel Geld (nicht nur) für den Arbeitslosengeld-II-Bezieher.

Auf meine Nachfrage, wie die Erhebung der Gebühr begründet werde, wurde lediglich darauf hingewiesen, dass sich die Gebühr am unteren Gebührenrahmen bewege. Die Gebührenvorauszahlung sei aufgrund

einer Regelung im Gebührengesetz NRW möglich. Auch sei die Gebührenhöhe trotz der geringen Arbeitslosengeld-II-Bezüge nicht unverhältnismäßig.

Eine inhaltliche Begründung, warum durch die Übersendung der Arbeitsanweisungen ein so erheblicher Verwaltungsaufwand entstanden sein soll, der den Gebührentatbestand erfüllt, wurde trotz mehrmaliger Aufforderung nicht mitgeteilt. Da bereits eine Begründung für die Gebührenerhebung als solche sowie die Prüfung einer Ermäßigung oder Befreiung von der Gebührenpflicht fehlten, habe ich eine Beanstandung ausgesprochen.

➧ Die Gebühr darf nicht dem Zweck dienen, Bürgerinnen und Bürger von der Wahrnehmung ihres Rechts auf Informationszugang abzuschrecken.

12.9 Manchen ist kein Argument zu schade

Eine Stadt berief sich zur Ablehnung eines Informationszugangsantrags auf nichts Geringeres als die Europäische Menschenrechtskonvention (EMRK).

Ein Antragsteller begehrte von einer Stadt die Offenlegung von Sitzungsprotokollen eines so genannten "Energiebeirats". Dabei handelt es sich um ein von einem Energieunternehmen geschaffenes Gremium, in dem auch Beschäftigte der Stadt vertreten sind. Die Stadt lehnte die Offenlegung mit dem Argument ab, der "Energiebeirat" sei Teil des Energieunternehmens; da dieses keine öffentliche Stelle sei und die Sitzungen nicht öffentlich seien, bestünde kein Zugangsanspruch.

Ich habe die Stadt darauf hingewiesen, dass für einen Zugangsanspruch allein maßgeblich sei, dass die beantragten Unterlagen bei der Stadt vorhanden seien. Ob das Gremium von einer juristischen Person gegründet worden sei, sei für den Anspruch nach dem Informationsfreiheitsgesetz NRW (IFG NRW) irrelevant.

Daraufhin teilte die Stadt mit, dass schwerwiegende Geheimschutzinteressen des Energieunternehmens einem Informationszugang entgegenstünden. Nach Art. 8 der EMRK, der sinngemäß auch für juristische Personen gelte, habe jede Person ein Recht auf Achtung ihrer Privatinteressen. Eine Behörde dürfe in die Ausübung dieses Rechts

nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sei für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Da diese Voraussetzungen nicht vorlägen, könne dem Zugangsanspruch nicht entsprochen werden.

Meine Behörde stellte klar, dass der vorliegende Antrag allein anhand der im IFG NRW selbst geregelten Verweigerungsgründe zu prüfen sei. Eine Antragsablehnung aus anderen rechtlichen Erwägungen, wie hier der EMRK, komme nicht in Betracht. Sollten ggf. personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse zu schützen sein, würde dem durch die Regelungen der §§ 8 und 9 IFG NRW hinreichend Rechnung getragen. In einem solchen Fall müsse jedoch nachvollziehbar dargelegt werden, warum der Zugang nicht gewährt werden könne. Zwar bedürfe es keiner bis in die Einzelheiten gehenden Begründung, weshalb die Offenbarung beispielsweise von Betriebs- und Geschäftsgeheimnissen nicht möglich sei, weil dann die schützenswerten Daten durch eben diese Begründung doch noch offenbart werden könnten. Ein gänzlicher Verzicht auf eine inhaltliche Begründung der Ablehnung stelle indes einen Verstoß gegen § 5 Abs. 2 Satz 3 IFG NRW dar.

Da die Stadt trotz mehrmaliger Aufforderung und Beratung keine hinreichende Begründung vortrug, war ihr Verhalten zu beanstanden.

➧ Eine Antragsablehnung kann nur auf die im IFG NRW selbst geregelten Verweigerungsgründe gestützt und muss nachvollziehbar begründet werden.

Anhang

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

85. Konferenz vom 13./14. März 2013

◆ Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

◆ Soziale Netzwerke brauchen Leitplanken - Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe "Soziale Netzwerke" erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

◆ Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

◆ Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.
- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.
- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.
- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.
- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.
- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.

- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.
- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.
- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.
- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

86. Konferenz vom 1./2. Oktober 2013

◆ Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung "Sicherheit bei E Government durch Nutzung des Standards

OSCI" Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

◆ Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von "gläsernen Patientinnen und Patienten oder Versicherten" weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.
- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.
- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

◆ Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung "Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

◆ Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt - wie repräsentative Studien belegen - mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.
- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.
- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z.B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

87. Konferenz vom 27./28. März 2014

◆ Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle ("One-Stop-Shop") vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen. Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob

die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.

6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

◆ Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke - Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürger n steigt das Interesse von Strafverfolgungsbehörden, dies e sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 20 13 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z.B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegender er Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies - ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen - nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Net z werken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen

werden kann. - In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret an zugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken u m fassen soll.

- Es ist sicherzustellen, dass
  - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,
  - die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
  - die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

◆ Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wiederherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung). Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o.g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

◆ Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet - Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i.S.d. § 4a BDSG rechtmäßig erfolgen .
- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Abs. 3 BDSG, entspricht.
- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckt en Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

◆ Beschäftigtendatenschutz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung "in angemessener Zeit" lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

◆ Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: "Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen." In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität d er Kontrolle einschränken. Für den Bereich der Telekommunika-

tionsüberwachung nach dem Gesetz zur Beschränkung des Brief - , Post - und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

88. Konferenz vom 8./9. Oktober 2014

◆ Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Vorsetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend vor. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes- und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.
- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem vor, dass die BfDI als künftige oberste Bundesbehör-

de mit reichenden personellen und sächlichen Mitteln gestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.

- Die Genehmigung, als Zeugin zusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt.
- Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite nahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden reichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

◆ Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs - und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3, 1 Mrd. US-Dollar das Werbeunternehmen Double - Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von

"Big Data" erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann. Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

◆ Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C - 131/12 "Google Spain" einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen

zu entscheiden. Die se Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihr er Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung üb er die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

◆ Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen. • Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein.

Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Entschließungen zwischen den Konferenzen:

◆ 25. Januar 2013 - Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.
- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.
- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.
- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.

- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

◆ 05.09.2013 - Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u.a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es "zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen ein-setzen muss", "dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf". Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmelde-

geheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.

- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.
- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.
- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

  Dazu gehört,

  - zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.
  - sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.
  - die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.
- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.
- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

◆ 14.11.2014 - Keine Pkw-Maut auf Kosten des Datenschutzes

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordern die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-) elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monate währende - Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weisen sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

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

Beschluss vom 26./27. Februar 2013

◆ Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines "stillen Alarms" oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbst tätig (z.B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Ei ne Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

Beschluss vom 11/12 September 2013

◆ Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z.B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss

(vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

Beschluss vom 27. Januar 2014

◆ Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressenten"

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe "Einholung von Selbstauskünften bei Mietinteressenten" zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird – ohne Anspruch auf Vollständigkeit – dargestellt, was zulässig ist.

Beschlüsse vom 25./26. Februar 2014

◆ Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierungentwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,
- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,
- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,
- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

◆ Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht-öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras- jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt - datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (BDSG) ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

Beschluss vom Mai 2014

◆ Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online-mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.
2. Soweit Web-oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:
   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.
   - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat.

- Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z.B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
- Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips "privacy by default": Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die RedButton-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.
4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige WebDienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Entschließung vom 28. November 2013

◆ Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!

Der freie Zugang der Bürgerinnen und Bürger der Bundesrepublik Deutschland zu den Informationen der öffentlichen Stellen muss auch in Deutschland ein fester Bestandteil der verfassungsrechtlich garantierten Rechte werden. Transparenz ist eine

wesentliche Grundlage für eine funktionierende freiheitlich demokratische Gesellschaft. Sie ist der Nährboden für gegenseitiges Vertrauen zwischen staatlichen Stellen und den Bürgerinnen und Bürgern.

Es reicht nicht aus, dass Informationen nur auf konkreten Antrag hin herauszugeben sind. In Zukunft sollten öffentliche und private Stellen, die öffentliche Aufgaben wahrnehmen, verpflichtet sein, Informationen von sich aus zur Verfügung zu stellen. Auf diese Weise wird der Zugang zu Informationen für alle erleichtert und der Aufwand der Informationserteilung reduziert.

Die Bundesrepublik Deutschland muss jetzt die nötigen gesetzlichen Regelungen für ein modernes Transparenzrecht schaffen, um mit den internationalen Entwicklungen Schritt zu halten und die Chancen der Transparenz wahrzunehmen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher alle Beteiligten in Bund und in den Ländern auf, sich für die Stärkung der Transparenz auf nationaler, europäischer und internationaler Ebene einzusetzen.

Sie fordert insbesondere:

- den Anspruch auf freien Zugang zu amtlichen Informationen endlich in alle Verfassungen aufzunehmen, einen gesetzlich geregelten effektiven Schutz von Whistleblowern, die über Rechtsverstöße im öffentlichen und nicht-öffentlichen Bereich berichten,
  - ein einheitliches Informationsrecht zu schaffen, das die Regelungen des Informationsfreiheitsgesetzes, des Umweltinformationsgesetzes und des Verbraucherinformationsgesetzes in einem Gesetz zusammenfasst, dass das Informationsfreiheitsrecht im Sinne eines Transparenzgesetzes mit umfassenden Veröffentlichungspflichten nach den Open-Data-Grundsätzen weiterentwickelt wird,
  - aus der vom Bundestag in Auftrag gegebenen Evaluation des Bundesinformationsfreiheitsgesetzes die notwendigen Konsequenzen zu ziehen und die Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß zu beschränken,

- die Bereichsausnahme für die Nachrichtendienste abzuschaffen, die entsprechende Ausnahmeregelung auf konkrete Sicherheitsbelange zu beschränken und den Umgang mit Verschluss-Sachen gesetzlich in der Weise zu regeln, dass die Klassifizierung von Unterlagen als geheimhaltungsbedürftig regelmäßig von einer unabhängigen Instanz überprüft, beschränkt und aufgehoben werden kann,
- Transparenz der Kooperationen auch zwischen privaten und wissenschaftlichen Einrichtungen sicherzustellen, die im Rahmen der Wahrnehmung öffentlicher Aufgaben für staatliche Stellen tätig sind. Dies gilt auch und insbesondere für Sicherheitsbehörden.
- die Berliner Erklärung der 8. Internationalen Konferenz der Informationsfreiheitsbeauftragten zur Stärkung der Transparenz auf nationaler und internationaler Ebene vom 20. September 2013, insbesondere die Anerkennung eines Menschenrechts auf Informationszugang im Rahmen der Vereinten Nationen, den Beitritt der Bundesrepublik zur Open Government Partnership und zur Tromsö-Konvention des Europarats (Konvention des Europarates über den Zugang zu amtlichen Dokumenten) umzusetzen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland bietet ihre Unterstützung an.

Entschließungen vom 27. Juni 2013

◆ Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!

Die gesellschaftlichen Erwartungen an einen transparenten Staat gehen inzwischen weit über das bisherige Recht der Bürgerinnen und Bürger, einen Antrag auf Informationszugang zu stellen, hinaus. Open Data – also die aktive Bereitstellung öffentlicher

Informationen im Internet – wird auf den ersten Portalen bereits praktiziert. Zahlreiche Projekte befinden sich im Aufbau. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt diese Entwicklungen ausdrücklich und formuliert in einem Positionspapier wesentliche Anforderungen an eine moderne Transparenzgesetzgebung.

Die Konferenzhält Regelungen in den Informationsfreiheits- und Transparenzgesetzen für erforderlich. Diese müssen um geeignete Instrumente zur Veröffentlichung von Informationen ergänzt werden. Datenbestände öffentlicher Stellen dürfen grundsätzlich nicht durch Urheberrecht oder Nutzungsbeschränkungen blockiert werden. Um Urheberrechten Dritter Rechnung zu tragen, sollten öffentliche Stellen mit diesen die Einräumung der Nutzungsrechte vertraglich vereinbaren.

Open Data muss als wesentlicher Bestandteil der Informationsfreiheit verstanden werden. Allerdings wird der Anspruch auf Informationszugang im herkömmlichen Antragsverfahren auch in Zukunft unverzichtbar sein. Eine Weiterentwicklung der bestehenden Informationsfreiheitsrechte um möglichst

umfassende Veröffentlichungspflichten halten die Informationsfreiheitsbeauftragten für unerlässlich. Mit dem Positionspapier unterstützen sie die begonnenen Open-Data-Projekte und empfehlen den Gesetzgebern eine enge Verzahnung von Informationsfreiheit und Open Data.

