LDI NRW

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Datenschutz und Informationsfreiheit

23. Bericht 2017

www.ldi.nrw.de

23. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Helga Block

für die Zeit vom 1. Januar 2015 bis zum 31. Dezember 2016

Herausgeber:
Landesbeauftragte für Datenschutz
und Informationsfreiheit
Nordrhein-Westfalen

Helga Block

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: 23. DIB LDI NRW
ISSN: 0179–2431

Düsseldorf 2017
Titelbild: psdesign1 @ Fotolia.com

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Anhang

Kühlungsborner Erklärung der unabhängigen Datenschutzbehörden der Länder vom 10. November 2016

Pressemitteilung der unabhängigen Datenschutzbehörden der Länder vom 1. Februar 2017:
Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz!

Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

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

Entschließungen und Beschlüsse der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Hinweise auf Informationsmaterial

Die Entschließungen und Beschlüsse sind zudem im Internetangebot der LDI NRW unter der folgenden Adresse abrufbar:

www.ldi.nrw.de

1. Vorwort

In unserer Landesverfassung ist das Grundrecht auf Datenschutz an prominenter Stelle in Artikel 4 Absatz 2 normiert. Es ist die Aufgabe der Landesbeauftragten, dieses Grundrecht zu schützen und zu verteidigen.

Am 1. Oktober 2015 habe ich dieses Amt, das in Nordrhein-Westfalen mit Artikel 77a auch auf der Ebene der Landesverfassung verankert ist, von meinem geschätzten Vorgänger, Herrn Ulrich Lepper, übernommen. Ich danke den Abgeordneten des Landtages und der Landesregierung für das Vertrauen, das mir als der nunmehr fünften Datenschutzbeauftragten des Landes geschenkt wurde.

Von den 24 Monaten des Berichtszeitraumes sind neun noch in die Amtszeit meines Vorgängers gefallen. Der Berichtszeitraum war im Wesentlichen geprägt von der Neuausrichtung des Datenschutzrechtes in Europa mit unmittelbarer Wirkung in Deutschland und Nordrhein-Westfalen, von technischen Neuerungen in Folge fortschreitender Digitalisierung sowie vom Spannungsverhältnis zwischen Innerer Sicherheit und Privatheit.

Zum letzten Aspekt nehme ich im Vergleich zum vorhergehenden Berichtszeitraum eine deutliche Schwerpunktverschiebung in der politischen Diskussion wahr. Wurde nach den Snowden-Enthüllungen noch eingehend erörtert, welche Maßnahmen möglich und nötig sind, um eine allumfassende staatliche Überwachung zu verhindern, so hat sich dies mit der politischen Debatte in Folge von Terroranschlägen und Amokläufen geändert: Nunmehr wächst die Bereitschaft, mit Hinweis auf Sicherheitserwägungen die Grundrechte einzuschränken. Staatliche Sicherheitsmaßnahmen haben Konjunktur und nach Meinung vieler auch Vorrang vor der informationellen Selbstbestimmung der Einzelnen. Solche Perspektivwechsel in der öffentlichen Debatte verändern jedoch nicht den Auftrag der Landesbeauftragten. Gerade in Zeiten, in denen Freiheitsrechte durch Ausweitung staatlicher Überwachungsmöglichkeiten in Gefahr geraten, halte ich es für entscheidend, als unabhängige Kontrollinstanz für das Grundrecht auf informationelle Selbstbestimmung einzustehen.

Auch die EU-Datenschutz-Grundverordnung trifft eine klare Aussage zugunsten unabhängiger Aufsichtsbehörden mit erweiterten Befugnissen. In diesem Sinne sehe ich mich gestärkt als Ansprechpartnerin für Landtag und Landesregierung, für Wirtschaft und Verwaltung sowie vor allem für die Bürgerinnen und Bürger. Durch standfestes Eintreten für das Grundrecht mit Augenmaß für konstruktive Lösungen möchte ich auf Ergebnisse hinwirken, die datenschutzgerecht und gleichzeitig – soweit möglich – auch aus Sicht der verantwortlichen Stellen zielführend sind.

Genauso wichtig ist mir, das noch ver-

gleichsweise junge Recht auf Informationsfreiheit in Nordrhein-Westfalen weiter voranzubringen. Ich sehe mich primär als Beraterin der Bürgerinnen und Bürger wie auch der verantwortlichen Stellen und nehme meine Ombudsaufgabe ernst, in Streitfällen zwischen beiden Seiten zu vermitteln. Den Gesetzgeber gilt es überdies zu überzeugen, das bestehende Recht im Sinne von Open Data weiterzuentwickeln und ein Transparenzgesetz zu schaffen, das nicht nur den Zugang zu Informationen auf Antrag, sondern auch die antragsunabhängige Verpflichtung der Behörden zur Veröffentlichung von Informationen vorsieht.

Als ich die Leitung der Behörde übernahm, habe ich ein gut aufgestelltes Team vorgefunden. Ich danke Herrn Lepper, der vorausschauend auf eine Erweiterung der Stellen hingewirkt hatte.

Bedanken möchte ich mich bei den Abgeordneten des Landtages, die erkannt haben, dass die Aufsichtsbehörde – zur Vorbereitung auf die Herausforderungen im Zusammenhang mit den neuen Aufgaben durch die EU-Reform – einer angemessenen Ausstattung bedarf. Ob mit dem bisher erreichten Stand allen Anforderungen des neuen Rechtes entsprochen werden kann, wird die Praxis zeigen.

Mein Dank gilt nicht zuletzt meinen Mitarbeiterinnen und Mitarbeitern für die ausgezeichnete Unterstützung. Ohne das engagierte Team wären die Aufgaben als Datenschutz- und Informationsfreiheitsbeauftragte nicht zu leisten.

Helga Block
Frühjahr 2017

2. Überblick

■ EU-Datenschutzreform

Die EU steht vor einer tiefgreifenden Veränderung des Datenschutzrechts: Ab Mai 2018 wird sich das Recht in den Mitgliedstaaten an den Vorgaben der unmittelbar geltenden **Datenschutz-Grundverordnung (DS-GVO)** und an der noch umzusetzenden **Datenschutz-Richtlinie im Bereich Justiz und Inneres (JI-RL)** ausrichten.

Ein wichtiger Schwerpunkt im Berichtszeitraum war deshalb die Vorbereitung auf diesen Umbruch im Datenschutzrecht.

Die Jahre 2015 und 2016 waren zunächst von dem Ringen um den Inhalt der DS-GVO und der JI-RL geprägt. Nach langen Verhandlungen hat das Europäische Parlament die DS-GVO und die JI-RL verabschiedet. In der Phase des europäischen Gesetzgebungsverfahrens haben wir unsere Kernanliegen in die Debatte eingebracht. Zuvorderst ging es darum, eine Absenkung des Datenschutzniveaus zu verhindern. Im Verbund mit den anderen deutschen Datenschutzbehörden ist es uns gelungen, einige wichtige Anliegen durchzusetzen.

Nach der Verabschiedung der Regelwerke der DS-GVO stehen nunmehr die **Bundes- und Landesgesetze auf dem Prüfstand**. Bis Mai 2018 müssen der Bund und die Länder ihre Gesetze an die neue Rechtslage anpassen.

Auf Landesebene stehen wir dazu der Landesregierung und dem Landtag beratend zur Seite.

Auf Bundesebene ist es dabei eine besondere Herausforderung, bei den aufsichtsrechtlichen Verfahren auf europäischer Ebene die Besonderheiten des Föderalismus zu berücksichtigen. Wir setzen uns dafür ein, dass die Einflussmöglichkeiten der jeweils zuständigen Aufsichtsbehörden der Länder gewahrt bleiben.

Nicht nur die Gesetzgeber, auch Wirtschaft und Verwaltung sowie die Datenschutzaufsichtsbehörden müssen sich vorbereiten. Auch auf die Bürgerinnen und Bürger kommen Änderungen zu.

Auf unserer Homepage informieren wir über Grundsatzfragen und aktuelle Entwicklungen zu diesem komplexen Thema. (Siehe hierzu unter 3.)

■ Von Safe Harbor zu EU-US Privacy Shield

Im Oktober 2015 hat der Europäische Gerichtshof die Safe-Harbor-Entscheidung der EU-Kommission für ungültig erklärt. Unternehmen können personenbezogene Daten damit nicht mehr auf der Grundlage von Safe Harbor in die USA übermitteln. Inzwischen ist das **EU-US Privacy Shield** als Nachfolgeregelung in Kraft. Wir stellen dazu umfangreiche Informationen und Interpretationshilfen auf unserer Homepage

zur Verfügung. Außerdem beteiligen wir uns an einer länderübergreifenden Prüfaktion zu Datenübermittlungen in das Nicht-EU-Ausland. Dazu haben wir in NRW 150 Unternehmen unterschiedlicher Branchen und Größen um Auskunft gebeten. (Siehe hierzu unter 4.)

■ Innere Sicherheit

Im Bereich der Inneren Sicherheit waren wir in zahlreichen Einzelfällen beratend tätig. Kritisch Stellung genommen haben wir zu den Novellierungen des **Verfassungsschutzgesetzes NRW** und des **Polizeigesetzes NRW**.

Außerdem haben wir mehrere Dateien im Sicherheitsbereich kontrolliert. So galt es turnusgemäß die **Antiterrordatei** zu überprüfen (§ 10 Antiterrordateigesetz). Erfreulicherweise konnten wir weder beim Verfassungsschutz NRW noch beim Landeskriminalamt NRW Datenschutzverstöße feststellen. Zu anderen Ergebnissen führte hingegen die Kontrolle der **Falldatei Rauschgift**. Hierbei deckten wir zahlreiche Datenschutzmängel auf. Aufgrund unserer Kontrollergebnisse wurden bereits über 112.000 der insgesamt 180.000 Datensätze gelöscht. Begonnen haben wir ferner mit der Überprüfung der sechs **Videoüberwachungsanlagen**, die insbesondere infolge der Silvesternacht 2015 von verschiedenen Polizeipräsidien in NRW installiert wurden. (Siehe hierzu unter 5.3)

■ Videoüberwachung

Eine Vielzahl von Eingaben mit steigender Tendenz betrifft die **Videoüberwachung durch Private**. Die Bürgerinnen und Bürger sind nicht bereit, die vielen Kameras im öffentlichen Raum wie in Bahnhöfen und Kaufhäusern oder auch am Arbeitsplatz hinzunehmen. Unsere Beratungserfahrung zeigt, dass die geltende Rechtslage im Einzelfall eine angemessene Abwägung zwischen den Interessen der für die Kamerainstallation Verantwortlichen und dem Recht der Bürgerinnen und Bürger auf Privatheit ermöglicht. Weder erforderlich noch zielführend ist daher eine Erweiterung der Videoüberwachungsbefugnisse für Private – wie im Entwurf des Bundesministeriums des Innern für ein „Videoüberwachungsverbesserungsgesetz“ vorgesehen. Es nicht die Aufgabe privater Stellen, die Sicherheit der Bevölkerung zu gewährleisten. Dies ist eine Kernaufgabe des Staates. Mehr Videoüberwachung führt überdies nicht automatisch zu mehr Sicherheit. (Siehe hierzu unter 14.)

■ Datenschutz in der Wirtschaft

Die bisher für Unternehmen einschlägigen Regelungen des deutschen Datenschutzrechts werden weitgehend durch die DS-GVO ersetzt. Das BDSG wird neu gefasst. Zur verbindlichen und einheitlichen Auslegung der DS-GVO ist insbesondere der Europäische Datenschutzausschuss berufen. Wir beraten die Wirtschaft bei den Vorbereitungen und stimmen uns in Grundsatzfragen bereits mit den deutschen Aufsichtsbehörden ab. So hat sich der Düsseldorfer Kreis – das Koordinierungsgremium der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder für den nicht-öf-

fentlichen Bereich – unter Vorsitz NRW wegen der grundlegenden Bedeutung von Einwilligungen auf Kriterien verständigt, nach denen bisher erteilte **Einwilligungen unter der DS-GVO fortgelten**.

In der Beratungspraxis ist festzustellen, dass bei der Entwicklung neuer Geschäftsmodelle oder Technologien der Datenschutz leider erst spät berücksichtigt wird. Dabei lassen sich bei der frühzeitigen Beachtung des Datenschutzes bereits bei der Technikgestaltung oft datenschutzfreundliche Lösungen finden.

Immobilienmaklerprüfung
Wir haben in Abstimmung mit dem Bayerischen Landesamt für Datenschutzaufsicht die Datenverarbeitung in der Wohnungswirtschaft geprüft. Vor allem Datenerhebungen und Mieterselbstauskünfte im Vorfeld von Mietverträgen waren zu kritisieren. Es hat sich gezeigt, dass die Verantwortlichen in diesem Wirtschaftszweig fortgesetzt für den Datenschutz sensibilisiert werden müssen. Wir werden das Thema weiter verfolgen und unsere Beratungen fortsetzen. (Siehe hierzu unter 15.1)

Fahrerbewertungsportal
Wir haben den Betrieb eines privaten Internetportals zur Bewertung von Fahrerverhalten durch Auflagen eingeschränkt. Das Verhalten von Menschen im privaten Umfeld zu bewerten und im Internet zu veröffentlichen, verletzt in unzulässiger Weise die Grundrechte der Bewerteten. Das Verwaltungsgericht hat unsere aufsichtsrechtlichen Maßnahmen bestätigt. (Siehe hierzu unter 15.2)

Wearables
Gemeinsam mit weiteren Datenschutzaufsichtsbehörden haben wir 16 Wearable-Computer wie Smart-Watches, Fitness-Armbänder oder Activity-Tracker geprüft, die einen Marktanteil von etwa 70 Prozent in Deutschland abdecken. Die Ergebnisse der Prüfung zeigen zahlreiche Mängel auf. (Siehe hierzu unter 10.6)

■ E-Government

Das Gesetz zur Förderung der elektronischen Verwaltung in NRW (**EGovG NRW**) schafft die Grundlage für eine moderne Kommunikation mit und innerhalb der öffentlichen Verwaltung. Wie schon bei der Abstimmung des Gesetzentwurfes und der untergesetzlichen Normen werden wir auch bei der Umsetzung der zahlreichen Maßnahmen des EGovG NRW darauf achten, dass datenschutzrechtliche Grundsätze – wie Datensparsamkeit und Datenvermeidung – beachtet werden. Ich begrüße daher die Möglichkeit, im zentralen Koordinierungs- und Entscheidungsgremium **E-Government-Rat** als Vertreterin mit Gaststatus mitwirken zu können.

Durch die neuen Kommunikations- und Interaktionswege wird die Verwaltung für die Bürgerinnen und Bürger unkomplizierter erreichbar und Informationen werden schneller und leichter zugänglich. Das kann aber nur ein erster Schritt in Richtung transparenten Verwaltungshandelns sein. (Siehe hierzu unter 8.)

■ Informationsfreiheit und Transparenz

Das **Informationsfreiheitsgesetz Nordrhein-Westfalen** (IFG NRW) hat sich in seinem nunmehr 15-jährigen Bestehen bewährt. Gleichwohl besteht immer wieder die Notwendigkeit informationspflichtige Stellen zu mehr Transparenz anzuhalten. Hier möchten wir die erforderlichen Einzelfallberatungen in den nächsten Jahren verstärkt durch den Ausbau von Vortrags- und Schulungsangeboten für Beschäftigte der Behörden flankieren.

Im Jahr 2016 hatte NRW den Vorsitz in der **Informationsfreiheitskonferenz**. Während der Informationsfreiheitsbeauftragte aus Rheinland-Pfalz berichten konnte, dass dort Ende 2015 ein **Transparenzgesetz** verabschiedet wurde, gab es aus NRW leider nichts Vergleichbares zu vermelden.

Trotz der schon im letzten Bericht angemahnten Umsetzung des Koalitionsvertrages fehlt es in NRW nach wie vor an einem Transparenzgesetz, das öffentliche Stellen verbindlich dazu verpflichtet, bestimmte Informationen unabhängig vom Behördenwillen im Internet zu veröffentlichen. Die aktive Bereitstellung von Informationen erhöht die Transparenz der Verwaltung, die Nachvollziehbarkeit, Akzeptanz und Kontrolle behördlicher Entscheidungsprozesse und ist damit für den demokratischen Willensbildungsprozess essentiell. Das Vorhaben, das IFG NRW im Rahmen von Open Data zu einem solchen Transparenzgesetz weiterzuentwickeln, muss endlich in die Tat umgesetzt werden. Immerhin zählte NRW bei Inkrafttreten des Gesetzes im Jahr 2002 zu den Vorreitern der Informationsfreiheit in Deutschland. Jetzt, 15 Jahre später, gibt es Transparenzgesetze in anderen Ländern, die umfangreiche Verpflichtungen zur proaktiven Veröffentlichung festschreiben – NRW gehört noch immer nicht dazu. Hier gibt es auf der Ebene der Landesgesetzgebung dringenden Handlungsbedarf. (Siehe hierzu unter 16.)