◆ Positionspapier: Informationsfreiheit und Open Data

Informationsfreiheit und Open Data sind wesentliche Voraussetzungen für Transparenz und Kontrollierbarkeit der Verwaltung und fördern die demokratische Partizipation.

Die Informationsfreiheits- und Transparenzgesetze der Länder sowie des Bundes (im Folgenden: Informationsfreiheitsgesetze) erfahren große Akzeptanz und werden intensiv genutzt. Ihnen ist zumeist eines gemeinsam: Wer Informationen von öffentlichen Stellen begehrt, muss einen Antrag stellen, ein Verwaltungsverfahren durchlaufen und dafür unter Umständen auch Gebühren entrichten. Die gesellschaftlichen Erwartungen an einen transparenten Staat gehen inzwischen jedoch darüber hinaus.

Dem in seiner Durchsetzung oft aufwändigen Antragsrecht der Bürgerinnen und Bürger sollte deshalb die Pflicht öffentlicher Stellen stärker als bisher zur Seite gestellt werden, Informationen von sich aus zu veröffentlichen. Open Data – also die aktive Bereitstellung öffentlicher Informationen im Internet – wird auf den ersten Portalen im Internet bereits praktiziert. Zahlreiche Projekte befinden sich im Aufbau.

Open Data beinhaltet begrifflich bereits die Forderung nach Offenheit. Daten des öffentlichen Sektors sind in diesem Sinne offen, wenn sie maschinenlesbar sind (maschinell interpretiert werden können), das Format der Datensätze offen und frei nutzbar ist (offene Standards), sie grundsätzlich keiner beschränkenden Lizenz unterliegen und ohne Kosten zugänglich sind sowie beliebig genutzt und weiterverwendet werden können. Damit dies zum Standard für den Umgang mit Informationen öffentlicher Stellen in Deutschland werden kann, müssen neben informationstechnischen auch rechtliche Voraussetzungen geschaffen werden. Die Informationsfreiheitsbeauftragten halten zur Umsetzung von Open Data klare gesetzliche Grundlagen für erforderlich und empfehlen die Berücksichtigung der folgenden Eckpunkte:

1. Open Data braucht starke Informationsfreiheitsgesetze

a. Open Data muss als wesentlicher Bestandteil der Informationsfreiheit verstanden werden. Der Anspruch auf Informationszugang im herkömmlichen Antragsverfahren wird auch in Zukunft unverzichtbar sein.

b. Länder, in denen noch keine entsprechenden gesetzlichen Regelungen existieren, sollten unverzüglich Informationsfreiheitsgesetze mit einem starken Anspruch auf Informationszugang und effektiver Verpflichtung zur proaktiven Veröffentlichung von Daten öffentlicher Stellen sowie zur Einrichtung von Informationsregistern bzw. Open-Data-Portalen beschließen.

c. Die Informationsfreiheitsgesetze sind, soweit erforderlich, so anzupassen, dass Informationen, die auf ihrer Grundlage herausge-

geben werden, in der Regel auch veröffentlicht werden können. Die Pflichten zur Veröffentlichung sind in den Informationsfreiheitsgesetzen zu regeln und müssen für alle öffentlichen Stellen gelten, die bereits einem Zugangsanspruch nach den jeweiligen Informationsfreiheitsgesetzen unterliegen. Wenn Informationen auf dem Antragswege herauszugeben sind, sollte auch deren Veröffentlichung so wenig wie möglich beschränkt werden. Hierfür kann die Anonymisierung von Daten förderlich sein.

d. Die Gefahr der weiteren Rechtszersplitterung durch neue Open-DataRegelungen außerhalb der Informationsfreiheitsgesetze bestätigt die Forderung der Informationsfreiheitsbeauftragten nach einer möglichst einheitlichen Rechtsgrundlage für den Informationszugang.

2. Klarere Regelungen zur Veröffentlichung als Voraussetzung für Open Data

a. Open Data ist weit mehr als Öffentlichkeitsarbeit: Bestehende Ansätze von Veröffentlichungspflichten in den Informationsfreiheitsgesetzen sind auszubauen und um effektive Instrumente zu ergänzen, die eine Veröffentlichung gewährleisten.

b. Kategorien von Dokumenten, die zu veröffentlichen sind, sollten in den Informationsfreiheitsgesetzen umfassend und konkret beschrieben werden. Die Informationsfreiheitsbeauftragten beraten bei der Konzeption und Umsetzung.

c. In den Informationsfreiheitsgesetzen sollte für alle Informationen, auf deren Zugang ein voraussetzungsloser Anspruch besteht, auf Verwendungsbeschränkungen verzichtet werden.

d. Der Ort der Veröffentlichung ist ausdrücklich zu regeln. Denkbar ist die Veröffentlichung in einem Informationsregister bzw. Open-Data-Portal. Auch kann die Einrichtung entsprechender Seiten auf den Homepages der informationspflichtigen Stellen sinnvoll sein.

e. Ein Informationsregister bzw. eine Open-Data-Plattform sollte ausschließlich in öffentlicher Regie errichtet werden. Durch die Verantwortlichkeit öffentlicher Betreiberinnen und Betreiber können nicht zuletzt die Richtigkeit und Aktualität der angebotenen Informationen am ehesten gewährleistet werden.

f. Die Ausgestaltung einer Open-Data-Plattform sollte sich bereits von der technischen Konstruktion bis hin zu den Voreinstellungen auf Funktionen beschränken, die für die Bereitstellung der Informationen für die Bürgerinnen und Bürger von Bedeutung sind, ihnen die Preisgabe nicht erforderlicher personenbezogener Daten aber nicht abverlangen (privacy by design).

3. Es bedarf eines subjektiven, durchsetzbaren Anspruchs auf Veröffentlichung

a. Ein wichtiges Instrument zur Durchsetzung von Open Data ist die Gewährleistung eines subjektiven Rechtsanspruches auf die aktive Veröffentlichung von Informationen in den Informationsfreiheitsge-

setzen von Bund und Ländern. Zwar ist die Verwaltung an Recht und Gesetz gebunden, jedoch hätten Bürgerinnen und Bürger ohne einen derartigen Anspruch keine Möglichkeit, eine öffentliche Stelle, die vorhandene Daten entgegen der Veröffentlichungspflicht rechtswidrig zurückhält, zur Veröffentlichung zu verpflichten.

b. Dieser Anspruch sollte dem bisherigen Informationszugangsanspruch im Hinblick auf Einklagbarkeit und Unterstützung durch die Informationsfreiheitsbeauftragten gleichgestellt werden.

4. Keine Verwendungseinschränkung für öffentlich bereitgestellte Daten

a. Datenbestände öffentlicher Stellen dürfen nicht durch Urheber- oder Nutzungsbeschränkungen der öffentlichen Stellen blockiert werden. Um Urheberrechten Dritter Rechnung zu tragen, sollten öffentliche Stellen mit diesen die Einräumung der Nutzungsrechte vertraglich vereinbaren.

b. Sowohl bei der Veröffentlichung als auch bei der Verwendung darf es nicht darauf ankommen, welche Absichten die Nutzerinnen und Nutzer verfolgen.

5. Open Data ist eine Investition in die Zukunft

a. Sowohl die Schaffung der Infrastruktur als auch die erstmalige Aufarbeitung und Bereitstellung der Daten können kostenintensiv sein. Auch die regelmäßige Veröffentlichung aktueller Informationen kann zusätzliche Sach- und Personalkosten binden. Es bedarf sowohl einer technischen Aufbereitung der Daten selbst (Maschinenlesbarkeit) als auch der Strukturierung einer nutzbaren, übersichtlichen Plattform.

b. Aus Praktikabilitätsgründen wird eine Beschränkung des Umfangs der tatsächlich zu veröffentlichenden Daten zunächst unumgänglich sein. Auch ein zeitlich gestaffeltes In-Kraft-Treten von Veröffentlichungspflichten kann dem Praktikabilitätsgedanken Rechnung tragen.

c. Angemessene Übergangsfristen sind auch für die Schaffung der technischen Voraussetzungen sowie für die etwaige Aufbereitung von Informationen, die vor dem In-Kraft-Treten einer entsprechenden Regelung angefallen sind, vertretbar.

d. Um die Bereitstellung von Informationen zu erleichtern, sollten Regelungen getroffen werden, damit neue Daten bereits von vornherein in den entsprechend verwertbaren Formaten geführt werden oder zumindest problemlos aufbereitet werden können.

e. Die Kosten der Verwaltung können durch Open Data langfristig reduziert werden. Insbesondere erspart die proaktive Bereitstellung von Informationen den öffentlichen Stellen die Bearbeitung individueller Informationszugangsanträge.

f. Durch innovative Geschäftsmodelle zur kommerziellen Weiterverwendung öffentlicher Daten kann Open Data zu positiven gesamtwirtschaftlichen Effektenbeitragen.

g. Die Kostenerhebung für den antragsgebundenen Informationszugang steht in einem Spannungsverhältnis zur Kostenfreiheit im Rahmen von Open Data. Ein stimmiges Gesamtkonzept sollte durch einen grundsätzlichen Verzicht auf die Erhebung von Gebühren erreicht werden.

h. Open Data bedeutet einen Aufgabenzuwachs bei den Informationsfreiheitsbeauftragten. Auch nach der Begleitung im Anfangsstadium (Gesetzgebung, Projekte für Plattformen etc.) bedürfen die öffentlichen Stellen einer permanenten Beratung zur Umsetzung der Veröffentlichungspflichten. Außerdem müssen die Kapazitäten der Informationsfreiheitsbeauftragten erweitert werden.

◆ Transparenz bei Sicherheitsbehörden

Im Zusammenhang mit den Enthüllungen der umfassenden und anlasslosen Überwachungsmaßnahmen des US-amerikanischen und des britischen Geheimdienstes wurde bekannt, dass auch ein großer Teil des Kommunikationsverhaltens der Bürgerinnen und Bürger in Deutschland ohne ihr Wissen von diesen Geheimdiensten überwacht worden ist.

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Verantwortlichen in Deutschland und Europa auf, für Transparenz auf nationaler und internationaler Ebene zu sorgen. Das Vertrauen der Bevölkerung kann nur zurück gewonnen werden, wenn die Aufgaben und Befugnisse der Sicherheitsbehördenvölkerrechtlich festgelegt und deren tatsächliche Arbeitsweisen nachvollziehbar sind.

Zweifellos verfügen die Nachrichtendienste über Informationen, die nicht offen gelegt werden dürfen. Gleichwohl hält die Konferenz die pauschale Ausnahme der Nachrichtendienste des Bundes und der Länder vom Anwendungsbereich der Informationsfreiheits- und Transparenzgesetze für nicht hinnehmbar und erwartet von den Gesetzgebern entsprechende Verbesserungen.

Darüber hinaus bedürfen die weit gefassten Ausnahmeregelungen für Sicherheitsbelange in den Informationsfreiheits- und Transparenzgesetzen einer Überprüfung und Einschränkung.

Die Informationsfreiheitsbeauftragten unterstützen die Verbesserung der Transparenz der nachrichtendienstlichen Aktivitäten gegenüber den Parlamenten und schließlich die Stärkung der parlamentarischen Kontrollgremien.

◆ Verbraucher durch mehr Transparenz im Lebensmittelbereich schützen – Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!

Mit der Reform des Verbraucherinformationsrechts zum 1. September 2012 hat der Gesetzgeber als Reaktion auf die Lebensmittelskandale der letzten Jahre mit § 40 Abs. 1a Lebensmittel- und Futtermittelgesetzbuch (LFGB) eine Rechtsgrundlage für die Veröffentlichung von Hygieneverstößen durch die zuständigen Behörden geschaffen. Schon im damaligen Gesetzgebungsverfahren hatte die Konferenz der Informationsfreiheitsbeauftragten darauf hingewiesen, dass die Vorschrift zu undifferenziert sei.