■ Beratung und Information der Öffentlichkeit

Öffentlichkeitsarbeit ist ein wichtiger Baustein, um die Bedeutung des Datenschutzes und der Informationsfreiheit zu vermitteln. Wir informieren auf unserer Internetseite Bürgerinnen und Bürger, Wirtschaft und öffentliche Stellen. Zudem haben wir Orientierungshilfen und Broschüren erstellt und an zahlreichen Informations- und Diskussionsveranstaltungen teilgenommen sowie Vorträge gehalten.

Die vielen **Presseanfragen** zeigen, dass das Interesse der Medien an den Themen Datenschutz und Informationsfreiheit zunimmt. Wir informieren die Presse regelmäßig nicht nur auf Anfrage, sondern auch mit unseren Pressemitteilungen.

Selbstdatenschutz wird zunehmend wichtiger, denn gegenüber ausländischen Internetdiensten oder internationalen Geheimdiensten sind die Möglichkeiten der deutschen Datenschutzaufsichtsbehörden begrenzt. Erforderlich ist daher

neben dem Wissen um die Gefahren auch die Kenntnis von Gegenmaßnahmen. Diese sind in der Regel leicht zu erlernen und nach derzeitigem Kenntnisstand wirksam einsetzbar. Hinweise zum Selbstdatenschutz geben wir unter anderem auf unserer Internetseite.

Gemeinsam mit der **Verbraucherzentrale NRW** haben wir die **Broschüre „Ihre Daten gehören Ihnen – Datensparsamkeit lohnt sich“** herausgegeben. Mit dem **Chaos Computer Club Düsseldorf (CCCD)** fand im Mai 2015 im Hause der LDI NRW die zweite **Cryptoparty** statt. Interessierte konnten sich über Möglichkeiten der Verschlüsselung von E-Mails sowie Festplatten informieren und praktisch anwenden. Unser Dank gilt dem CCCD und allen Interessierten für die Vorbereitung und Teilnahme an der Veranstaltung.

Darüber hinaus beteiligen wir uns gemeinsamen mit den Datenschützern des Bundes und der Länder an der Website www.youngdata.de. Insbesondere Jugendliche können sich hier zu Themen des Datenschutzes und der Informationsfreiheit informieren. Um Jugendlichen darüber hinaus Kompetenzen im Umgang mit Medien zu vermitteln, setzen wir uns für das Thema **Medienkompetenz** in den Lehrplänen der Schulen ein. Dazu sind zunächst die Lehrkräfte in der universitären Ausbildung auf diesem Gebiet zu schulen. Gemeinsam mit der Kultusministerkonferenz (KMK) haben wir daran mitgewirkt, Strategien zur Bildung in der digitalen Welt zu erarbeiten. Besonders begrüßenswert ist, dass das von der KMK entwickelte Kompetenzmodell zur Medienbildung für die Länder verpflichtend sein soll.

■ Ansprechpartnerin der Bürgerinnen und Bürger

Wir sind vor allem für die Bürgerinnen und Bürger da. Das Anrufungsrecht ist sowohl im Datenschutzgesetz NRW (DSG NRW) als auch im IFG NRW ausdrücklich festgeschrieben – und wir nehmen diesen Auftrag sehr ernst. Die Zahl der **Beschwerden und Beratungsanfragen** lag in den vergangenen Jahren regelmäßig bei rund 4.000 jährlich. Im Jahr 2016 verzeichneten wir mit etwa **4.400** eine **Steigerung von rund 10 Prozent** gegenüber dem Vorjahr. Davon nicht erfasst sind die vielen Beratungen, in denen wir Bürgerinnen und Bürgern, Unternehmen und Behörden etwa bereits am Telefon schnell weiterhelfen konnten.

■ Ausblick

Das Jahr 2018 steht für uns nicht nur unter dem Vorzeichen der DS-GVO. Wir werden zudem turnusmäßig den **Vorsitz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder** von Niedersachsen übernehmen. Neben der Organisation der Konferenzen werden wichtige Abstimmungsprozesse zu koordinieren sein.

Mit der Anwendung der DS-GVO werden auf uns neue wichtige Aufgaben zukommen. Von besonderer Bedeutung ist die verbindliche internationale Abstimmung innerhalb kurzer Fristen. Die verpflichten-

de Beratung von Unternehmen und Behörden bei einzelnen Datenverarbeitungen (Vorherige Konsultation) bringt eine neue Ausrichtung unserer Aufgaben mit sich. Der Aufwand dafür ist schwer vorherzusehen.

Wir sind zuversichtlich, dass dem Landtag die Bedeutung des Datenschutzes und der Informationsfreiheit weiterhin bewusst bleibt und er eine angemessene Ausstattung der Aufsichtsbehörde gewährleisten wird.

3. Europäische Datenschutzreform

3.1. Datenschutz-Grundverordnung

Nach langen Verhandlungen hat das Europäische Parlament die Datenschutz-Grundverordnung (DS-GVO) verabschiedet. Das neue Recht wird im Mai 2018 anwendbar sein.

Ab dem 25. Mai 2018 wird die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (DS-GVO) als unmittelbar geltendes Recht anwendbar sein. In ihrem Regelungsbereich wird sie den bisherigen Vorschriften, insbesondere des Bundesdatenschutzgesetzes (BDSG), und des Datenschutzgesetzes NRW (DSG NRW) vorgehen. Das geltende Datenschutzrecht muss in vielen Bereichen angepasst werden.

Die Datenschutzreform soll besonders im Bereich der Wirtschaft künftig ein europaweit einheitliches hohes Schutzniveau gewährleisten, das ebenfalls europaweit einheitlich von den Datenschutzaufsichtsbehörden durchgesetzt werden soll. Zu diesem Zweck enthält die DS-GVO insbesondere Regelungen zu folgenden Punkten:

■ Marktortprinzip

Wer seine Geschäftstätigkeit auf die EU richtet, muss sich auch an europäisches Datenschutzrecht halten.

■ One-Stop-Shop

Unternehmen haben eine bestimmte Datenschutzaufsichtsbehörde als zuständigen Ansprechpartner.

■ Datenportabilität

Nutzerinnen und Nutzer von Diensten haben das Recht, bestimmte Daten von einem Anbieter so zu erhalten, dass zu einem anderen gewechselt werden kann.

■ Recht auf Löschung („Recht auf Vergessenwerden“)

Die DS-GVO enthält insbesondere das Recht auf Löschung von Links zu personenbezogenen Daten oder von Kopien oder Replikationen. Verantwortliche haben hierzu unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen zu ergreifen.

■ Privacy by Design und by Default

Anbieter haben bereits in der Phase der Entwicklung ihre Produkte und Dienstleistungen datenschutzfreundlich zu gestalten. Sie haben durch datenschutzfreundliche Voreinstellungen dafür zu sorgen, dass grundsätzlich nur die für den jeweiligen Zweck erhobenen personenbezogenen Daten verarbeitet werden.

■ Zweckbindung

Erhobene Daten dürfen nur für den Zweck, zu dem sie erhoben wurden oder für damit vereinbare Zwecke verarbeitet werden.

■ Betriebliche Datenschutzbeauftragte

Unternehmen müssen Datenschutzbeauftragte bestellen, wenn die Datenverarbeitung risikobehaftet ist oder wenn die Mitgliedstaaten hierzu Regelungen vorsehen.

■ Verbesserte Durchsetzung

Die Datenschutzaufsichtsbehörden erhalten erweiterte Befugnisse. Jede betroffene Person soll sich bei Verstößen an die örtliche Behörde wenden können. Es sind zudem erhöhte Geldbußen in Höhe von bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens vorgesehen.

■ Europäischer Datenschutzausschuss (EDSA)

Der Vollzug der DS-GVO erfordert in grenzüberschreitenden Fällen eine effektive Organisationsstruktur. Zentrale Bedeutung kommt dabei dem neu geschaffenen EDSA zu, der für alle Aufsichtsbehörden verbindliche Beschlüsse treffen kann und in dem jeder Mitgliedstaat eine Stimme hat.

■ Datenschutz-Folgenabschätzung

Eine Folgenabschätzung muss durchgeführt werden, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

■ Vorherige Konsultation

Verantwortliche sind verpflichtet, vor der Verarbeitung die Aufsichtsbehörde zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, und keine Maßnahmen zur Eindämmung des Risikos getroffen wurden.

■ Akkreditierung und Zertifizierung

Schließlich enthält die DS-GVO für die zuständigen Aufsichtsbehörden Regelungen zur Akkreditierung und zur Zertifizierung sowie für ein Europäisches Datenschutzsiegel bei gemeinsamer Zertifizierung.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich bereits während des europäischen Gesetzgebungsverfahrens zur DS-GVO geäußert. So hat die 89. Konferenz im März 2015 die Entschließung „Datenschutz-Grundverordnung darf keine Mogelpackung werden“ verabschiedet (Abdruck im Anhang). Hiermit reagierte sie auf Vorschläge des Rates der Europäischen Union, die ein Absenken des Datenschutzniveaus zur Folge gehabt hätten. Im August 2015 hat die Konferenz „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung“ formuliert und an das Europäische Parlament, die Kommission und den Rat der Europäischen Union gerichtet (Das Kernpunktepapier ist auf unserer Internetseite www.ldi.nrw.de abrufbar). In der DS-GVO wurden folgende Forderungen berücksichtigt:

- gesetzliche Bestimmung zur Datensparsamkeit
- klarer gefasste Definition des Begriffs „Personenbezogenes Datum“
- ausdrückliche Regelung, wonach eine

verantwortliche Stelle die Erbringung einer Leistung nicht davon abhängig machen darf, dass der Betroffene in die Verarbeitung weiterer Daten einwilligt, die hierfür nicht erforderlich sind (so genanntes Kopplungsverbot).

Nicht in der Verordnung aufgenommen wurden hingegen:

- weitergehende Forderungen nach Mindeststandards bei der Verarbeitung von Beschäftigtendaten sowie
- die ausdrückliche Verpflichtung für soziale Netzwerke, die Nutzung ihrer Dienste unter Pseudonym zu ermöglichen.

Zur Beratung der Unternehmen sowie der Bürgerinnen und Bürger haben wir zunächst einen Überblick über die Änderungen der DS-GVO auf unserer Homepage veröffentlicht. Die Information der Fachöffentlichkeit über die Auslegung einzelner Bestimmungen der DS-GVO hat ebenfalls begonnen. Dazu gehören Vorträge auf Fachveranstaltungen und Beiträge auf unserer Homepage, die kontinuierlich ausgebaut werden.

Nicht zuletzt bei diesen Aufgaben wird eine neue Herausforderung deutlich: Es genügt nicht, dass sich eine deutsche Aufsichtsbehörde eine Auffassung zum neuen Recht bildet und diese mit den übrigen Datenschutzbehörden in Deutschland abstimmt. Vielmehr muss bereits jetzt ein europaweit einheitliches Verständnis angestrebt werden. Dazu kommt, dass das europäische Recht selbst oft wenig detaillierte Vorgaben macht, so dass eine gemeinsame Auslegung und Anwendung von Grund auf zu entwickeln ist. Das ist eine zeitaufwändige und umfangreiche Aufgabe. Die Verfahren für eine verbindliche europäische Meinungsbildung der Aufsichtsbehörden sind zudem noch nicht in Kraft. Um trotzdem zügig die Umstellung auf das neue Recht zu unterstützen, geben wir schon jetzt Hinweise zur Rechtslage, die in wichtigen Fragen europa- bzw. deutschlandweit koordiniert sind. Hierzu gehören die Arbeitspapiere der Artikel 29-Gruppe zur Datenübertragbarkeit, zum betrieblichen Datenschutzbeauftragten sowie zur Bestimmung der zuständigen Aufsichtsbehörde nach der DS-GVO. Ebenso gehört hierzu der Beschluss des Düsseldorfer Kreises zur Fortgeltung von Einwilligungen nach Anwendbarkeit der DS-GVO (Abdruck im Anhang). Allerdings gilt hier der Vorbehalt, dass derzeit gefasste Meinungen später durch verbindliche Entscheidungen im Ausschuss abgeändert werden können.

Zur Vorbereitung auf die europäischen Verfahren der Zusammenarbeit und der Kohärenz werden unsere Mitarbeiterinnen und Mitarbeiter in englischer Sprache geschult. Zudem beteiligen wir uns an der Organisation der europäischen Prozesse zum Beispiel beim Aufbau eines Informationssystems oder bei der Geschäftsordnung des Europäischen Datenschutzausschusses.

Die DS-GVO stellt alle, die das neue Recht anwenden, vor Herausforderungen. Wir beraten Politik, Wirtschaft, Verwaltung und nicht zuletzt Bürgerinnen und Bürger in NRW zu Fragen zum neuen europäischen Datenschutzrecht.

3.2 JI-Richtlinie

Die JI-Richtlinie regelt die Datenverarbeitung in den Bereichen Polizei und Justiz und soll erstmalig eine Mindestharmonisierung in der EU herbeiführen. Das europäische Gesetzgebungsverfahren wurde und die Umsetzung in nationales Recht wird von den Datenschutzaufsichtsbehörden kritisch begleitet.

Im Vergleich zur DS-GVO stand weniger im Blickfeld der Öffentlichkeit das Gesetzgebungsverfahren zur „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ (JI-RL). Insbesondere wegen ihrer sensiblen Regelungsmaterie ist die JI-RL allerdings nicht weniger gewichtig. Da sie sowohl die Datenverarbeitung zu präventiven als auch zu repressiven Zwecken erfasst, betreffen die Umsetzungsaufträge den Bundesgesetzgeber ebenso wie die für das allgemeine Polizeirecht zuständigen Bundesländer. So hat sich die Datenschutzkonferenz von Beginn an und nachfolgend mehrfach öffentlich zur JI-RL positioniert, unter anderem mit der Entschließung „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres“ vom 29. Oktober 2015. Die Entschließung ist im Anhang abgedruckt und über unserer Homepage www.ldi.nrw.de abrufbar.

Die JI-RL verpflichtet die Mitgliedstaaten zur Umsetzung in ihr nationales Recht bis zum 6. Mai 2018. Ziel ist es zum einen, in den Bereichen Polizei und Justiz eine Mindestharmonisierung des Datenschutzes innerhalb der EU herbeizuführen. Zum anderen soll die grenzüberschreitende Zusammenarbeit zur Bekämpfung von Straftaten geregelt werden. Die Regelungen stärken das in der EU-Grundrechte-Charta gewährleistete Recht auf Datenschutz und geben den einzelnen Bürgerinnen und Bürgern mehr Kontrolle über ihre persönlichen Daten.

Dabei wird deutlich, dass die Voraussetzungen der DS-GVO und der JI-RL für eine zulässige Datenverarbeitung eng aufeinander abgestimmt sind und sich gegenseitig ergänzen sollen. Die JI-RL hält verschiedene Differenzierungen bereit, um dem besonders eingriffsintensiven Regelungsbereich Rechnung zu tragen. Beispielsweise erfordern besonders sensible Daten eine strenge Erforderlichkeitsprüfung und zusätzliche Sicherungen. Im nationalen Recht sind Lösch- und Prüffristen zu regeln und bei der Verarbeitung ist zu differenzieren, ob die Betroffenen als Verdächtige, Verurteilte, Opfer, Zeugen oder Hinweisgeber erfasst sind. Stellt sich die Unrichtigkeit oder Unvollständigkeit

von Daten heraus, sind Korrekturen und bei Übermittlungen Benachrichtigungen vorzusehen. Darüber hinaus wird besonderes Augenmerk auf die Anforderungen und Regelungsspielräume hinsichtlich Zweckänderung, Betroffenenrechten, Verantwortlichkeit und Datenübermittlung ins Ausland zu legen sein.

Eine Vielzahl von bundes- und landesrechtlichen Regelungen ist folglich am Maßstab der JI-RL zu überprüfen und gegebenenfalls anzupassen. Dabei ist hervorzuheben:

- Bei den Vorgaben der JI-RL handelt es sich um Mindestanforderungen.
- Die JI-RL soll ein hohes Schutzniveau in der gesamten Union gewährleisten.

Im Ergebnis sind die Mitgliedstaaten damit nicht daran gehindert, zum Schutz der Rechte und Freiheiten der betroffenen Person Garantien festzulegen, die strenger sind als die Garantien der JI-RL. Zudem darf es in Staaten mit einem derzeit höheren Datenschutzniveau durch die Umsetzung in Zukunft nicht zu einer „Angleichung nach unten“ kommen.

Die Datenschutzaufsichtsbehörden sprechen sich für eine weitgehend einheitliche Umsetzung der JI-RL innerhalb Deutschlands aus. Dort wo nationales Recht bereits ein höheres Schutzniveau gewährleistet, ist sicherzustellen, dass dieses ausnahmslos erhalten bleibt. Auslegungs- und Umsetzungsspielräume sind in diesem Sinne auszufüllen.

3.3 Anpassung auf Bundesebene

Bis zur Anwendbarkeit der DS-GVO und Umsetzungsfrist der JI-Richtlinie im Mai 2018 muss der Bundesgesetzgeber das Datenschutzrecht des Bundes auf die Vereinbarkeit mit dem europäischen Recht überprüfen und gegebenenfalls anpassen.

Auf ihrer 91. Konferenz im April 2016 verabschiedeten die unabhängigen Datenschutzbehörden des Bundes und der Länder die Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen“ (Abdruck im Anhang). Darin wurden die nationalen Gesetzgeber aufgefordert, die in der DS-GVO enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen, insbesondere durch:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung des bestehenden Schutzniveaus des Bundesdatenschutzgesetzes (BDSG),
- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden und
- Beibehaltung der Verpflichtung des BDSG, einen betrieblichen Datenschutzbeauftragten zu bestellen.

Im Februar 2017 veröffentlichte das Bundesministerium des Innern den vom Bundeskabinett beschlossenen Entwurf für ein Gesetz zur Anpassung datenschutzrechtlicher Vorschriften des Bundes an die DS-GVO und zur Umsetzung der JI-RL (DSAnpUG-EU). Zur Zeit der Berichtserstellung war das Gesetzgebungsverfahren noch nicht abgeschlossen. Der Entwurf enthielt zum größten Teil Vorschläge zur Änderung des BDSG. Darin sind die genannten Forderungen der 91. Konferenz zwar zum Teil berücksichtigt. In einer gemeinsamen Pressemitteilung vom 1. Februar 2017 (Abdruck im Anhang) kritisierten die unabhängigen Datenschutzbehörden der Länder jedoch

- die angestrebte Absenkung des Datenschutzniveaus bei den Betroffenenrechten auf Information, Auskunft und Löschung,
- die Einschränkung der Aufsichtsbefugnisse gegenüber Berufsgeheimnisträgern,
- die sehr weitgehenden Regelungen zur Verarbeitung von Gesundheitsdaten,
- die Aushöhlung des Zweckbindungsgebots durch weitgehende Ausnahmeregelungen,
- die Vorschriften zur Ausweitung der Videoüberwachung und
- die Regelung zur Bestimmung des gemeinsamen Vertreters bzw. der gemeinsamen Vertreterin im Europäischen Datenschutzausschuss und das Verfahren zur Festlegung der inhaltlichen Positionierung Deutschlands im EDSA (siehe hierzu unter anderem die „Kühlungsborner Erklärung“ der Landesbeauftragten für den Datenschutz

vom 10. November 2016, im Anhang abgedruckt und auf unserer Internetseite www.ldi.nrw.de abrufbar).

Das DSAnpUG-EU wird bei der Umsetzung der JI-RL an vielen Stellen schon den Umsetzungsbefehlen der JI-RL nicht gerecht. Dies gilt insbesondere hinsichtlich besonders eingriffsintensiver Datenverarbeitungen und der Verarbeitung zu anderen Zwecken.

Wir stehen mit dem Bundesinnenministerium, der Innenministerkonferenz sowie dem Ministerium für Inneres und Kommunales NRW zu Fragen der Anpassung des Bundesrechts im Rahmen der Datenschutzreform in Kontakt, begleiten das Gesetzgebungsverfahren und formulieren Änderungsvorschläge an den Gesetzgeber. Ziel unserer Gespräche und Stellungnahmen ist, zum einen das Schutzniveau der DS-GVO nicht durch Ausnahmetatbestände im nationalen Recht abzusenken. Zum anderen sollen datenschutzfreundliche Regeln im Bundesrecht so weit wie möglich übernommen werden. Wir setzen uns zudem dafür ein, beim aufsichtsrechtlichen Verfahren auf europäischer Ebene den Föderalismus so zu berücksichtigen, dass den Aufgaben und Befugnissen der Landesaufsichtsbehörden angemessen Rechnung getragen wird.

Wir beraten im Gesetzgebungsverfahren mit dem Ziel, einen hohen Datenschutzstandard zu erhalten.

3.4 Anpassung auf Landesebene

Die europäische Datenschutzreform betrifft auch das Recht des Landes NRW. Bis Mai 2018 sind umfangreiche Arbeiten erforderlich, um das Datenschutzrecht des Landes zu prüfen und europarechtskonform zu gestalten.

Die erforderliche Neugestaltung des Datenschutzrechts im Land NRW betrifft nicht nur die allgemeinen Regelungen im Datenschutzgesetz Nordrhein-Westfalen, sondern auch alle Datenschutzvorschriften in bereichsspezifischen Landesgesetzen. Zum einen müssen die vorhandenen Regelungen daraufhin überprüft werden, inwieweit sie aufgrund der direkten Anwendbarkeit der DS-GVO obsolet geworden sind und inwieweit die verbleibenden Regelungen mit dem europäischen Datenschutzrecht vereinbar sind. Zum anderen müssen europarechtliche Regelungsaufträge, insbesondere im Bereich der JI-RL, umgesetzt und Regelungsoptionen geprüft werden. Hierbei handelt es sich zum Beispiel um folgende Aspekte:

- Für die Datenverarbeitung zur Erfüllung von Aufgaben, die im öffentlichen Interesse liegen, verweist die DS-GVO auf das Recht der Mitgliedsstaaten und macht zugleich Vorgaben, denen die jeweilige Rechtsgrundlage entsprechen muss. In diesem Bereich ist also eine Revision bestehender Normen des allgemeinen und bereichsspezifischen Rechts vorzunehmen.
- Sollen Betroffenenrechte, wie zum Beispiel Auskunfts- oder Löschungsrechte, aus besonderen Gründen beschränkt werden, müssen diese Beschränkungen daraufhin überprüft werden, ob sie den Zielen und Anforderungen entsprechen, die die DS-GVO in Art. 23 abschließend auflistet. Auch nationale Zweckänderungserlaubnisse erlaubt die DS-GVO nur in diesem Rahmen.
- Im Anwendungsbereich der JI-RL sind spezifische Regelungen vor allem im Polizeirecht zu treffen und bestehende Regelungen zu überprüfen. Dabei ist zum Beispiel zu berücksichtigen, dass die JI-RL keine Regelung dazu trifft, ob auch die Einwilligung als Rechtfertigungsgrund für die Datenverarbeitung von den Mitgliedstaaten vorgesehen werden kann. Aus den Erwägungsgründen ergibt sich, dass in bestimmen Fällen der Verhütung und Verfolgung von Straftaten die Einwilligung keine alleinige rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen kann, da keine echte Wahlfreiheit des Betroffenen besteht.
- Stellung, Aufgaben und Befugnisse der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit müssen im Hinblick auf die europäischen Festlegungen neu überdacht und formuliert werden. Hierbei ist auch zu entscheiden, ob die oder der Landesbeauftragte befugt sein soll, Bußgelder gegenüber öffentlichen Stellen zu verhängen.

- Außerdem sind klare Regelungen zu treffen, um das Recht auf Schutz der personenbezogenen Daten mit der Meinungsfreiheit sowie dem so genannten „Medienprivileg“ in Einklang zu bringen, etwa im Presse- und Rundfunkrecht.
- Im Übrigen muss in allen betroffenen Normkomplexen die verwendete Terminologie an das europäische Regelwerk angepasst werden.

In der kommenden Legislaturperiode steht also eine umfangreiche Reform des Datenschutzrechts des Landes an. Wir werden diesen Prozess beratend begleiten. Dabei gilt: Das Datenschutzniveau sollte gehalten werden – sowohl im Vergleich zum europäischen Recht als auch zum bisherigen Landesrecht.

Wir werden uns weiterhin für einen hohen Datenschutzstandard einsetzen.

3.5 E-Privacy-Richtlinie/Verordnung

Nach der DS-GVO und der JI-Richtlinie reformiert die Europäische Union ebenfalls die datenschutzrechtlichen Vorgaben für Dienste der elektronischen Kommunikation (RL 2002/58/EG, so genannte E-Privacy-Richtlinie). Auch diesbezüglich gilt es, ein Absenken des Datenschutzniveaus zu verhindern.

Die E-Privacy-Richtlinie aus dem Jahr 2002 regelt den Datenschutz für Dienste der elektronischen Kommunikation. Sie gilt vorwiegend für geschäftsmäßige Anbieter von Telekommunikationsdiensten für Dritte und ist im nationalen Recht in der Hauptsache im Telekommunikationsgesetz umgesetzt. Darüber hinaus enthält sie jedoch auch einzelne Regelungen für Betreiber von Internetseiten im Sinne des Telemediengesetzes (Cookie-Regelung).

Im Januar 2017 stellte die EU-Kommission ihre Vorschläge für eine Neuregelung der E-Privacy-Richtlinie vor. Wesentliche inhaltliche Neuerung ist, dass der Regelungsbereich auf so genannte Over-The-Top-Dienste (OTT-Dienste) erweitert werden soll. Damit sind neue Kommunikationsdienste wie WhatsApp, Skype oder GoogleMail gemeint. Diese finden immer mehr Verbreitung und treten zunehmend in Konkurrenz zu herkömmlichen Telekommunikationsdiensten wie Telefon und SMS, auf welche die Vorgängerregelung zugeschnitten ist. Außerdem enthält der Entwurf der Kommission unter anderem Vorschläge:

- zu den Anforderungen an die Speicherung von Cookies auf dem Endgerät der Nutzerin oder des Nutzers zum Zweck des Tracking bzw. der Werbung,
- zur Befugnis beispielsweise IP-Adressen zu speichern, um Angriffe auf die Netze der Anbieter zu erkennen und abzuwehren,
- zur Anwendbarkeit der Vorschriften der DS-GVO zur Zusammenarbeit und zur Kohärenz auf grenzüberschreitende Angebote von Telekommunikationsdiensten sowie
- zur Änderung der Richtlinie in eine direkt anwendbare Verordnung.

Die Neuregelung ist Gegenstand der Debatte zwischen Internetunternehmen, Sicherheitsbehörden, Vertreterinnen und Vertretern des Verbraucherschutzes und des Datenschutzes sowie netzpolitischen Interessengruppen. Im Kern der Auseinandersetzung steht insbesondere die Erweiterung des Anwendungsbereichs der Richtlinie auf OTT-Dienste. Nach geltender Rechtslage ist umstritten, ob die E-Privacy-Richtlinie und das Telekommunikationsgesetz auf diese Dienste anwendbar sind. Hierzu gab es bislang unterschiedliche Auffassungen zwischen der nationalen Regulierungsbehörde Bundesnetzagentur und dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (BEREC, englisch: Body of European Regulators for Electronic Communication).

Positiv an einer Aufnahme der OTT-Dienste in die Verordnung wäre zum einen, dass damit in dieser Frage Rechtsklarheit geschaffen würde. Zum anderen wäre aus Sicht des Datenschutzes positiv zu bewerten, dass OTT-Dienste sich wie herkömmliche Telekommunikationsdienste ausdrücklich an das Telekommunikationsgeheimnis halten müssten. Negativ bewerten wir hingegen, dass mit der geplanten Ausweitung des Anwendungsbereichs auf OTT-Dienste diese ebenfalls zur Mitwirkung an staatlichen Maßnahmen der Telekommunikationsüberwachung bis hin zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten aufgrund nationaler Vorschriften verpflichtet sein könnten. Ob diese Maßnahmen gegenüber OTT-Diensten erfolgversprechend sind, ist zudem zweifelhaft. Vielfach können sich Nutzerinnen und Nutzer bei solchen Diensten nämlich unter Pseudonym anmelden. Außerdem bieten OTT-Dienste teilweise ihren Nutzerinnen und Nutzern bereits Ende-zu-Ende-Verschlüsselung ihrer Kommunikation an.

Wir haben uns im Vorfeld des Kommissionsentwurfs im Rahmen der Artikel-29-Arbeitsgruppe an einer gemeinsamen Stellungnahme der europäischen Datenschutzaufsichtsbehörden gegenüber der Europäischen Kommission zur Neuregelung der E-Privacy-Richtlinie beteiligt. Dabei haben wir zum einen darauf gedrungen, dass das Setzen von Cookies nur mit Einwilligung der Nutzerin oder des Nutzers der Internetseite zulässig ist. Zum anderen haben wir darauf hingewiesen, dass Verpflichtungen zur Datenspeicherung gegenüber OTT-Diensten eine Absenkung des Datenschutzniveaus darstellen.

Wir werden die Reform der E-Privacy-Richtlinie über das gesamte kommende Gesetzgebungsverfahren begleiten. Auch bei OTT-Diensten, die zunehmend an die Stelle herkömmlicher Telekommunikationsdienste treten, werden wir zugunsten der Nutzerinnen und Nutzer ein hohes Datenschutzniveau fordern.

4. Übermittlungsinstrumente für Datentransfers in Drittstaaten

Das moderne Wirtschaftsleben in einer digitalisierten Welt bedingt den Austausch personenbezogener Daten über nationale und europäische Grenzen hinweg. Dies gilt insbesondere für Datenübermittlungen in die USA. Basis für diese Datentransfers war lange die Angemessenheitsentscheidung der EU-Kommission zu den Safe-Harbor-Grundsätzen. Der Europäische Gerichtshof (EuGH) hatte diese im so genannten Schrems-Urteil für ungültig erklärt. Inzwischen ist das EU-US Privacy Shield als Nachfolger von Safe Harbor in Kraft. Einige Fragen sind jedoch noch offen.

Ob die USA tatsächlich ein angemessenes Schutzniveau „gewährleisten", habe die EU-Kommission in ihrer Angemessenheitsentscheidung nicht ausreichend begründet, so der EuGH (Urteil vom 6. Oktober 2015, Az. C-362/14). Zudem habe die EU-Kommission die Befugnisse der nationalen Datenschutzaufsichtsbehörden nicht einschränken können. Entsprechende Regelungen in solchen Entscheidungen seien unzulässig. Der EuGH fällte dabei keine Entscheidung zu den Inhalten der Safe-Harbor-Grundsätze. Bereits vor dem Urteil des EuGH hatte die EU-Kommission mit den USA darüber verhandelt, die Safe-Harbor-Grundsätze zu überarbeiten und zu verbessern. Auslöser des Verfahrens vor dem EuGH war eine Beschwerde des Österreichers Maximilian Schrems bei der irischen Datenschutzaufsichtsbehörde.

Unternehmen können personenbezogene Daten damit nicht mehr auf der Grundlage von Safe Harbor in die USA übermitteln. Sollten dennoch Datenübermittlungen auf dieser Grundlage erfolgen, würden wir sie untersagen und ggf. sanktionieren. Dazu bestand bisher keine Veranlassung.

Ergebnis der weiteren Verhandlungen der EU-Kommission mit den USA ist das so genannte EU-US Privacy Shield. Dabei handelt es sich um einen Selbstzertifizierungsmechanismus für US-amerikanische Unternehmen. Um daran teilnehmen zu dürfen, müssen sich die Unternehmen beim US-Handelsministerium registrieren. Das EU-US Privacy Shield definiert in seinen Datenschutzgrundsätzen Verpflichtungen, welche die Unternehmen einhalten müssen. Die EU-Kommission hat dazu im Juli 2016 festgestellt, dass unter den Regelungen des EU-US Privacy Shield ein angemessenes Datenschutzniveau für Datenübermittlungen in die USA besteht. Ob und wie sich das EU-US Privacy Shield bewährt hat, wird bei der ersten gemeinsamen jährlichen Evaluation der Regelungen in 2017 geprüft werden. Der genaue Zeitpunkt dafür steht noch nicht fest.