Nachdem zahlreiche Bundesländer begonnen hatten, Verbraucherinnen und Verbraucher auf eigens dafür geschaffenen Internetplattformen über entsprechende Hygieneverstöße zu informieren, sind die Veröffentlichungen durch eine Reihe von verwaltungsgerichtlichen Entscheidungen in Baden-Württemberg, Bayern, Berlin, Nordrhein-Westfalen und Rheinland-Pfalz gestoppt worden. Nach Auffassung der Gerichte greift § 40 Abs. 1a LFGB unter anderem deshalb unverhältnismäßig in die Rechte der betroffenen Unternehmen ein, weil die Vorschrift schon bei geringen Verstößen eine Veröffentlichung zulasse und keine Grenzen für die Dauer der Veröffentlichung vorsehe.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, dringend die lebensmittelrechtlichen Vorschriften über die Information der Öffentlichkeit zu überarbeiten und wie vom Bundesrat angeregt im Fachdialog mit den Ländern ein Transparenzsystem zu schaffen, das in eine rechtskonforme und effektive Gesamtkonzeption eingebunden wird. Nach der Rechtsprechung sind als Kriterien für eine Neuregelung der Veröffentlichungspflicht im Sinne des § 40 Abs. 1a LFGB insbesondere die Schwere des Rechtsverstoßes, eine behördliche Hinweispflicht auf die Tatsache und den Zeitpunkt der Mängelbeseitigung, Löschungspflichten sowie Ermessens- und Härtefallregelungen in Erwägung zu ziehen.

Umfassende Transparenz bei der Lebensmittelsicherheit darf nicht als Belastung für die Betriebe verstanden werden. Vielmehr ist dies der einzige Weg, das Vertrauen von Verbraucherinnen und Verbrauchern in die Qualität der Lebensmittel langfristig herzustellen und zu wahren.

◆ Für einen effektiven presserechtlichen Auskunftsanspruch gegenüber allen Behörden - auch des Bundes

Das Bundesverwaltungsgericht hat mit Urteil vom 20. Februar 2013 entschieden, dass die Pressegesetze der Länder keine Verpflichtung von Bundesbehörden zur Auskunftserteilung an Journalistinnen und Journalisten begründen. Die Gesetzgebungskompetenz für den presserechtlichen Auskunftsanspruch gegenüber Bundesbehörden liege danach beim Bund. Eine entsprechende Auskunftsverpflichtung existiert bislang nicht. Das Bundesverwaltungsgericht sieht einen unmittelbar aus der Garantie der Pressefreiheit abgeleiteten "Minimalstandard von Auskunftspflichten" und einen einklagbaren, ebenfalls unmittelbar aus Art. 5 Abs. 1 Satz 2 GG abgeleiteten Rechtsanspruch auf Auskunft, soweit dem nicht berechtigte schutzwürdige Vertraulichkeitsinteressen von Privatpersonen oder öffentlichen Stellen entgegenstehen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt die Entscheidung des Bundesverwaltungsgerichtes insofern, als damit der Auskunftsanspruch von Journalistinnen und Journalisten grundrechtlich abgeleitet und abgesichert wird.

Aus Sicht der Konferenz gilt es - unabhängig von der kontrovers diskutierten Regelungszuständigkeit - die notwendigen gesetzlichen Grundlagen für eine effektive journalistische Recherche herzustellen, die eine zeitnahe, aktuelle und profunde Berichterstattung ohne abschreckende Kostenhürden möglich machen. Das Urteil, das einen unscharfen, beliebig interpretierbaren Minimalstandard mit unklaren Grenzen und Beschränkungsmöglichkeiten zugesteht, darf hier jedenfalls nicht das letzte Wort sein! Bundesbehörden müssen denselben Auskunftspflichten unterliegen wie Landesbehörden.

Entschließungen vom 9. Dezember 2014

◆ Mehr Transparenz bei technischen Ermittlungsmethoden – Vertrauen in den Rechtsstaat stärken!

In den vergangenen Jahren wurden die Ermittlungsbefugnisse für Polizeien, Strafverfolgungsbehörden und Nachrichtendienste kontinuierlich ausgeweitet. Ihnen steht ein beträchtliches Instrumentarium unterschiedlich eingriffsintensiver technischer Maßnahmen zur Verfügung, wie zum Beispiel Funkzellenabfragen, Einsatz von IMSI-Catchern, Telekommunikationsüberwachung und Verkehrsdatenerhebung. Im Rahmen der Erweiterung wurden in die Landespolizeigesetze und die Strafprozessordnung Berichterstattungspflichten aufgenommen. Dadurch sollte garantiert werden, dass die Gesellschaft sich der Auswirkungen dieser neuen Maßnahmen bewusst ist.

Eine kritische Überprüfung der Berichtspflichten zeigt, dass eine Transparenz der Auswirkungen solcher Ermittlungsmaßnahmen nicht erreicht wird. Die Berichterstattungspflichten sind nicht nur uneinheitlich geregelt: Zum Teil fehlen für einige Maßnahmen wie zum Beispiel die Bestandsdatenabfrage Berichtspflichten vollständig, zum Teil lassen die bestehenden Berichtspflichten keine hinlänglichen Erkenntnisse über das Ausmaß der Überwachung und insbesondere die Zahl der Betroffenen zu. Die Berichte über Funkzellenabfragen zu Strafverfolgungszwecken lassen etwa nicht erkennen, dass von einer einzelnen gerichtlichen Anordnung tausende Bürgerinnen und Bürger betroffen sein können, die keinen Anlass für die Erhebung ihrer Daten gegeben haben. Das Bundesverfassungsgericht verlangt in seinem Urteil zur Vorratsdatenspeicherung aber gerade, dass der Gesetzgeber eine "Überwachungsgesamtrechnung" betreibt und beim Erlass neuer Überwachungsregelungen berücksichtigt. Nur so könne verhindert werden, dass die Freiheitswahrnehmung der Bürger total erfasst und registriert wird, denn dies verstieße gegen die verfassungsrechtliche Identität Deutschlands. Deshalb ist es jedenfalls erforderlich, nicht nur die theoretisch bestehenden, vom Gesetz erlaubten Überwachungsmöglichkeiten in den Blick zu nehmen, sondern gerade auch das konkrete Ausmaß ihres Einsatzes sichtbar zu machen.

Auf der Grundlage der gegenwärtig veröffentlichten Statistiken und zum Teil schmalen Berichtspflichten ist es nicht möglich, die gesamtgesellschaftlichen Auswirkungen aller Maßnahmen differenziert zu erfassen. Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern daher auf, die bestehenden Verpflichtungen zur Erstellung und Veröffentlichung von Statistiken auf alle Maßnahmen im Rahmen verdeckter Ermittlungsmethoden auszudehnen und sie durch die Angabe der Anzahl der Betroffenen so aussagekräftig zu gestalten, dass sich der Effekt auf die Bevölkerung klar erkennen lässt.