Auch die übrigen Übermittlungsinstrumente, wie Standardvertragsklauseln, stehen unter dem Vorbehalt möglicher Auswirkungen dieser Prüfergebnisse.

Bis Ende 2016 wurden außerdem auf EU-Ebene zwei Nichtigkeitsklagen gegen die Angemessenheitsentscheidung der EU-Kommission zum EU-US Privacy Shield erhoben. Ihr weiterer Verlauf ist noch offen.

Zudem hat die irische Datenschutzaufsichtsbehörde bei dem zuständigen irischen Gericht (High Court) beantragt, dem EuGH die Standardvertragsklauseln für Auftragsdatenverarbeiter vorzulegen. Ob und wann mit eine Vorlage an den EuGH stattfindet, ist offen.

Das Schrems-Urteil des EuGH enthält einen eindeutigen Auftrag an die nationalen europäischen Gesetzgeber, eine Klagemöglichkeit der Aufsichtsbehörden gegen Angemessenheitsentscheidungen der EU-Kommission zu schaffen. Gleichwohl gibt es diese in Deutschland bislang nicht. Die Datenschutzaufsichtsbehörden setzen sich dafür ein, dass dieser Auftrag in Deutschland zügig umgesetzt wird. Die Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder „Klagerecht für Datenschutzbehörden – EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein“ vom 20. April 2016 ist im Anhang abgedruckt und auf unserer Internetseite www.ldi.nrw.de abrufbar.

Zur weiteren Umsetzung der Aussagen des Schrems-Urteils änderte die EU-Kommission am 16. Dezember 2016 alle ihre weiteren Angemessenheitsbeschlüsse und ihre Beschlüsse zu den Standardvertragsklauseln. Bis dahin enthielten die Beschlüsse Regelungen, nach denen Aufsichtsbehörden Datenübermittlungen nur unter bestimmten Voraussetzungen aussetzen durften. Nun verweisen die Beschlüsse allgemein auf die Befugnisse der Aufsichtsbehörden. Die Änderungen enthalten außerdem zusätzliche Regelungen zur kontinuierlichen Überwachung der Angemessenheitsentscheidungen durch die EU-Kommission.

Vor diesem Hintergrund werden wir stärker darauf achten, dass datenübermittelnde Stellen die Übermittlungsinstrumente korrekt einsetzen. Für eine erste Orientierung sind auf unserer Homepage allgemeine Informationen zu internationalen Datenübermittlungen abrufbar, einschließlich Informationen zum EU-US Privacy Shield (www.ldi.nrw.de). Sie richten sich in erste Linie an Unternehmen in NRW. In unserer täglichen Arbeit beantworten wir viele Fragen von Unternehmen zu den Übermittlungsinstrumenten. Darunter sind komplexe Fragen zu den notwendigen Vertragsverhältnissen beim Einsatz von EU-Standardvertragsklauseln, zur Genehmigungsfreiheit von Ergänzungen zu EU-Standardvertragsklauseln oder zum Genehmigungsprozess von verbindlichen Unternehmensregelungen (so genannte Binding Corporate Rules, BCR).

Ende 2016 starteten wir gemeinsam mit neun Aufsichtsbehörden eine koordinierte schriftliche Prüfaktion zu Datenübermittlungen in das Nicht-EU-Ausland bei Unternehmen unterschiedlicher Branchen und

Größen. Wir haben die Unternehmen mit einem umfangreichen Fragebogen aufgefordert, Auskunft darüber zu geben, ob und ggf. in welchem Rahmen sie personenbezogene Daten in Nicht-EU-Länder übermitteln. Im Rahmen der Prüfaktion wird gezielt nach dem Einsatz von Produkten und Leistungen externer Anbieter in verschiedenen Bereichen wie Fernwartung, Support, Customer Relation Management (CRM) oder Bewerbermanagement gefragt. Mit der Prüfaktion sensibilisieren und beraten wir die Unternehmen. Darüber hinaus erhalten wir Informationen zu den Bereichen, in denen Datenübermittlungen in Drittländer stattfinden. Diese werden wir für unsere aufsichtsbehördliche Tätigkeit in NRW nutzen. Unsere Auswertung der Rückmeldungen ist noch nicht abgeschlossen.

Datenverarbeitende Stellen sollten weiterhin sorgfältig prüfen, ob sie Leistungen in Anspruch nehmen, bei denen Daten in Länder außerhalb der EU und des Europäischen Wirtschaftsraumes (Drittstaaten) übermittelt werden. Erfolgt ein Datentransfer in Drittstaaten empfehlen wir den datenverarbeitenden Stellen weiterhin dringend, für die technischen-organisatorischen Sicherungsmaßnahmen höchste Standards anzuwenden. Dazu ist zumindest eine starke Verschlüsselung zu empfehlen. Nutzerinnen und Nutzer können sich in Nutzungsbedingungen und Datenschutzerklärungen über vorgesehene Datenverarbeitungen in Drittstaaten informieren. Sie können sich dann bewusst entscheiden, ob sie das entsprechende Angebot nutzen möchten. Bleibt ein Angebot insoweit intransparent, raten wir davon ab.

5. Innere Sicherheit und Justiz

5.1 Bodycams – Änderungen des Polizeigesetzes NRW

In NRW werden demnächst etwa 200 ausgewählte Polizeibeamtinnen und -beamten Schulterkameras nebst kleinen Bildschirmen auf der Brust tragen. Die so genannten Bodycams sollen polizeiliche Einsätze mit Bild und Ton aufzeichnen.

Rechtsgrundlage für die Erprobung der Bodycams bildet der im Zuge der Änderung des Polizeigesetzes NRW (PolG NRW) neu eingefügte § 15c PolG NRW. Zum Schutz der Polizeibeamtinnen und -beamten können Personen, die im Rahmen einer Anhalte- und Kontrollsituation im öffentlichen und privaten Raum angetroffen werden, in Bild und Ton aufgenommen werden. Gegen eine damit einhergehende (probeweise) Ausweitung der Videoüberwachung durch die Polizei hatten wir bereits mit Stellungnahme vom 5. Januar 2015 (LT-Drs. 16/2453) gegenüber dem Landtag NRW Bedenken geäußert. Zur aktuellen Änderung des PolG NRW haben wir mit Stellungnahme vom 20. September 2016 darauf hingewiesen, dass mit dem Einsatz von Bodycams im öffentlichen und im privaten Bereich erheblich in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung, auf allgemeine Handlungsfreiheit sowie auf Unverletzlichkeit der Wohnung eingegriffen wird.

Zweifel bestehen zunächst an der Geeignetheit der Maßnahme. Belastbare wissenschaftliche Untersuchungen zur Wirksamkeit von Bodycams existieren nicht. Das Pilotprojekt im Bundesland Hessen wurde wissenschaftlich nicht begleitet, sodass dort lediglich „Erfahrungen“ der dortigen Polizei vorliegen; eine Wirkungsanalyse hat dagegen nicht stattgefunden. Die Frage der Erforderlichkeit ist ebenfalls nicht ausreichend beantwortet, denn mit der Vorschrift des § 15b PolG NRW existiert in NRW bereits eine Regelung, nach der Bildaufnahmen zur Eigensicherung in Polizeifahrzeugen unter bestimmten Voraussetzungen erlaubt sind. Vor der Schaffung weiterer Eingriffsbefugnisse hätte daher untersucht werden müssen, welche Wirkung der Einsatz optisch-elektronischer Mittel in Fahrzeugen der Polizei bisher gebracht hat. Schließlich bleibt völlig offen, auf welcher belastbaren Tatsachenbasis die behauptete „deeskalierende Wirkung“ der Bodycams gestützt wird.

Der Einsatz von Bodycams soll wie erwähnt nicht nur Bild-, sondern auch Tonaufzeichnungen umfassen. Eine Begründung, warum dies bei tätlichen Auseinandersetzungen, die eine konkrete Gefahr für die Rechtsgüter Leib und Leben darstellen, erforderlich sein soll, ist der Gesetzesbegründung nicht zu entnehmen. Inwieweit Tonaufnahmen dem Zweck des Gesetzes dienlich sein sollen, ist ebenso nicht erkennbar. Da auch eine positive Wirkung in statistischer Hinsicht

bisher unbelegt ist, bestehen Bedenken hinsichtlich der Rechtmäßigkeit des § 15c PolG NRW als Rechtgrundlage für die Anfertigung von Tonaufnahmen.

Aus Gründen der „Waffengleichheit“, wegen der Transparenz staatlichen Handelns und wegen des Gebotes des effektiven Rechtsschutzes ist zu fordern, dass auch die Betroffenen Einsicht und Zugriff auf die Aufnahmen erhalten müssen, um diese als Beweismittel nutzen zu können. Ob und wie dies in der Praxis gehandhabt werden wird, bleibt abzuwarten.

Schließlich lässt die Gesetzesbegründung Ausführungen dazu vermissen, ob auch das Verhalten der handelnden Polizeibeamtinnen und -beamten aufgenommen wird, um einen möglichst umfassenden Geschehensablauf zu dokumentieren. Es gilt zu vermeiden, dass durch eine beschränkte Bildaufzeichnung wesentliche Handlungen der Polizei gerade nicht dokumentiert werden, die das Verhalten der betroffenen Bürgerinnen und Bürger ggf. in einem anderen Licht erscheinen lassen könnten.

Die im Gesetz vorgesehene Evaluation der Auswirkungen und die Befristung der Vorschrift des § 15c PolG NRW bis zum 31. Dezember 2019 sind sinnvoll. Es bleibt jedoch die Sorge, dass Bodycams – einmal in das Gesetz aufgenommen und in der Praxis eingeführt – auch über den Stichtag der Befristung hinaus im Polizeialltag eingesetzt werden. Die Ergebnisse der Evaluation werden wir begleiten.

Unsere Stellungnahme vom 20. September 2016 (LT-Drs. 16/4201) mit der ausführlichen Kommentierung der Vorschrift sowie der einzelnen Absätze des § 15c PolG NRW ist auf www.ldi.nrw.de abrufbar.

5.2 Änderungen des Verfassungsschutzgesetzes NRW

Mit der Änderung des Verfassungsschutzgesetzes (VSG NRW) im September 2016 hat der Gesetzgeber die rechtlichen Möglichkeiten für eine Beobachtung Minderjähriger durch den Verfassungsschutz erweitert. Außerdem wurden die neu gefassten Regelungen des Bundesverfassungsschutzgesetzes über die Übermittlung von Daten zwischen Verfassungsschutz und Polizei in das Landesgesetz übernommen.

Vor dem Hintergrund des Anschlages auf einen Sikh-Tempel im April 2016 und mit der Begründung, dass die Zahl der sich radikalisierenden Jugendlichen auch vor Vollendung des 16. Lebensjahres stetig steige, hat der Gesetzgeber Regelungsbedarf gesehen.

Mit der Änderung des VSG NRW wurden die Voraussetzungen und Altersgrenzen für die Speicherung personenbezogener Daten Minderjähriger herabgesetzt. Soweit tatsächliche Anhaltspunkte für den Verdacht einer geheimdienstlichen Tätigkeit oder einer extremistischen Bestrebung bestehen, ist eine Speicherung personenbezogener Daten Minderjähriger zwischen Vollendung des 14. und des 16. Lebensjahres möglich. Die Speicherung personenbezogener Daten von Minderjährigen nach Vollendung des 16. Lebensjahres ist nunmehr, unter Wegfall der bisherigen Beschränkungen, unter den allgemeinen Voraussetzungen des § 8 Abs. 1 VSG NRW wie bei Erwachsenen möglich.

Ob diese Erweiterung der Befugnisse des Verfassungsschutzes, wie in der Gesetzesbegründung ausgeführt, erforderlich ist, kann nur unter fachlichen Aspekten bewertet werden. Jedenfalls wird durch die Neuregelung das Recht auf Datenschutz der Minderjährigen deutlich eingeschränkt, was wir bei der Anhörung zu den Gesetzentwürfen der Landesregierung und einer Fraktion im Landtag NRW kritisch angemerkt haben. Die nunmehr nach Altersgruppen differenzierten Regelungen zur Speicherdauer bzw. Löschung tragen diesem Schutzgedanken zumindest ansatzweise Rechnung.

Nach dem Ergebnis der Anhörung wurde eine Regelung zur Evaluation der geänderten Voraussetzungen zur Speicherung personenbezogener Daten Minderjähriger unter wissenschaftlicher Begleitung aufgenommen. Dies ist mit Blick auf den Schutz Minderjähriger zu begrüßen.

Grundsätzliche Bedenken haben wir im Rahmen der Anhörung auch hinsichtlich der Änderung des § 17 VSG NRW vorgetragen. Dieser erlaubt dem Verfassungsschutz nunmehr unter bestimmten Voraussetzungen (§ 17 Abs. 2 Nr. 1 bis 4 VSG NRW) die Übermittlung personenbezogener Daten etwa an Staatsanwaltschaften und Polizei. Diese Regelungen sind nicht vereinbar mit der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Trennungsprinzip zwischen Polizei und Nachrichtendiensten. Die

Aufgaben der Polizei und die des Verfassungsschutzes sind demnach von verschiedenen, voneinander organisatorisch getrennten Behörden wahrzunehmen. Damit geht einher, dass dem Verfassungsschutz die Befugnisse der Polizei nicht zustehen – und umgekehrt.

In § 17 Abs. 2 VSG NRW hat der Landesgesetzgeber die in § 19 neu gefasste Regelung des Bundesverfassungsschutzgesetzes übernommen. Deshalb haben wir auf die bereits seitens der Bundesbeauftragten für Datenschutz geäußerten Bedenken hingewiesen, die auch bezüglich der Bundesregelung den Grundsatz des informationellen Trennungsprinzips verletzt sieht.

Die Erweiterung der Befugnisse des Verfassungsschutzes und die damit verbundene Zunahme der Datenverarbeitung bewerten wir grundsätzlich kritisch. Die begrüßenswerte Evaluation unter wissenschaftlicher Begleitung wird zeigen, ob die deutliche Einschränkung der Datenschutzrechte Minderjähriger verhältnismäßig ist. Unsere Stellungnahme vom 19. August 2016 ist unter www.ldi.nrw.de abrufbar.

5.3 Videoüberwachung durch Polizei und Ordnungsbehörden

Nach den Vorkommnissen in der Silvesternacht 2015 in Köln und anderen Städten stellte die Landesregierung NRW einen „15-Punkte-Plan“ auf, mit dem sie für mehr Innere Sicherheit und bessere Integration sorgen möchte. Ein Punkt ist die Videobeobachtung von Kriminalitätsschwerpunkten. Ziel ist es, Straftäterinnen und Straftäter abzuschrecken bzw. Straftaten besser nachweisen zu können.

Nach § 15a Abs. 1 Polizeigesetz NRW (PolG NRW) kann die Polizei zur Verhütung von Straftaten einzelne öffentlich zugängliche Orte, an denen wiederholt Straftaten begangen wurden und deren Beschaffenheit die Begehung von Straftaten begünstigt, mittels Bildübertragung beobachten und die Bilder aufzeichnen. Als weitere Voraussetzung müssen Tatsachen die Annahme rechtfertigen, dass an diesem Ort weitere Straftaten begangen werden. Im Bereich mehrerer Polizeipräsidien wird in Umsetzung des 15-Punkte-Planes Videobeobachtung durchgeführt. Wir sind mit den jeweiligen Polizeibehörden im Gespräch und überprüfen sukzessive alle diese neuen polizeilichen Maßnahmen zur Videobeobachtung, wozu auch jeweils die Kontrolle der Anlagen vor Ort gehört. Zum Zeitpunkt der Berichterstellung waren die Gespräche mit den Polizeibehörden noch nicht abgeschlossen. Bei den Prüfungen richten wir unser Augenmerk vor allem darauf, dass die Beobachtung der Bürgerinnen und Bürger im Umfeld der Kameras auf das Nötigste beschränkt bleibt.

Neben der Polizei können auch die Ordnungsbehörden in NRW unter den Voraussetzungen des § 24 Nr. 6 Ordnungsbehördengesetz NRW in Verbindung mit § 15 PolG NRW Videoüberwachungsmaßnahmen durchführen. Nach diesen Vorschriften dürfen bei öffentlichen Versammlungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, personenbezogene Daten durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmenden erhoben werden, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten und Ordnungswidrigkeiten begangen werden. Ob diese Anforderungen erfüllt sind, ist im Einzelfall und unter Berücksichtigung aller konkreten Umstände zu bewerten.

Über die rechtlichen Voraussetzungen und Grenzen der Videoüberwachung durch Behörden und Polizei informieren wir in unserer Veröffentlichung „Videoüberwachung durch öffentliche Stellen des Landes Nordrhein-Westfalen – Allheilmittel oder Teufelszeug?“, abrufbar auf unserer Internetseite www.ldi.nrw.de. Die Hinweise richten sich an verantwortliche Stellen und deren behördliche Datenschutzbeauftragte ebenso wie an interessierte Bürgerinnen und Bürger.

5.4 Kontrolle der Falldatei Rauschgift

Eine nachhaltige Bekämpfung der Betäubungsmittelkriminalität bedarf einer länderübergreifenden Zusammenarbeit. Dabei sind in jedem Einzelfall die Anforderungen des Datenschutzes sowie die Grenzen der Verhältnismäßigkeit zu wahren. Bei der Kontrolle der Falldatei Rauschgift (FDR) stellten wir fest, dass die Polizei über Jahre hinweg Daten zu Rauschgiftdelikten gespeichert hat, obwohl die gesetzlichen Voraussetzungen nicht vorlagen.

Die FDR ist eine bundesweite Verbunddatei, in der die Polizeibehörden von Bund und Ländern Sicherstellungen von Betäubungsmitteln und Verstöße gegen das Betäubungsmittelgesetz speichern. Sie wird zentral beim Bundeskriminalamt (BKA) geführt. Aufgenommen werden unter anderem Angaben

- zu den Tatverdächtigen und deren Beteiligung,
- Tatörtlichkeit und -mittel sowie
- zum erlangten Gut.

Die Rechtsgrundlage für die Errichtung der Falldatei Rauschgift findet sich in §§ 8 Abs. 1, Abs. 2, 11 Abs. 2 Satz 3 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG). Voraussetzung für eine Speicherung ist eine Straftat von länderübergreifender oder erheblicher Bedeutung (§ 2 BKAG) sowie eine Negativprognose zu jedem Einzelfall (§ 8 Abs. 2 BKAG), die zu dokumentieren und einzelfallbezogen zu begründen ist.

Im Rahmen einer gemeinsamen Aktion haben die Datenschutzbeauftragten des Bundes sowie der Länder Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen die FDR parallel geprüft. Dabei sind sie sowohl der Struktur der Datei als auch den einzelnen Speicherungen nachgegangen.

In NRW haben wir eine Kontrolle beim Landeskriminalamt NRW und einem Polizeipräsidium durchgeführt. Im Rahmen der Stichprobenkontrolle wiesen verschiedene Speicherungen Inhalte auf, die nicht den gesetzlichen Anforderungen entsprachen. Beispielsweise wurden auch Angaben zu Minderjährigen unter vierzehn Jahren gespeichert. Darüber hinaus waren Personen erfasst, die zwar nur einmalig ein Rauschgiftdelikt, jedoch noch mindestens ein anderes Delikt begangen hatten, was automatisch zu einer verlängerten Speicherung führte. Es fanden sich auch Speicherungen zum Erstkonsum lediglich geringfügiger Mengen so genannter harter Drogen. Darüber hinaus waren zahlreiche Bagatellfälle ohne nähere Begründung personenbezogen gespeichert (zum Beispiel Erstkonsum von Marihuana, geringe Menge Amphetamin in einem gestohlenen Geldbeutel).

Eine Bereinigung des Datenbestandes fand generell nicht statt; sie erfolgte lediglich bei Zufallsfunden oder bei Auskunfts- und Löschungsbegehren betroffener Personen.

Aufgrund der aufgedeckten Defizite hat die Konferenz der Datenschutzbehörden des Bundes und der Länder am 9./10. November 2016 in der gemeinsamen Entschließung „Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf " Konsequenzen für die polizeiliche Datenverarbeitung gefordert (Abdruck im Anhang).

Zwischenzeitlich wurden aufgrund der Kontrollergebnisse in NRW bereits über 112.000 der insgesamt 180.000 Datensätze gelöscht. Um generell eine zeitnahe Löschung durchführen zu können, sind die Polizeibehörden allerdings auf entsprechende Mitteilungen der Staatsanwaltschaften angewiesen (vgl. § 482 Abs. 2 Strafprozessordnung).

Die zeitnahe Überprüfung und Bereinigung des Datenbestandes ist aus Gründen des Datenschutzes unbedingt erforderlich. Vor dem Hintergrund, dass für das Jahr 2017 die Ablösung der bisherigen Falldatei Rauschgift durch die neue Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV) geplant ist, gewinnt sie zusätzlich an Bedeutung: Nur Daten, die (noch) rechtmäßig gespeichert sind, dürfen in die neue Verbunddatei übernommen werden.

Nicht nur für die Falldatei Rauschgift gilt: Die Polizeibehörden haben in eigener Verantwortung sicherzustellen, dass die Einhaltung von grundlegenden datenschutzrechtlichen Standards für jedwede Speicherung in bundesweiten Verbunddateien umfassend gewährleistet ist.

5.5 Beteiligung der Polizei an Medienproduktionen

Aufgrund einer Presseanfrage zur Mitwirkung der Polizei an einer Medienproduktion haben wir uns erneut mit der Problematik „Reality-TV“ unter Beteiligung der Polizei beschäftigt.

Eine Fahrradstaffel der Polizei nahm an Dreharbeiten einer Medienproduktion teil, wobei die Beamtinnen und Beamten auf ihren Helmen Kameras trugen und ihre realen Einsätze filmten.

Diese Medienbeteiligung war unzulässig. Im Ergebnis wird diese Rechtsauffassung vom Innenministerium NRW geteilt. Die ohne die erforderliche Genehmigung des Innenministeriums NRW begonnenen Arbeiten an der Sendung wurden abgebrochen, die bereits aufgenommenen Daten gelöscht, eine Ausstrahlung erfolgte nicht.

Medienproduktionen über reale Einsätze der Polizei stellen eine Datenübermittlung von der Polizei an private Dritte dar. Nach § 4 Abs. 1 Datenschutzgesetz NRW (DSG NRW) ist diese Datenverarbeitung nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder die betroffene Person eingewilligt hat. Eine entsprechende Rechtsgrundlage enthalten weder das Polizeigesetz NRW (PolG NRW) noch das DSG NRW. Auch die Einholung einer schriftlichen Einwilligungserklärung kommt regelmäßig nicht in Betracht, insbesondere bei unvorhergesehenen Einsätzen, die spontanes und schnelles Handeln erfordern. Voraussetzung einer wirksamen Einwilligung ist nämlich, dass die betroffene Person in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären ist. Über die Freiwilligkeit, den Verwendungszweck der Daten und – bei einer beabsichtigten Übermittlung – über die Empfänger der Daten dürfen keine Zweifel bestehen. Darüber hinaus bedarf es eines Hinweises, dass die Einwilligung verweigert und eine bereits erteilte Einwilligung mit Wirkung für die Zukunft widerrufen werden kann. Besonders problematisch sind solche Aufnahmen, wenn die Betroffenen in ihren „eigenen vier Wänden“ von der Polizei aufgesucht werden, da dann in ihre Privatsphäre und dadurch besonders intensiv in ihre Persönlichkeitsrechte eingegriffen wird.

Ungeachtet dessen wurden in der Vergangenheit „Reality-TV-Formate“ produziert und ausgestrahlt. Auf diese Problematik wurde bereits im Bericht 2005 unter 8.5 „Zweifelhafter Fernsehruhm“ hingewiesen. Gegen diese Art des Voyeurismus richtete sich auch die Entschließung der Datenschutzkonferenz „‚Reality-TV‘ – Keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen“ vom 8./9. Oktober 2009. Die Entschließung ist auf unserer Internetseite www.ldi.nrw.de abrufbar.

Die datenschutzrechtlichen Fragen im Zusammenhang mit dem Genehmigungsverfahren wurden einvernehmlich mit dem Innenministerium NRW geklärt:

Grundlage für die Presse- und Öffentlichkeitsarbeit der Polizei in NRW ist ein Runderlass des Innenministeriums NRW aus dem Jahr 2011, der auch die Mitwirkung an Medienproduktionen regelt.

Für die Beteiligung der Polizei an Medienproduktionen ist inzwischen ein mehrstufiges Genehmigungsverfahren vorgesehen, an dessen Ende eine Entscheidung des Innenministeriums NRW steht.

Unterstützt werden in Zukunft ausschließlich Sendeformate, die Dokumentations- oder Reportagecharakter haben und thematisch im Interesse der Polizei liegen. So müssen etwa die Informationen über die Polizeiarbeit im Vordergrund stehen, das Interesse für den Polizeiberuf geweckt oder polizeiliche Botschaften platziert werden. Keine Genehmigung erhalten Sendeformate wie die typischen „Reality-TV"-Produktionen, bei denen voyeuristische Motive eine Rolle spielen, die die Sensationslust der Zuschauerinnen und Zuschauer ansprechen sollen oder überzogene Gewaltdarstellungen zeigen.

Bei der Entscheidung über eine Genehmigung ist der Datenschutz ein wichtiger Aspekt. Eine Begleitung durch ein Kamerateam ist nur in den Fällen zulässig, in denen problemlos eine wirksame Einwilligung der betroffenen Person eingeholt werden kann.

Dies ist nach Mitteilung des Innenministeriums NRW beispielsweise der Fall, wenn die Polizei eine Reportage über die Gefahren von Geschwindigkeitsüberschreitungen unterstützen möchte. Sollen dabei allgemeine Verkehrskontrollen gefilmt werden, informiert die Polizeibeamtin bzw. der Polizeibeamte die zu kontrollierende Person zunächst in einem Vier-Augen-Gespräch über die Situation, die beabsichtigte Filmaufnahme, die Freiwilligkeit sowie die weiteren Einwilligungsvoraussetzungen. Anschließend holt sie ihre Einwilligung ein. Erst danach ist eine Filmaufnahme zulässig. Zudem muss es Betroffenen möglich sein, sich im Nachhinein doch noch anders zu entscheiden. Filmaufnahmen sind dann zu löschen oder technisch derart zu bearbeiten, dass keinerlei personenbeziehbare Rückschlüsse möglich sind. Dieses Vorgehen trägt damit den Datenschutzbelangen der von der Verkehrskontrolle betroffenen Personen Rechnung.

Bei der Überarbeitung des Runderlasses zur Presse- und Öffentlichkeitsarbeit hat das Innenministerium NRW zugesagt, uns zu beteiligen.

Bei der Beteiligung der Polizei an Medienproduktionen ist im Rahmen von „Echteinsätzen" sorgfältig darauf zu achten, dass die Datenschutzbelange der durch die Filmaufnahmen betroffenen Personen umfassend gewahrt bleiben. Unbedenklich sind die so genannten „Scripted-Reality-Formate", in denen echte oder unechte Polizistinnen und Polizisten vermeintliche Einsätze nachspielen: Datenschutzbelange werden hierbei nicht berührt.

6. Kommunales

6.1 Änderungen im Bereich der Meldegesetzgebung

Mit Inkrafttreten des Bundesmeldegesetzes (BMG) zum 1. November 2015 wurde das Melderecht in Deutschland erstmals bundesweit vereinheitlicht. Damit einhergehend war es erforderlich, die landesrechtlichen Regelungen entsprechend anzupassen.

Das Meldewesen war bislang im Melderechtsrahmengesetz (MRRG) geregelt. Zur Umsetzung der rahmenrechtlichen Vorgaben des Bundes erließen die Länder – so auch NRW – eigene melderechtliche Vorschriften. Nach Inkrafttreten des BMG können landesrechtliche Regelungen nunmehr nur noch in dem dort zugelassenen, wesentlich geringeren Umfang getroffen werden. Der Gesetzgeber des Landes NRW hat die landesrechtlichen Normen dementsprechend novelliert. Hervorzuheben ist: Sowohl durch das BMG als auch durch das Meldegesetz Nordrhein-Westfalen (MG NRW) wurde nach wie vor kein zentrales Bundes- bzw. Landeszentralregister geschaffen. Dies ist aus Sicht des Datenschutzes zu begrüßen. Personenbezogene Daten werden bundes- und landesweit weder in ein zentrales Register eingegeben noch können sie aus einem bundes- oder landesweiten Zentralregister abgerufen werden. Vielmehr bleibt es bei den bisherigen dezentralen Melderegistern auf Ortsebene.

Weitergehende Informationen zu den wesentlichen datenschutzrechtlichen Änderungen im Bereich des Meldewesens und Antworten auf häufig gestellte Fragen haben wir auf unserer Homepage www.ldi.nrw.de eingestellt.

6.2 Livestream von Ratssitzungen

Die Möglichkeit der Liveübertragung von Rats- und Ausschusssitzungen via Internet erweitert den Kreis der Öffentlichkeit und kann die Transparenz von Entscheidungsprozessen im kommunalen Bereich fördern. Allerdings muss das Recht auf informationelle Selbstbestimmung betroffener Personen dabei gewahrt bleiben.

Aufgrund des steigenden Interesses, die Teilhabe an Beschlussfassungen orts- und zeitunabhängig zu gestalten, stellen mittlerweile verschiedene Kommunen in NRW auf ihren Homepages Livestreams zur Verfügung. Zum Teil sind Aufzeichnungen von Sitzungen sogar noch über deren Ende hinaus abrufbar.

Das Kommunalverfassungsrecht normiert das Prinzip der Öffentlichkeit von Sitzungen der Stadt- und Gemeinderäte sowie Kreistage als Ausgestaltung des Demokratieprinzips. Dieses ist jedoch im Sinne einer Saalöffentlichkeit zu verstehen. Das Streamen von Sitzungen via Internet geht darüber hinaus.

Kraft seiner Geschäftsordnungsautonomie obliegt es prinzipiell dem Rat, im Rahmen der Gesetze über eine Erweiterung auf die so genannte Medienöffentlichkeit zu entscheiden. Beim Streamen und Aufzeichnen von Ratssitzungen in Bild und Ton werden allerdings auch personenbezogene Daten verarbeitet, und zwar in Form der weltweiten Übermittlung an einen unbestimmten Personenkreis. Betroffen sind in erster Linie Mandatsträgerinnen und -träger, aber ggf. auch Beschäftigte der Kommunen, sachkundige Bürgerinnen und Bürger sowie Zuschauerinnen und Zuschauer.

Die Verarbeitung dieser personenbezogenen Daten ist nach § 4 Abs. 1 Datenschutzgesetz NRW (DSG NRW) nur zulässig, sofern eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat. An einer speziellen Rechtsgrundlage zur Übertragung von Sitzungen via Internet fehlt es im nordrhein-westfälischen Landesrecht. Eine solche Rechtsgrundlage kann auch nicht in der Geschäftsordnung des Rates geschaffen werden, da es sich schon mangels Außenwirkung nicht um eine Rechtsvorschrift im Sinne des DSG NRW handelt. Die Schaffung einer Rechtsgrundlage in der Hauptsatzung scheitert daran, dass der Gesetzgeber alle wesentlichen, das heißt insbesondere alle grundrechtseinschränkenden Entscheidungen, selbst treffen muss.

Demnach kann die Übertragung von Sitzungen nur zulässig sein, wenn die betroffenen Personen eingewilligt haben. Die Einwilligung muss auf der Grundlage einer umfassenden vorherigen Information freiwillig und schriftlich erfolgen; außerdem muss sie jederzeit widerrufbar sein.

Der Rat seinerseits sollte Regelungen zum Verfahren der Einholung von Einwilligun-

gen und den Rahmenbedingungen der Übertragung treffen. Dabei sind insbesondere die Interessen der unterschiedlichen Personengruppen am Schutz ihrer personenbezogenen Daten, an Teilhabe und Demokratiekontrolle, an ungestörter Mandatsausübung sowie die Funktionsfähigkeit des Rates zu berücksichtigen und in ein angemessenes Verhältnis zu setzen. Im Allgemeinen gebietet es der Grundsatz der Verhältnismäßigkeit, dass das Streamen einer Sitzung nur so weit gehen darf, wie es zur Informationsübermittlung erforderlich ist. So kann etwa im Einzelfall die Übertragung auf die Aufnahmen des Rednerpults beschränkt werden. Außerdem ist dafür Sorge zu tragen, dass die Kamera für den nicht-öffentlichen Teil der Sitzung oder beim Fehlen der entsprechenden Einwilligungserklärung einer betroffenen Person ausgeschaltet wird. Auch ist ein Archivierungskonzept zu erstellen, in dem etwa Löschungsfristen und Zugriffsrechte festgelegt werden.