Darüber hinaus muss eine gesetzliche Veröffentlichungspflicht für die Berichte der Bundesnetzagentur zur Bestandsdatenabfrage festgeschrieben werden.

Eine besondere Bedeutung kommt der Transparenz der Nachrichtendienste zu. Erforderlich ist die Verschärfung bestehender bzw. Schaffung neuer Berichtspflichten gegenüber parlamentarischen Kontrollgremien und Datenschutzbeauftragten und die Verpflichtung zur Aufnahme aussagekräftiger statistischer Angaben zu Überwachungsmaßnahmen in die Verfassungs-

schutzberichte von Bund und Ländern. Geboten ist insbesondere eine Berichterstattung für den gesamten Bereich der strategischen Auslands-Telekommunikationsüberwachung.

Die Transparenz beim Einsatz staatlicher, insbesondere geheimer Ermittlungsmethoden ist neben den datenschutzrechtlichen Anforderungen eine wesentliche Voraussetzung für eine effiziente demokratische Kontrolle sowie die Beurteilung der Angemessenheit des staatlichen Eingriffshandelns und damit eine unabdingbare Wissensgrundlage für das Vertrauen der Bürgerinnen und Bürger in ihren Rechtsstaat.

◆ Open Data muss in Deutschland Standard werden!

Die Bundesregierung hat mit der Digitalen Agenda 2014 - 2017, der Digitalen Verwaltung 2020 und dem nationalen Aktionsplan zur Umsetzung der G8 Open-Data-Charta wesentliche Regierungsprogramme zur Etablierung von E- und Open-Government sowie zur Digitalisierung der Verwaltung auf den Weg gebracht. Die Regierungsprogramme sehen aus informationsfreiheitsrechtlicher Sicht u.a. die Einführung einer gesetzlichen Open-Data-Regelung, die Schaffung von Open-Data-Ansprechpartnern in den Behörden, die Einführung der elektronischen Verwaltungsakte und eine verstärkte Zusammenarbeit mit den Ländern vor.

Die Konferenz der Informationsfreiheitsbeauftragten betont in diesem Zusammenhang das Erfordernis weitgehender gesetzlicher Veröffentlichungspflichten und die Übertragung der Aufgabe des Open-Data-Ansprechpartners auf behördliche Informationsfreiheitsbeauftragte.

Insbesondere bei Planung und Einführung der eAkte sind Aspekte der Informationsfreiheit und des Datenschutzes frühestmöglich im Anforderungskatalog abzubilden. Schon bei Anlage einer Akte sollten personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse und sonstige Beschränkungen vor einer weiteren Verwendung markiert werden, so dass sie automatisiert ersetzt oder hervorgehoben werden können. Dies erleichtert eine nachfolgende Weitergabe und Weiterverwendung erheblich und unterstützt die aktenführenden Stellen bei der effizienten Bearbeitung von IFG-Anträgen.

Es gilt jetzt, die Regierungsprogramme zügig in die Tat umzusetzen, damit Open Data in Deutschland zum Standard werden kann. Die Konferenz fordert die Länder und den Bund auf, soweit noch nicht geschehen, mit dieser Zielsetzung E- und Open-Government-Strategien gemeinsam zu entwickeln.

◆ Umfassende und effektive Informationsfreiheitsaufsicht unabdingbar!

Mit den Informationsfreiheitsgesetzen des Bundes und der Länder wurde der Bundes- bzw. den Landesbeauftragten für Informationsfreiheit die Aufgabe eines "außergerichtlichen Streitschlichters" im Bereich des allgemeinen Informationsfreiheitsrechts übertragen. Sie kontrollieren die Anwendung der Informationsfreiheitsgesetze, vermitteln in Streitfällen und wirken auf die Einhaltung des geltenden Rechts hin. Im Bund sowie in den meisten Bundesländern verfügen die Informationsfreiheitsbeauftragten jedoch nur über eine

eingeschränkte Kontroll- und Beratungskompetenz. Sie überwachen nur die Einhaltung des allgemeinen Informationsfreiheitsrechts, nicht jedoch der besonderen Informationszugangsrechte, wie z.B. nach dem Umwelt- oder dem Verbraucherinformationsrecht.

Diese Situation ist unbefriedigend. Bürgerinnen und Bürger erwarten, dass ihr Informationsanliegen von den Informationsfreiheitsbeauftragten umfassend geprüft wird. Mangels umfassender Kontroll- und Beratungszuständigkeit ist dies jedoch zu häufig nicht der Fall, sodass es im Umwelt- und im Verbraucherinformationsrecht an einer unabhängigen Aufsichtsbehörde fehlt.

Auch die wissenschaftlichen Evaluierungsberichte zum Informationsfreiheitsgesetz des Bundes und einiger Länder haben sich dafür ausgesprochen, den Informationsfreiheitsbeauftragten zusätzlich die Kontrollkompetenzen für das besondere Informationsfreiheitsrecht zu übertragen. Im Bereich des Datenschutzes sind die Beauftragten bereits für das besondere Datenschutzrecht zuständig. Dieser Standard muss auch in der Informationsfreiheit hergestellt werden.

Die Konferenz der Informationsfreiheitsbeauftragten fordert daher die Gesetzgeber in Bund und Ländern auf, die Kontroll- und Beratungskompetenzen der Informationsfreiheitsbeauftragten um das Umwelt- und das Verbraucherinformationsrecht – wo dies noch nicht geschehen ist - zu erweitern und die Informationsfreiheitsbeauftragten mit ausreichenden personellen und sachlichen Mitteln auszustatten, damit sie ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen können. Nur so ist gesichert, dass Bürgerinnen und Bürger bei der Ausübung ihrer Informationsrechte umfassend beraten werden und die Einhaltung der verschiedenen Informationsgesetze unabhängig kontrolliert wird.

Entschließungen vom 17.06.2014

◆ Informationsfreiheit nicht Privaten überlassen!

Öffentliche Stellen vertreten vielfach die Auffassung, staatliche Transparenz könne durch die Bereitstellung amtlicher Informationen auf von Privaten nach deren Regularien betriebenen Plattformen wie Facebook, Twitter etc. hergestellt werden. Auch wenn derartige Internetdiensteanbieter einen großen Nutzerkreis erreichen, stehen kommerzielle Interessen der Betreiber vielfach einem bedingungslosen und freien Informationszugang entgegen.

Öffentlichkeit ist gekennzeichnet durch voraussetzungslose, für ausnahmslos alle Menschen bestehende Zugangsmöglichkeiten. Sie kann deshalb nicht durch die Bereitstellung von Inhalten auf Internetseiten und -diensten hergestellt werden, die zum Beispiel ausschließlich durch allgemeine Geschäftsbedingungen Privater geregelt sind, nur Mitgliedern offen stehen oder keinen unbeobachteten Zugang gewähren. Staatliche Transparenz darf nicht durch die Offenbarung personenbezogener Daten erkauft werden.

Nur die Veröffentlichung auf von öffentlichen Stellen steuerbaren und der Allgemeinheit kostenfrei und anonym zugänglichen Kanälen genügt den Anforderungen der Herstellung staatlicher Transparenz. Die Konferenz der In-

formationsfreiheitsbeauftragten fordert, die Veröffentlichung amtlicher Informationen auf ausschließlich von den öffentlichen Stellen selbst gesteuerten Veröffentlichungsmedien vorzunehmen. Eine Steuerung und Kontrolle in diesem Sinne kann beispielsweise auch durch Einzelverträge mit Privaten geschehen. Der im Hamburger Transparenzgesetz formulierte Grundsatz, wonach der Zugang zum Informationsregister kostenlos und anonym ist, sollte in alle Informationsfreiheits-und Transparenzgesetze aufgenommen werden.

◆ Keine Flucht vor der Informationsfreiheit ins Privatrecht!

Es ist für weite Bereiche der Rechtsordnung anerkannt, dass der Staat sich nicht durch Wahl einer privaten Rechtsform seiner verfassungsrechtlichen Bindungen entledigen kann. Für das Recht aller Bürgerinnen und Bürger, sich voraussetzungslos über staatliches oder kommunales Handeln zu informieren, gilt dies leider nicht in gleichem Maße. Entscheidet sich der Staat für eine formale Privatisierung und erledigt eine öffentliche Aufgabe durch eine juristische Person des Privatrechts, so ist diese nach vielen Informationsfreiheitsgesetzen nicht direkt auskunftsverpflichtet. Informationszugang muss für alle Unter-lagen gelten, die im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen. Dabei darf es nicht darauf ankommen, ob die Aufgaben durch Behörden oder durch Private, an denen die öffentliche Hand mehrheitlich beteiligt ist, wahrgenommen werden. Ebenso wenig kommt es auf die Rechtsform an, in der jeweils gehandelt wird.

Da häufig gerade die Bereiche privatisiert werden, die über große Finanzvolumina verfügen, ist hier die Herstellung von Transparenz hinsichtlich der Verwendung öffentlicher Steuermittel besonders wichtig. Bereits 2003 hatten die Informationsfreiheitsbeauftragten die Gesetzgeber im Bund und in den Ländern dazu aufgerufen, die Herstellung von Transparenz nicht davon abhängig zu machen, in welcher Form die öffentliche Aufgabe erledigt wird. Leider ist diese Forderung längst nicht überall umgesetzt worden. Es gilt weiterhin: Für die Auskunftsverpflichtung sollte allein entscheidend sein, ob es sich um eine staatliche oder kommunale Aufgabe, insbesondere eine der Grundversorgung handelt. Bei der Erfüllung öffentlicher Aufgaben müssen Ansprüche auf Auskunft auch direkt gegenüber den Unternehmen geschaffen werden.

Die Anwendung der Informationsfreiheitsgesetze darf nicht von der Rechtsform abhängen, in der öffentliche Aufgaben erledigt werden. Eine Flucht vor der Informationsfreiheit in das Privatrecht ist mit einem modernen Staatsverständnis nicht zu vereinbaren.

◆ Das Urheberrecht dient nicht der Geheimhaltung!

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland betrachtet mit Sorge die Entwicklung, dass sich auskunftspflichtige Stellen zur Ablehnung von Anfragen auf das Urheberrecht oder andere Rechte des "Geistigen Eigentums" berufen. Das Urheberrecht darf nicht dazu eingesetzt werden, staatliche Informationen zurück zu halten.

Amtliche Vermerke sind in aller Regel nicht urheberrechtlich geschützt. Gedankliche Inhalte können in ihrer politischen, wirtschaftlichen oder gesell-

schaftlichen Aussage nicht über das Urheberrecht monopolisiert werden, sondern müssen vielmehr Gegenstand der freien geistigen Auseinandersetzung bleiben. Mit Steuermitteln finanzierte und für die Erfüllung einer öffentlichen Aufgabe erstellte Vermerke dürfen nicht unter Berufung auf Rechte des "Geistigen Eigentums" zurückgehalten werden. Hintergrund insbesondere des urheberrechtlichen Schutzes ist die Garantie einer angemessenen Vergütung der Urheber. Diese ist aber nicht bedroht, wenn Werke betroffen sind, die in Erfüllung dienstlicher Pflichten erstellt wurden.

Nur in Ausnahmefällen kann es sein, dass von Dritten für staatliche Stellen erstellte Gutachten tatsächlich dem Urheberrecht unterfallen und die Dritten schutzbedürftig sind. Wer mit der Verwaltung Verträge schließt, muss wissen, dass diese an gesetzliche Transparenzpflichten gebunden ist, die sich nicht abbedingen lassen. Wo dies nicht bereits gesetzlich vorgeschrieben ist, sollen sich die staatlichen Stellen in solchen Fällen das Recht an einer Herausgabe einräumen lassen. Soweit diese Stellen einem Informationsfreiheitsgesetz unterliegen, ist es ihre Pflicht, dafür Sorge zu tragen, dass Rechte Dritter nicht einem gesetzlichen Informationszugang entgegenstehen. Was mit staatlichen Mitteln für die Verwaltung von staatlichen Stellen oder Dritten hergestellt wird, muss grundsätzlich zugänglich sein.

Entschließung der Landesdatenschutzkonferenz

◆ Entschließung vom 19. Februar 2015

Aufgrund des Beschlusses des Landtags Nordrhein-Westfalen (Drucksache 16/1469 vom 20.11.2012) hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zu einer Landesdatenschutzkonferenz eingeladen, um Möglichkeiten und Voraussetzungen einer Datenschutzzertifizierung zu prüfen.