Das Streaming von Rats- und Ausschusssitzungen über das Internet ist grundsätzlich zulässig, soweit schriftliche Einwilligungen der betroffenen Personen vorliegen und der Rat angemessene Rahmenbedingungen festgelegt hat.

6.3 IT-Sicherheit bei den Kommunen

Die Querschnittserhebung zur Datensicherheit bei den Kommunen hatte im vorherigen Berichtszeitraum gezeigt, dass die IT-Sicherheit bei den Kommunen verbesserungsfähig ist (siehe Bericht 2015 unter 11). Vieles wurde inzwischen in Angriff genommen, aber es verbleibt noch Handlungsbedarf.

Neuartige Angriffe auf IT-Systeme beispielsweise mittels der so genannten Ransomware (Einzelheiten dazu unter 13.4), die große Schäden anrichten können, haben in der jüngeren Vergangenheit verdeutlicht, wie wichtig Maßnahmen zur IT-Sicherheit sind. Auch die Kommunen haben dieses Gefahrenpotential erkannt und sind aufgerufen, entsprechende Gegenmaßnahmen zu ergreifen. Im Anschluss an die seinerzeitige Querschnittserhebung haben die Kommunen wichtige Schritte zur Behebung der aufgezeigten Mängel unternommen.

Von besonderer Bedeutung ist dabei die lückenlose Erstellung von Sicherheitskonzepten. Einige der Kommunen, die nach eigenen Angaben über kein Sicherheitskonzept verfügten, haben dies nachgeholt. Etliche arbeiten noch an der Umsetzung.

Zur weiteren Unterstützung und Beratung der Kommunen führten wir mit den Kommunalen Spitzenverbänden NRW eine gemeinsame Aktion zur Sensibilisierung für das Thema IT-Sicherheit durch:
Ab Frühjahr des Jahres 2016 fand unter unserer Beteiligung eine gemeinsame Veranstaltungsreihe der Kommunalen Spitzenverbände NRW und dem Dachverband kommunaler IT-Dienstleister (KDN) statt. Die einzelnen Veranstaltungen wurden in Aachen, Ibbenbüren, Hemer, Köln und Lemgo durchgeführt und fanden ein positives Echo. Die gute Organisation durch den KDN, für die wir uns gerne an dieser Stelle noch einmal bedanken, hat dazu sicher beigetragen.

Unter Beteiligung unseres Referats für Technik wurde das Thema IT-Sicherheit aus verschiedenen Blickwinkeln beleuchtet. Vertreterinnen und Vertreter des Cybercrime-Kompetenzzentrums des Landeskriminalamtes NRW berichteten eindrucksvoll aus ihrer Praxis. Dabei wurde deutlich, dass sich die Cyber-Kriminellen verstärkt professionalisieren und mittlerweile dem Bereich der organisierten Kriminalität zuzuordnen sind. Im so genannten Darknet gibt es bereits „Dienstleister“, die Cybercrime-Werkzeuge für kriminelle Aktivitäten vermieten. Die Vertreterinnen und Vertreter der Spionageabwehr des Verfassungsschutzes NRW wiesen darauf hin, dass auch die Daten der Kommunen für ausländische Geheimdienste von Interesse sind.

Aus Sicht des Datenschutzes haben wir verschiedene Bedrohungsszenarien dargestellt: Cyberwar, Cybercrime, Hacking, Spionage, bis hin zum konventionellen Einbruch, Social Engineering und Angriffe

durch eigene Beschäftigte („Innentäter“). Die Bedrohungslage ist komplex und die Veranstaltungen machten die Notwendigkeit von Sicherheitskonzepten deutlich. Nur ein strukturiertes und methodisches Vorgehen in Form eines IT-Sicherheitskonzepts bietet die Chance, die richtigen IT-Abwehrmaßnahmen zu treffen. Im Rahmen der Veranstaltungen haben wir daher die Vorgehensweise zur Erstellung von Sicherheitskonzepten nach der IT-Grundschutz Methode des Bundesamtes für Sicherheit in der Informationstechnik erläutert.

Im Ergebnis wurde erneut deutlich, wie wichtig und unabdingbar IT-Sicherheitskonzepte gerade vor dem Hintergrund der immer komplexeren Angriffe sind.

Als Erkenntnis bleibt festzuhalten: Die IT-Systeme der Kommunen sind bedroht. Sie sollten daher ihren Nachholbedarf erkennen und entsprechende Schritte unternehmen.

Einige Kommunen haben sich zur Bewältigung dieser Aufgaben zu Arbeitsgruppen zusammengeschlossen. Andere lassen sich von ihren kommunalen IT-Dienstleistern beraten und unterstützen. Teilweise wurden auch externe Fachfirmen mit der Sicherheitskonzeptionierung beauftragt.

Das Thema IT-Sicherheit bleibt weiterhin ein Schwerpunkt. Wir werden die Kommunen dazu anhalten, alles Erforderliche zu veranlassen und sie dabei beraten. Soweit erforderlich werden wir weitere Kontrollen durchführen.

7. Elektronische, digitale, internetbasierte Datenverarbeitung im Schulbereich

Dürfen Lehrkräfte ihre privaten Endgeräte, wie Computer, Notebooks und Tablets zur Erfüllung dienstlicher Aufgaben einsetzen? Ist es ihnen erlaubt, über ihre privaten E-Mail-Adressen dienstlich zu kommunizieren? Unter welchen Voraussetzungen lässt sich E-Learning an Schulen datenschutzkonform umsetzen? Kann das Klassenbuch durch ein elektronisches Klassenbuch ersetzt werden?

Die Bedeutung der elektronischen, digitalen, internetbasierten Datenverarbeitung nimmt im Schulbereich stetig zu. Damit sind viele Chancen, aber auch datenschutzrechtliche Risiken und Probleme verbunden. Zu vier Themen haben uns besonders viele Anfragen erreicht:

Dienstliche Verarbeitung personenbezogener Daten auf privaten Geräten

Die Datenverarbeitung der personenbezogenen Daten der Schülerinnen und Schüler erfolgt zu einem großen Teil elektronisch. Die Lehrkräfte nutzen hierzu mangels eigener Arbeitsplätze in den Schulen und mangels dienstlich zur Verfügung gestellter Geräte ihre eigenen privaten Geräte, wie Computer, Notebooks und Tablets. Hieraus ergeben sich erhebliche Probleme für den Schutz der Daten der Schülerinnen und Schüler.

Die Zulässigkeit der Verarbeitung von personenbezogenen Daten von Schülerinnen und Schülern auf privaten Geräten richtet sich nach § 2 Abs. 2 der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I). Grundsätzlich soll jegliche Datenverarbeitung innerhalb der Schule stattfinden. Die Schulleitung hat so jederzeit die Möglichkeit, die Ordnungsgemäßheit der Datenverarbeitung zu kontrollieren und auf die Datensicherheit Einfluss zu nehmen. Bei der Nutzung von privaten Geräten ist diese Kontrollmöglichkeit nur sehr eingeschränkt gegeben. Deswegen muss die Schulleitung, die weiterhin die Verantwortung trägt, jeden Einsatz eines privaten Gerätes vorab schriftlich genehmigen. Voraussetzung hierfür ist, dass die Datenverarbeitung auf privaten Geräten für die Erfüllung der schulischen Aufgaben erforderlich ist und ein hinreichender technischer Zugriffsschutz auf die gespeicherten Daten besteht (vgl. § 2 Abs. 2 Satz 2 VO-DV I). Die Schulleitung hat als verantwortliche Stelle ferner sicherzustellen, dass bei der Verarbeitung die Anforderungen des § 10 Datenschutzgesetz NRW (DSG NRW) – technische und organisatorische Maßnahmen – eingehalten werden.

Der Regelungskomplex in der VO-DV I stammt aus einer Zeit, in der es erst wenige Computer und vor allem keine modernen Geräte, wie Smartphones oder Tablets gab und überdies auch keine weltweite Vernetzung via Internet bestand. Die durch die Schulleitung vorzunehmen-

de Prüfung war zwar auch schon damals technisch anspruchsvoll; sie musste jedoch die Gefahren, die sich heutzutage aus der weltweiten Vernetzung und aus der Vielzahl technischer Geräte ergeben, nicht mit einbeziehen.

Die Schulleitung ist aufgrund der Vielfältigkeit der Risiken bei der Datenverarbeitung auf privaten Geräten nicht mehr in der Lage, alle technisch relevanten Sicherheitsaspekte zu überschauen.

Sie müsste unter anderem

- in eigener Verantwortung die Sicherheit jedes einzelnen privaten Geräts, sei es Notebook, Tablet oder Smartphone, umfassend prüfen und hierzu die technischen Aspekte jedes einzelnen Modells jedes Herstellers kennen,
- zudem die (Betriebs-)Software jedes Geräts von Apples iOS bis zu Googles Android kennen, um die Risiken einschätzen zu können,
- sich mit jeder installierten Software auseinandersetzen, sei es Notenverwaltungssoftware oder Stundenplan- und Vertretungssoftware,
- insbesondere auch die Wechselwirkung der verschiedenen Softwareanwendungen untereinander berücksichtigen und
- alle weiteren Aspekte, wie die Einsatzumgebung (Router, Firewall, Nutzung durch andere Familienmitglieder) in die Prüfung einbeziehen.

Erschwerend kommt hinzu, dass bislang keine fundierte technische Risikoanalyse für Smartphones und Tablets existiert. Dies macht es nahezu unmöglich, angemessene Empfehlungen zur Herstellung der erforderlichen Datensicherheit solcher Geräte auszusprechen. Mangels Prüfgrundlage dürfte daher derzeit die Nutzung solcher Geräte von der Schulleitung nicht genehmigt werden.
Die Lösung der beschriebenen Probleme dürfte nach unserem gegenwärtigen Erkenntnisstand darin bestehen, sämtlichen Lehrkräften – wie bei Telearbeitsplätzen in der öffentlichen Verwaltung – dienstliche Geräte zur ausschließlich dienstlichen Nutzung bereitzustellen. Diese wären durch die schulische IT vorab auszuwählen, zu prüfen und datenschutzgerecht einzurichten. Hierauf haben wir das Schulministerium NRW aufmerksam gemacht und sehen dies als Auftakt zu weiteren Gesprächen zu diesem Thema an.

Dienstliche Kommunikation via E-Mail

Wie die Eingaben der letzten Jahre gezeigt haben, kommunizieren Lehrkräfte oftmals dienstlich über private E-Mail-Konten. Sie benutzen dabei entweder ihre gemischt genutzten privaten E-Mail-Konten oder private E-Mail-Konten, welche sie in eigener Verantwortung für die dienstliche Kommunikation angelegt haben. Aus datenschutzrechtlicher Sicht ist die Verwendung solcher privaten E-Mail-Konten jedoch problematisch.
Für die Bewertung der Zulässigkeit der Datenübermittlung via E-Mail ist entscheidend, an welchem Standort bzw. in welchem Land die E-Mails verarbeitet werden, sprich wo die E-Mail-Server stehen. Die Diensteanbieter geben jedoch in den

meisten Fällen gerade diese Informationen nicht preis. Es bleibt vielfach offen, ob die Daten in Deutschland, dem EU-Ausland oder in Nicht-EU-Ländern verarbeitet werden. Daraus folgt zugleich, dass weder die Lehrkräfte noch die Schulleitung Kenntnis darüber und Einfluss darauf haben bzw. nehmen können, wo die personenbezogene dienstliche E-Mail-Kommunikation verarbeitet wird. § 17 DSG NRW enthält zur Übermittlung an ausländische Stellen detaillierte Regelungen.

Da oftmals nicht nachvollzogen werden kann, an welchem Standort die personenbezogenen Daten verarbeitet werden und wie der konkrete Datenfluss verläuft, kann die Schulleitung nicht immer prüfen, ob in dem Zielland ein angemessenes Datenschutzniveau besteht. Unabhängig hiervon ist die Möglichkeit einer Kontrolle durch die Schulleitung nur eingeschränkt bis gar nicht möglich, da keine Zugriffsmöglichkeit auf die privaten Konten besteht und eine solche auch nicht bestehen dürfte.

Zusammenfassend ist daher festzustellen, dass zur dienstlichen Kommunikation via E-Mail ausschließlich dienstliche E-Mail-Adressen in Betracht kommen, welche die Schulleitung den Lehrkräften bereitstellt.

E-Learning

Immer mehr Schulen setzen auf die webgestützte Wissensvermittlung via Online-Lernplattformen. Solche E-Learning-Produkte werden von Schulbuchverlagen, Computer- und Softwareherstellern und sonstigen Anbietern bereitgestellt. Neben den Vorteilen einer orts- und zeitunabhängigen Nutzung ist jedoch zu beachten, dass dabei eine Vielzahl von personenbezogenen Schüler- und Lehrerdaten nunmehr elektronisch verarbeitet werden. Es findet eine Weitergabe dieser personenbezogenen Daten an eine außerschulische, oftmals private Stelle statt. Hierdurch entstehen Risiken für die informationelle Selbstbestimmung, denn im Gegensatz zum klassischen Unterricht in der Schule hinterlassen die Schülerinnen und Schüler bei jedem Lernschritt Datenspuren, die hinsichtlich Inhalt, Ort, Zeit und Person zusammengeführt und zur Profilbildung genutzt werden können.

Um in der Schule E-Learning als verpflichtenden Bestandteil des Unterrichts einsetzen zu können, bedarf es einer gesetzlichen Grundlage. Da es eine solche in NRW gegenwärtig nicht gibt, ist E-Learning allein auf Grundlage informierter Einwilligungen (vgl. § 4 Abs. 1 Buchstabe b DSG NRW) datenschutzrechtlich zu rechtfertigen. Da eine Einwilligungserklärung jederzeit widerrufen werden kann, kann dies erheblichen Einfluss auf den Schulunterricht haben.

Weitere Informationen, insbesondere zu Fragen der Auftragsdatenverarbeitung und technisch-organisatorischen Maßnahmen können der von der Datenschutzkonferenz des Bundes und der Länder am 6./7. April 2016 verabschiedeten Orientierungshilfe für Online-Lernplattformen im

Schulunterricht entnommen werden, die über unsere Homepage www.ldi.nrw.de abrufbar ist.

Elektronisches Klassenbuch

Das Klassenbuch 2.0 ist die elektronische Variante des schulischen Papierdokuments, in dem für jede Stunde der behandelte Unterrichtsstoff, die Fehlzeiten, Hausaufgaben, Verhalten von Schülerinnen und Schülern und andere wichtige Informationen eingetragen werden können. Die vielfältig verfügbaren Applikationen (Apps) für Smartphones und Tablets haben den Wunsch der Lehrkräfte zur Nutzung der elektronischen Variante verstärkt. Bei der Auswahl der Software gilt es jedoch insbesondere auf den Datenschutz zu achten.

Schulen dürfen gemäß § 120 Abs. 1 Satz 1 Schulgesetz NRW personenbezogene Daten der Schülerinnen und Schüler sowie der Eltern verarbeiten, soweit dies zur Erfüllung der ihnen durch Rechtsvorschrift übertragenen Aufgaben erforderlich ist. Grundsätzlich dürfen sich daher Schulen elektronischer Klassenbücher zur Erfüllung ihrer Aufgaben bedienen. Bei der Nutzung ist besonderes Augenmerk auf die erteilten Zugriffsrechte zu legen. Die personenbezogenen Daten der Schülerinnen und Schüler, Eltern und Lehrkräfte dürfen in der Schule nur den Personen zugänglich gemacht werden, die sie für die Erfüllung ihrer Aufgaben benötigen. Orientierung zum Zugriff von Lehrkräften auf die Daten der Schülerinnen und Schüler bietet zum Beispiel die Regelung in § 4 Abs. 3, 4 und 6 VO-DV I. Die eingetragenen Daten der Schülerinnen und Schülern sowie der Eltern dürfen darüber hinaus in aller Regel auch nicht von der Schule an Personen oder Stellen außerhalb der Schule (beispielsweise die Eltern anderer Schülerinnen und Schüler) übermittelt werden.