Die Landesdatenschutzkonferenz setzt sich aus folgenden Institutionen zusammen:

- Landesvereinigung der Unternehmensverbände Nordrhein-Westfalen e. V.
- Die Industrie- und Handelskammern in Nordrhein-Westfalen e. V.
- Nordrhein-Westfälischer Handwerkstag
- Westdeutscher Handwerkskammertag
- Deutscher Gewerkschaftsbund Bezirk Nordrhein-Westfalen
- Verbraucherzentrale Nordrhein-Westfalen e. V.
- Städte- und Gemeindebund Nordrhein-Westfalen e. V.
- Städtetag Nordrhein-Westfalen
- Landkreistag Nordrhein-Westfalen
- Ministerium für Inneres und Kommunales Nordrhein-Westfalen
- Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz Nordrhein-Westfalen
- Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk Nordrhein-Westfalen
- Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Vorsitz)

I.

Die Landesdatenschutzkonferenz stellt fest:

Datenschutzsiegel auf Grundlage freiwilliger Zertifizierungsverfahren können einen bedeutsamen Beitrag für den Datenschutz leisten, wenn sie insbesondere folgende Anforderungen erfüllen:

1. Mehrwert für den Datenschutz

Datenschutzsiegel dienen der Orientierung, sie bescheinigen eine definierte Datenschutzqualität. Die mit einem Siegel ausgezeichneten Produkte oder Verfahren müssen daher einen datenschutzrechtlichen Mehrwert aufweisen – etwa erhöhte Sicherheitsstandards, erweiterte Rechte für Verbraucherinnen und

Verbraucher oder sonstige Betroffene, datenschutzfreundliche Voreinstellungen, festgelegte und überprüfte Prozesse, die Bestellung von betrieblichen Datenschutzbeauftragten und die Durchführung von Vorabkontrollen auch in den Fällen, in denen es keine gesetzliche Verpflichtung dazu gibt.

2. Von Aufsichtsbehörden gebilligter Prüfmaßstab

Die im Rahmen der Siegelvergabe zu prüfenden Kriterien müssen von den Datenschutzaufsichtsbehörden befürwortet werden. Dazu ist abhängig vom jeweiligen Gegenstand der Zertifizierung – in der Regel datenschutzrelevante Produkte oder Verfahren – ein allgemeiner Prüfmaßstab zu formulieren und den Aufsichtsbehörden vorzulegen. Um bundesweit einheitliche Anforderungen zu gewährleisten, nehmen die Aufsichtsbehörden im Rahmen ihres Koordinierungsgremiums für den Datenschutz im nicht-öffentlichen Bereich ("Düsseldorfer Kreis") dazu abgestimmt Stellung (siehe auch beiliegenden Beschluss des Düsseldorfer Kreises vom 25./26.Februar 2014). Auf Landesebene bewertet der LDI den Prüfmaßstab für eine Siegelvergabe.

3. Eindeutige, nachvollziehbare Aussagekraft des Siegels

Das im Anschluss an eine erfolgreiche Zertifizierung vergebene Datenschutzsiegel muss für die Verbraucherinnen und Verbraucher sowie sonstige Adressaten aussagekräftig, eindeutig und nachvollziehbar sein. Insbesondere muss erkennbar sein, wer nach welchem veröffentlichten Prüfstandard das Siegel vergeben hat, auf welche Eigenschaften und Prüfgegenstände es sich bezieht und wie lange es gültig ist.

4. Transparenz

Der Prüfmaßstab und die wesentlichen Elemente des Prüfverfahrens sind offenzulegen. Diese Transparenz ermöglicht

- Orientierung für die Verbraucherinnen und Verbraucher und sonstigen Marktteilnehmer/innen und kann damit deren Vertrauen und die Akzeptanz des Siegels erhöhen;
- Orientierung auch für die Unternehmen, die ihre Dienstleistungen oder Produkte nicht zertifizieren lassen – der Prüfmaßstab wird insoweit zum "Allgemeingut", das Dritte für die eigenverantwortliche Verbesserung des Datenschutzes nutzen können;
- eine öffentliche Diskussion und Weiterentwicklung des Prüfstandards.

5. Qualifizierte und unabhängige Prüfungs- und Zertifizierungsstellen

Prüfung und Zertifizierung müssen durch neutrale Stellen erfolgen, die von dem geprüften Unternehmen unabhängig sind. Die Eignung und Qualifizierung der am Zertifizierungsverfahren Beteiligten sind ebenso festzulegen wie die jeweiligen Verantwort-

lichkeiten und Regelungen zur Vermeidung von Interessenkollisionen. So dürfen etwa die prüfenden Personen keine über die Zertifizierung hinausgehende wirtschaftliche Verbindung zu dem Unternehmen haben und auch im Anschluss in einer Karenzzeit nicht für das Unternehmen tätig werden.

Um bundesweit auch insoweit einheitliche Anforderungen zu gewährleisten, nehmen die Aufsichtsbehörden im Rahmen ihres Koordinierungsgremiums für den Datenschutz im nicht-öffentlichen Bereich ("Düsseldorfer Kreis") dazu abgestimmt Stellung (siehe auch beiliegenden Beschluss des Düsseldorfer Kreises vom 25./26.02.2014).

6. Befristung der Siegelvergabe und Sanktion von Verstößen

Das Siegel wird zeitlich befristet vergeben. Zertifizierungsrelevante Änderungen des Prüfgegenstands führen zur Unwirksamkeit des Siegels, soweit keine Ergänzungs- oder Neuprüfung die Vereinbarkeit mit den Siegelanforderungen ergibt. Für Verstöße gegen die Bestimmungen des Siegels sind Sanktionen durch die Zertifizierungsstelle vorzusehen.

7. Kontrollrechte der Aufsichtsbehörden bleiben unberührt

Die Zertifizierung lässt die Kontrollrechte der Aufsichtsbehörden unberührt. Die Aufsichtsbehörden können daher sowohl bei konkreten Anhaltspunkten für Verstöße wie auch im Rahmen von Stichprobenkontrollen die Einhaltung des Datenschutzes bei zertifizierten Unternehmen überprüfen.

II.

Die Landesdatenschutzkonferenz empfiehlt

1. der Landesregierung, im Rahmen ihrer Möglichkeiten darauf hinzuwirken, dass in der geplanten EU-Datenschutz-Grundverordnung Rahmenbedingungen für die genannten Anforderungen an Datenschutzsiegel geschaffen werden;

2. dem Landtag und der Landesregierung, Möglichkeiten zu prüfen, die Verbreitung derartiger Datenschutzsiegel in der Wirtschaft zu fördern.

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