Weil die personenbezogenen Daten beim Einsatz elektronischer Klassenbücher auch durch externe Dritte verarbeitet werden, muss die Schulleitung streng darauf achten, eine die Datensicherheit gewährleistende und zuverlässige Institution mit der Aufgabe der Verarbeitung der Daten im Auftrag gemäß § 2 Abs. 3 VO-DV I, § 3 Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer (VO-DV II) in Verbindung mit § 11 DSG NRW zu betrauen. Für diese Datenverarbeitung im Auftrag trägt die Schulleitung die datenschutzrechtliche Verantwortung. Vor der Beauftragung und sodann regelmäßig muss die Schulleitung prüfen und sicherstellen, dass die Anbieterin oder der Anbieter die in § 10 DSG NRW aufgeführten technischen und organisatorischen Maßnahmen einhält.

Die Schulleitung muss auch wissen, ob personenbezogene Daten über die Landesgrenzen hinaus übermittelt werden, um ggf. die Vorgaben des § 17 DSG NRW prüfen zu können. Insbesondere wenn die Anbieterin oder der Anbieter keinen Sitz in Deutschland hat, ist die Schulleitung als Auftraggeber gemäß § 11 Abs. 3 DSG NRW verpflichtet, „sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich, sofern

die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für Datenschutz und Informationsfreiheit unterwirft.“ Die Verantwortung für den Datenschutz und die Datensicherheit trägt gleichwohl weiterhin die Schulleitung. Auf der Basis der eingeholten Informationen muss die Schulleitung dann ein Verfahrensverzeichnis gemäß § 8 DSG NRW erstellen.

Um die Schulleitungen bei der Prüfung zu unterstützen und auch verfahrensrechtlich abzusichern, wäre es aus datenschutzrechtlicher Sicht wünschens- und empfehlenswert, wenn das Schulministerium NRW eine Vorabauswahl an elektronischen Klassenbüchern im Sinne einer so genannten „whitelist“ treffen würde.

Zu den aufgeführten Teilaspekten der elektronischen Datenverarbeitung in Schulen haben wir Gespräche mit dem Schulministerium NRW aufgenommen. Für die Zukunft wird es wichtig sein, dass das Ministerium aus seiner Verantwortung nach § 7 DSG NRW heraus die Schulen in angemessener Form begleitet und dass – soweit erforderlich – die bestehenden gesetzlichen Regelungen an die digitalen Herausforderungen angepasst werden.

8. E-Government-Gesetz NRW

Am 16. Juli 2016 ist das Gesetz zur Förderung der elektronischen Verwaltung in NRW (E-Government-Gesetz NRW – EGovG NRW) in Kraft getreten. Damit sind auf Landesebene die rechtlichen Voraussetzungen für die Erleichterung der elektronischen Kommunikation zwischen der öffentlichen Verwaltung und den Bürgerinnen und Bürgern geschaffen worden. Zudem regelt das Gesetz die elektronische und medienbruchfreie Durchführung von Arbeitsprozessen innerhalb der Landesverwaltung.

Auf Bundesebene ist ein entsprechendes Gesetz bereits im Jahr 2013 mit dem Ziel in Kraft getreten, durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung zu erleichtern. Das Gesetz soll über die föderalen Ebenen hinweg Wirkung entfalten und Bund, Ländern und Kommunen ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten. Für die Bereiche, in denen Landesrecht ausgeführt wird, fehlte bislang eine landesgesetzliche Regelung.

Das EGovG NRW schließt diese Lücke. Wir wurden sowohl zum Referentenentwurf, als auch im parlamentarischen Gesetzgebungsverfahren angehört. Unsere datenschutzrechtlichen Hinweise hat der Gesetzgeber im Ergebnis übernommen. Wichtig ist uns insbesondere, dass die Verarbeitung von Identitätsdaten der Bürgerinnen und Bürger nur zulässig ist, wenn sie ihre Einwilligung für die jeweilige E-Government-Anwendung erteilt haben. Durch diese Regelung behalten die Nutzerinnen und Nutzer die Hoheit über ihre personenbezogenen Daten und können selbst frei darüber entscheiden, ob die konkrete Datenverarbeitung ihrem Willen entspricht.

Wir werden die weiteren Entwicklungen im Bereich der elektronischen Kommunikation mit und innerhalb der öffentlichen Verwaltung aufmerksam verfolgen.

9. Beschäftigtendatenschutz

9.1 Öffentlicher Bereich

9.1.1 Problematische Verarbeitung von Beschäftigtendaten im Verfahren EPOS.NRW

Mehrere Anfragen und Eingaben von Personalvertretungen machten deutlich, dass bei der Einführung des landeseinheitlichen Haushaltsmittelbewirtschaftungsverfahrens EPOS.NRW datenschutzrechtlicher Nachbesserungsbedarf bestand.

Die Landesregierung stellt das öffentliche Haushalts- und Rechnungswesen um: Das kamerale Rechnungswesen soll durch eine doppelte Buchführung mit Kosten- und Leistungsrechnung (Integrierte Verbundrechnung – IVR) und die Einführung einer neuen Software für das Rechnungs- und Kassenwesen ersetzt werden. Zur Umsetzung dieser Ziele hat die Landesregierung das IT-gestützte Programm EPOS.NRW (Einführung von Produkthaushalten zur Outputorientierten Steuerung – Neues Rechnungs Wesen) ins Leben gerufen.
Bestandteil des Programms sind auch so genannte Geschäftspartnerdatenbanken. Diese sollen unter anderem Doppelerfassungen von Daten ersparen, aber auch Aufrechnungslagen erkennen, falls Personen vom Land sowohl Geld bekommen als auch Forderungen gegenüber dem Land haben. Personalvertretungen machten darauf aufmerksam, dass die Geschäftspartnerdatenbank neben sonstigen Personen auch Beschäftigte mit ihren Personalien und Kontoverbindungen erfasst. Kritisiert wurde, in jeder Landesbehörde seien mehreren Personen Zugriffsberechtigungen auf die genannten Daten eingeräumt. Daher könne ein unüberschaubarer Personenkreis Kenntnis von den Daten erhalten. Besonders kritisch sei die Speicherung der Privatadressen der Beschäftigten in dieser Datenbank. Dies könne etwa in den Bereichen Strafverfolgung oder Justizvollzug zu einem Sicherheitsrisiko für die Beschäftigten führen.

Die Bedenken waren begründet. Eine Verarbeitung von Beschäftigtendaten der beteiligten öffentlichen Stellen bei zahlungsrelevanten Geschäftsprozessen ist unzulässig, soweit Daten der Betroffenen zur Erkennung von Aufrechnungslagen verwendet werden sollen. Denkbar ist etwa der Fall, in dem eine Gehaltsforderung aus dem Dienstverhältnis mit einer Forderung des Landes außerhalb dieses Rechtsverhältnisses (zum Beispiel Gebühr für eine Erlaubnis) gegenübersteht. Für eine solche Datennutzung besteht keine Rechtsgrundlage. Das Finanzministerium ist dem gefolgt und hat mitgeteilt, auf solche Aufrechnungen künftig zu verzichten.

Erörterungsbedürftig waren auch die Aufgaben der in diesem Projekt mitwirkenden

behördlichen Datenschutzbeauftragten. Nach unseren Hinweisen wurde in dem Datenschutzkonzept klargestellt, dass für die Datenverarbeitung nicht behördliche Datenschutzbeauftragte verantwortlich sind. Die Verantwortung trägt vielmehr die Daten verarbeitende Stelle.

Hinsichtlich der nicht eingegrenzten Abfragemöglichkeiten hat das Finanzministerium umfangreiche technische Anpassungen und spezielle Berechtigungsprüfungen vorgenommen sowie besondere Analysen hinsichtlich möglicher kritischer Transaktionen angekündigt. Daneben werden bezogen auf Stamm- und Bewegungsdaten umfangreiche Protokollierungen von Systemzugriffen etabliert. Mit diesen Maßnahmen kann künftig sichergestellt werden, dass nur noch die für die jeweilige Aufgabe zuständigen Personen die entsprechenden Daten in der Geschäftspartnerdatenbank einsehen können.

Zu begrüßen ist zudem, dass die Beschäftigten selbst entscheiden können, ob ihre dienstliche oder private Anschrift in dem Verfahren EPOS.NRW gespeichert wird.

Auf die Umsetzung dieser Maßnahmen sollte bei der weiteren Einführung von EPOS.NRW besonders geachtet werden.

9.1.2 Bewerbervorauswahl durch Videopräsentation

Eine Kommune beabsichtigt den dauerhaften Einsatz einer Software, die es ermöglicht, zur Vorauswahl automatisiert videogestützte Interviews mit Bewerberinnen und Bewerbern zu führen.

Bei diesem Verfahren erfolgt das Videointerview mit automatisiert eingeblendeten Fragen ohne die Beteiligung einer weiteren Person. Die Bewerberinnen und Bewerber kommunizieren vor ihrem PC ausschließlich mit dem Computerprogramm. Die nach einer Vorbereitungszeit gegebenen Antworten werden in Ton und Bild aufgezeichnet, wobei die Bewerberinnen und Bewerber ihre jeweiligen Antworten weder unterbrechen noch wiederholen können.

Das neue Verfahren soll obligatorisch neben die bewährten Personalauswahlinstrumente treten, etwa Auswertung der Bewerbungsunterlagen, kognitive Leistungstests, persönliches Auswahlgespräch. Die Notwendigkeit der vorab aufgezeichneten Interviews begründet die Kommune damit, dass die hohe Bewerberzahl und die für die Auswahl verfügbare Zeit es nicht zuließen, alle nach schriftlicher Bewerbung und Eignungstest grundsätzlich geeigneten Bewerberinnen und Bewerber auch zu einem persönlichen Gespräch einzuladen. Mit dem Einsatz der Interview-Software könnten sich die mit der Personalauswahl betrauten Personen („Evaluatoren“) bereits frühzeitig und mit frei zu planendem zeitlichen Aufwand ein persönliches Bild von den Betroffenen machen. Auf diese Weise könne die Anzahl der zu einem Auswahlgespräch einzuladenden Personen auf ein zu bewältigendes Maß begrenzt werden.

Das geschilderte Verfahren ist datenschutzrechtlich unzulässig. Eine videogestützte Erhebung und Verwendung von Bewerberdaten durch die Kommune ist weder von der Regelung des § 29b Datenschutzgesetz NRW (DSG NRW) erfasst noch sind die Voraussetzungen des § 29 Abs. 1 DSG NRW erfüllt. Eine Erhebung und weitere Verarbeitung der Daten von Bewerberinnen und Bewerbern durch derartige Videointerviews wäre nach § 29 Abs. 1 DSG NRW nur zulässig, wenn dies zur Eingehung eines Dienst- oder Arbeitsverhältnisses erforderlich ist. Das Erforderlichkeitsprinzip zwingt die öffentliche Verwaltung, sich auf die Datenverarbeitungen und -erhebungen zu beschränken, die für die rechtmäßige Aufgabenerledigung unerlässlich sind. Aufgrund dieses strengen Maßstabs genügt es nicht, dass eine Erhebung von Daten zur Aufgabenerfüllung lediglich geeignet ist oder sie erleichtert.

Derartige Videointerviews mit zeitversetzter Auswertung greifen erheblich stärker in das Recht auf informationelle Selbstbestimmung der Bewerberinnen und Bewerber ein als herkömmliche Auswahlgespräche. Im Unterschied zu flüchtigen, weil nicht reproduzierbaren Wahrnehmungen in einem Gespräch ermöglicht

die Aufzeichnung von Ton und Bild eine detailliertere und intensivere Auswertung auch des nonverbalen Verhaltens (etwa Mimik, Gestik, Tonfall). Dies mag für die Auswahl für Berufe mit starkem Öffentlichkeitsbezug etwa bei Fernsehsendern erforderlich und daher ggf. zulässig sein – für künftige Beschäftigte in der Verwaltung ist es das nicht. Entsprechend gelingt es offenbar anderen Kommunen, vergleichbare Bewerbungsverfahren ohne die Aufzeichnung solcher Videointerviews durchzuführen. Als mildere Mittel, um die Anzahl der einzuladenden Bewerberinnen und Bewerber auf ein zu bewältigendes Maß zu reduzieren, kommen etwa eine Konkretisierung des Anforderungsprofils, die eine bessere Auswertung der Bewerbungsunterlagen ermöglicht, oder eine stellenspezifische Ausweitung kognitiver Eignungstests in Betracht.

Die Aufzeichnung von Videointerviews in Bewerbungsverfahren lässt sich rechtlich auch nicht auf eine Einwilligung der Bewerberinnen und Bewerber stützen, weil eine Einwilligung nur wirksam ist, wenn sie freiwillig erteilt wird. Die Kommune macht die Einladung zu einem persönlichen Vorstellungsgespräch jedoch von der erfolgreichen Auswertung eines Videointerviews abhängig. Daher wissen die Betroffenen, dass sie ohne Einwilligung zur Aufzeichnung ihres Videointerviews keine Chance auf die ausgeschriebene Stelle haben. Da insoweit Einwilligungen nicht freiwillig, sondern wegen eines faktischen Zwangs erteilt würden, kommt das Einverständnis der Bewerberinnen und Bewerber hier nicht als Rechtsgrundlage für die Datenverarbeitung in Betracht.

Aufgrund der dargestellten Erwägungen zu Erforderlichkeit und Freiwilligkeit ist ein solches zeitversetztes Videointerviewverfahren auch nicht mit dem Anspruch der Bewerberinnen und Bewerbern aus Art. 33 Abs. 2 Grundgesetz (GG) vereinbar. Nach Art. 33 Abs. 2 GG darf über Anträge auf Zugang zu öffentlichen Ämtern nur nach Maßgabe von Eignung, Befähigung und fachlicher Leistung entschieden werden. Wie erläutert nimmt die Kommune bei ihrem Verfahren in Kauf, dass sie diejenigen Personen vom weiteren Bewerbungsverfahren ausschließt, die nach den vorliegenden Bewerbungsunterlagen zwar grundsätzlich geeignet sind, aber ihr Recht am eigenen Bild und am gesprochenen Wort nicht preisgeben wollen. Ein Ausschluss wegen der Geltendmachung von Rechten der informationellen Selbstbestimmung widerspricht jedoch dem Anspruch der Bewerberinnen und Bewerber gemäß Art. 33 Abs. 2 GG auf Durchführung eines Verfahrens, in dem ausschließlich Eignung, Befähigung und fachliche Leistung über die Auswahl entscheiden.

Das videounterstützte Vorauswahlverfahren ist im Übrigen im konkreten Fall für die Betroffenen intransparent. Sie werden im Unklaren gelassen, welchen Personen bzw. Stellen die ihnen abverlangten Bild- und Tonaufnahmen zur Kenntnis gelangen. Unklar ist auch, wie bei der zeitversetzten Auswertung durch die so genannten Evaluatoren die Verpflichtung gemäß

§§ 1 und 6 Abs. 1 Satz 2 Allgemeines Gleichbehandlungsgesetz gewahrt wird und gesetzwidrige Benachteiligungen von Bewerberinnen und Bewerbern unterbleiben.
Wir haben der Kommune empfohlen, von der weiteren Durchführung solcher zeitversetzten Videointerviews abzusehen. Leider konnte keine Verständigung erzielt werden, sodass wir ihre Vorgehensweise förmlich beanstandet haben.

Der Einsatz neuer Auswahlinstrumente in Bewerbungsverfahren hat stets auch das Recht der Bewerberinnen und Bewerber auf informationelle Selbstbestimmung zu beachten. Die einstellende Behörde hat ein berechtigtes Interesse, Auswahlverfahren möglichst effizient zu gestalten. Nicht erforderliche intensive Eingriffe in die Persönlichkeitsrechte der Betroffenen rechtfertigen dies jedoch nicht. Daher gilt es Lösungen zu entwickeln, die beide Ziele vereinbaren statt Effizienz und informationelle Selbstbestimmung zum Nullsummenspiel zu machen.

9.1.3 Beschäftigtendaten in der DNA-Referenzdatei

Die Analyse von DNA-Substanzen wird immer leistungsfähiger. Manchmal reichen bereits wenige Körperzellen am Tatort aus, um den Täter zu überführen. Sichergestellte DNA-Substanzen können jedoch auch von mit der Ermittlung und Auswertung solcher Spuren betrauten Beschäftigten stammen. Um diese von DNA-Merkmalen Tatverdächtiger abzugrenzen, wird beim Landeskriminalamt (LKA) eine DNA-Referenzdatei geführt. Eine Rechtsgrundlage hierfür fehlt bisher.

In der DNA-Referenzdatei werden DNA-Muster von Personen erfasst, die im Bereich der Polizei häufig engen Kontakt zu Spuren und Asservaten haben – so genannte berechtigte Spurenträger. Die Abgabe von Speichelproben der Betroffenen zur Bestimmung ihres DNA-Identifizierungsmusters und dessen Speicherung in der DNA-Referenzdatei werden bislang lediglich auf ihre Einwilligungen gestützt. Einzelheiten werden durch einen Erlass des Ministeriums für Inneres und Kommunales NRW geregelt. Hiergegen bestehen grundsätzliche datenschutzrechtliche Bedenken.

Die Feststellung, Speicherung und Auswertung eines DNA-Identifizierungsmusters greifen in das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz verbürgte Recht auf informationelle Selbstbestimmung ebenso wie in das Grundrecht auf Datenschutz nach Art. 4 Abs. 2 der Landesverfassung NRW ein. Einwilligungen der Betroffenen allein reichen als Rechtsgrundlage für solche Datenverarbeitungen nicht aus. Geboten ist daher eine gesetzliche Regelung, die flankierende Schutzpflichten und -maßnahmen enthält.

Bereits bei weniger eingriffsintensiven Datenerhebungen im Beschäftigungsverhältnis sind Einwilligungen der Betroffenen problematisch. Rechtswirksam sind Einwilligungen nur bei einer tatsächlich freiwilligen Entscheidung von Betroffenen, mit der Erhebung, Speicherung und Nutzung ihrer Daten einverstanden zu sein. Verlangt wird ein ohne Zwang erteiltes Einverständnis mit der vorgesehenen Datenverarbeitung. Die Betroffenen dürfen sich nicht in einer Situation befinden, die sie faktisch dazu zwingt, sich mit der Erhebung und Verwendung der von ihnen verlangten Daten einverstanden zu erklären. Eine Einwilligungserklärung muss die Datenverarbeitung zudem gemäß Art. 7 und Art. 2 Buchstabe h) der EU-Datenschutzrichtlinie „ohne jeden Zweifel“ und „ohne Zwang“ legitimieren. Mit Inkrafttreten der DS-GVO wird sich hieran nichts ändern (siehe Erwägungsgrund 43 der DS-GVO). Zweifel an der Freiwilligkeit bestehen hier, weil die Betroffenen in einem Formblatt „Erläuterungen zur Einwilligungserklärung DNA-Referenzdatei NRW“ erfahren, dass ihr Dienstherr den Aufbau einer solchen Datei als erforderlich und gewünscht einstuft. Dadurch dürften sie sich jedenfalls

einer bestimmten Erwartungshaltung ausgesetzt sehen, an dem vom Dienstherrn gewünschten Verfahren teilzunehmen.

Geboten erscheint daher ein gesetzlicher Rahmen, der es den Betroffenen ermöglicht, informiert und ohne Zwang über die Erteilung der Einwilligung zu entscheiden. Auch bei polizeilichen DNA-Reihenuntersuchungen ist etwa festgelegt, dass diese nicht allein auf Einwilligungen von Personen im näheren Tatumfeld gestützt werden dürfen, sondern gesetzlichen Voraussetzungen unterliegen. § 81h Strafprozessordnung sieht in den Absätzen 1 und 4 neben schriftlichen Einwilligungen der betreffenden Personen ergänzende Belehrungspflichten vor.

Eine entsprechende gesetzgeberische Grundentscheidung ist ebenso bei den vorliegend betroffenen Beschäftigten geboten. Eine Regelung allein durch Erlass des Ministeriums erscheint nicht ausreichend, weil es um Eingriffe in die Grundrechte der Beschäftigten geht. Der Gesetzgeber muss darüber befinden, ob und ggf. unter welchen Voraussetzungen auch für Beschäftigte im Polizeidienst sowie dem Assistenzpersonal vorgesehen werden kann, von ihnen DNA-Identifizierungsmuster zum Ausschluss von Trugspuren zu erfassen. Die Einwilligung der Betroffenen in die Entnahme ihrer Körpersubstanz und die anschließende Datenspeicherung und -nutzung ihrer DNA ist durch Schutzpflichten und -maßnahmen zu flankieren. Nur eine auf die Einwilligung der Betroffenen abstellende Gesetzesregelung mit klaren Rahmenbedingungen kann zu einer eigenverantwortlichen und freien Entscheidung der Betroffenen führen, ob sie mit der Abgabe, Speicherung und Nutzung ihrer DNA zu den vorgesehenen Zwecken einverstanden sind. Die gesetzliche Vorgabe muss zudem Rechtssicherheit bis hin zu (äußerstenfalls einklagbaren) Ansprüchen vermitteln, dass mit der DNA ausschließlich nach gesetzlich klar begrenzten Zwecken verfahren wird. Zudem ist ein Benachteiligungsverbot für die Betroffenen gesetzlich zu verankern, die sich gegen diese Maßnahme entscheiden.

Gesetzlich abgesicherte Datenschutz- und Persönlichkeitsrechte der betroffenen Beschäftigten dürften zu einer höheren Akzeptanz der DNA-Referenzdatei und damit zu einer vermehrten Teilnahme daran führen. Damit ließe sich das Risiko fehlgeleiteter Fahndungsmaßnahmen der Strafverfolgungsbehörden deutlich verringern.

9.1.4 Keine einheitliche Kennziffer für allgemeine Personalverwaltung und Beihilfe

Vorgänge der allgemeinen Personalverwaltung sind von Beihilfevorgängen getrennt zu halten. Eine einheitliche Personalnummer für beide Bereiche ist daher unzulässig. Darauf haben wir bei der Änderung des Gesetzes über die kommunalen Versorgungskassen und Zusatzversorgungskassen im Lande NRW hingewiesen.

Im Zuge der Evaluation des Gesetzes über die kommunalen Versorgungskassen und Zusatzversorgungskassen im Lande NRW setzten sich die kommunalen Zusatzversorgungskassen für eine Ausweitung ihrer Datenverarbeitungsbefugnisse ein. Eine beabsichtigte geschäftsbereichsübergreifende Verarbeitung von Beschäftigtendaten sollte sich auf die Änderung von Stammdaten der Bereiche Bezüge- und Beihilfebearbeitung erstrecken. Die vorgeschlagene Gesetzesergänzung hätte für eingehende Änderungsanzeigen zu einer einheitlichen personenbezogenen Kennziffer geführt – anstelle der bislang getrennten Personalkennzeichen (Beihilfenummer und Personalnummer).

Eine Zusammenführung der bislang getrennten Personal- und Beihilfenummern zu einer einheitlichen Personalkennziffer für allgemeine Personalangelegenheiten und Beihilfezwecke ist unzulässig. Das gesetzliche Abschottungsgebot (§ 84 Gesetz über die Beamtinnen und Beamten des Landes Nordrhein-Westfalen – LBG NRW) gebietet eine vollständige Trennung von Personal- und Beihilfevorgängen. Zudem sind mit einer einheitlichen Personalnummer höhere datenschutzrechtliche Missbrauchsrisiken verbunden. Auch auf den Grundgedanken aus § 290 Abs. 1 Sätze 4 und 5 Sozialgesetzbuch Fünftes Buch (SGB V) muss in diesem Zusammenhang hingewiesen werden: Die Rentenversicherungsnummer darf zur Vermeidung von Rückschlüssen nicht als Krankenversichertennummer verwendet werden. Im Beamtenrecht sollte hinsichtlich der Personal- sowie der Beihilfenummer Vergleichbares gelten.

Unsere Stellungnahme gegen eine Zusammenführung der Personal- und der Beihilfenummer wurde erfreulicherweise vom Innenministerium NRW berücksichtigt. Personal- und Beihilfenummern bleiben daher auch weiterhin getrennt.

9.2 Nicht-öffentlicher Bereich

9.2.1 Digitale Medien und Beschäftigtenkontrolle

Digitale Medien halten auch in das Beschäftigungsverhältnis Einzug. Mit Unterstützung digitaler Informations- und Kommunikationstechnologie, zum Beispiel Internet und Mobiltelefonie, können Beschäftigte nahezu lückenlos überwacht werden. Zu nennen sind hier Arbeitszeiterfassung, automatisierte Personalmanagementsysteme, Telekommunikations- und Bürokommunikations-Systeme, biometrische Erkennung und Erfassung sowie Videoüberwachung. Der Datenschutz zeigt hier Grenzen auf.

Arbeitgeber haben spezifische Informationsbedürfnisse hinsichtlich der betrieblichen Tätigkeit ihrer Beschäftigten. Dies betrifft die Einhaltung von arbeitsvertraglichen Pflichten und Sicherheitsbestimmungen, die Beobachtung von Produktionsabläufen sowie die optimierte Einbindung des Personals in die betrieblichen Abläufe. Ist Beschäftigten die private Nutzung betrieblicher Einrichtungen, etwa Telefon, E-Mail und Internet am Arbeitsplatz gestattet, kommt zudem eine Kontrolle des Umfangs dieser privaten Tätigkeit während der Arbeitszeit in Betracht.
Demgegenüber steht das Interesse der Beschäftigten, nicht fortwährend kontrolliert und überwacht zu werden. Jede darauf ausgerichtete Maßnahme betrifft das Persönlichkeitsrecht der Betroffenen und greift in ihre Privatsphäre ein.

Grundsätzlich gilt: Arbeitgeber dürfen Beschäftigtendaten nur erheben, verarbeiten und nutzen, wenn hierfür eine Rechtsgrundlage besteht und soweit die beabsichtigte Maßnahme erforderlich ist. Eine anlasslose und unbegrenzte Überwachung von Beschäftigten ist nicht verhältnismäßig und damit unzulässig. Es bedarf insoweit einer Prüfung im Einzelfall. Eine Einwilligung Beschäftigter scheidet wegen der zumeist mangelnden Freiwilligkeit einer solchen Erklärung aufgrund des Über- und Unterordnungsverhältnisses im Beschäftigtenverhältnis regelmäßig aus.

Mit der „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ hat die Datenschutzkonferenz privaten Arbeitgebern, Beschäftigten und Betriebsräten eine Übersicht über die datenschutzrechtlichen Anforderungen und Regelungsmöglichkeiten gegeben. Sie ist auf unserer Internetseite www.ldi.nrw.de abrufbar. Die Orientierungshilfe soll es den Interessierten insbesondere erleichtern, eine klare Regelung im Unternehmen zu erreichen, soweit eine private Nutzung des Internets und/oder des E-Mail-Dienstes erlaubt sein soll. Zudem enthält sie ein Muster für eine Betriebsvereinbarung für die private Nutzung von Internet und/oder des betrieblichen E-Mail Postfachs.

Zudem werden wir weiterhin um Bewertungen zur Nutzung moderner Ortungssysteme gebeten, insbesondere durch die Global Positioning System (GPS)-Ortung via Satellit. Aus den empfangenen Positions- und Zeitdaten von GPS-Satelliten können Positionen bestimmt und unter Verwendung der Telematik an einem Computer angezeigt werden. Häufig kommt die GPS-Ortung bei der Fahrzeug- und Handyortung zum Einsatz. Die Zulässigkeit ist im Einzelfall unter Beachtung des Zwecks der Datenverarbeitung, der technischen Möglichkeiten des Systems und dessen tatsächlichem Gebrauch genau zu prüfen. Soweit durch den Einsatz jedoch detaillierte Bewegungsprofile der Beschäftigten erstellt werden (können), ist der Einsatz unzulässig.

Zu der Frage der rechtlichen Zulässigkeit von Ortungssystemen geben wir mit unserer Orientierungshilfe „Ortungssysteme und Beschäftigtendatenschutz“ Hinweise und Empfehlungen dazu, was Unternehmen beachten müssen, die den Einsatz solcher Ortungssysteme beabsichtigen. Sie ist auf unserer Internetseite www.ldi.nrw.de abrufbar.

Unabhängig davon, ob der Arbeitgeber beabsichtigt, die genannten technischen Einrichtungen zu Kontrollzwecken der Beschäftigten zu nutzen, handelt es sich bei deren Einsatz regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten objektiv geeignet ist (ständige Rechtsprechung des Bundesarbeitsgerichts, BAG Beschluss vom 6. Dezember 1983, 1 ABR 43/81). Daher ist gem. § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Betriebsrat zu beteiligen. In einer Betriebsvereinbarung ist darauf hinzuwirken, dass der Katalog der Daten und die Auswertung in so engen Grenzen gehalten werden wie möglich.

Einer Vielzahl technisch machbarer – und häufig auch angewandter – Überwachungsszenarien im Beschäftigungsverhältnis steht ein nur geringer datenschutzrechtlicher Regelungsrahmen gegenüber. Die Rechtsprechung der Arbeitsgerichte gibt hier weitere Anhaltspunkte. Unsicherheiten auf Seiten der Beschäftigten wie auch der Arbeitgeber kann nur durch ständige Aufklärung und Beratung seitens der Aufsichtsbehörden unter Einbeziehung der betrieblichen Datenschutzbeauftragten begegnet werden. Ein Allgemeines Beschäftigtendatenschutzgesetz würde zu mehr Rechtssicherheit beitragen.

9.2.2 Einsatz einer Sprachanalyse-Software bei der Personalrekrutierung

Ein Unternehmen verspricht, mit einer Sprachanalyse-Software schnell und mit wenig Aufwand weitgehende Erkenntnisse über Eigenschaften und Persönlichkeitsmerkmale von Bewerberinnen und Bewerbern zu liefern. Das wirft datenschutzrechtliche Probleme auf.

Wie einsatzbereit, wie belastbar, wie kommunikativ, wie teamfähig, wie charismatisch sind die Bewerberinnen und Bewerber? Wie gestalten sie ihre Beziehungen? Sind sie zielorientiert, ausgeglichen, offen für neue Erfahrungen und bereit, Verantwortung zu übernehmen? Das sind Fragen, die viele Arbeitgeber interessieren – und ein Unternehmen aus NRW verspricht, die Fragen allein mit seiner Software anhand einer kurzen Sprachprobe der Betroffenen schnell und belastbar beantworten zu können.

Alles, was das Unternehmen für seine umfassende psychologische Beurteilung von den zu bewertenden Personen benötigt, ist eine Aufzeichnung eines kurzen Telefoninterviews der Person mit einem Computer. Die Software analysiert anschließend nicht, was die Person sagt, sondern ausschließlich, wie sie es sagt: die Sprache und die Sprechweise – zum Beispiel die sprachliche Vielfalt, die Wortwahl, die Satzlängen, die Anzahl der Füllwörter und Pausen, aber auch die Sprachmelodie und stimmliche Eigenschaften wie Lautstärke, Monotonie.

Das individuelle Ergebnis wird verglichen mit einer Referenzdatei, in der Sprach- und Sprechmuster von Vergleichspersonen mit deren psychologischen Profilen verknüpft sind, die aus herkömmlichen Tests und Begutachtungen gewonnen wurden. Im Wege des Abgleichs werden die sprachlichen Eigenarten der getesteten Person auf ihre Abweichungen vom Durchschnitt der Vergleichspersonen untersucht. Die kommunikativen und psychologischen Eigenschaften einer Vergleichsgruppe mit ähnlichen Sprach- und Sprechmustern werden dann der konkret zu bewertenden Person zugeschrieben. Im Ergebnis trifft die Software also auf Basis einer kurzen Sprachprobe automatisiert eine Wahrscheinlichkeitsaussage über das jeweilige Persönlichkeitsprofil. Das Unternehmen spricht insoweit von Vorhersagen. Diese seien valide und annähernd so aussagekräftig wie deutlich aufwändiger erstellte psychologische Gutachten.

Ob der Rückschluss etwa von stimmlichen Eigenschaften auf den Charakter einer Person tatsächlich im behaupteten Umfang wissenschaftlich haltbar ist, wurde in der Vergangenheit bereits bei so genannten Lügendetektoren angezweifelt. Zusätzlich stellen sich hier konkrete Fragen, wie etwa: Erzielen Personen mit professioneller Sprach- und Stimmbildung nur bessere Ergebnisse in Bezug auf kommunikative Fähigkeiten oder schneiden sie auch bei sonstigen Charaktereigenschaften

besser ab? Werden Personen, die zur Vermeidung gesundheitlicher oder herkunftsbezogener Sprachschwierigkeiten langsamer oder mit anderer Stimmmelodie sprechen, allein deswegen abweichende Charaktereigenschaften zugeschrieben? Welche Qualität hat die Referenzdatei mit den psychologischen Profilen der Vergleichspersonen? Gibt es eine unabhängige wissenschaftliche Prüfung zur Aussagekraft der Vorhersagen und den insoweit bestehenden Grenzen des zugrunde liegenden Modells?

Unabhängig von diesen grundsätzlichen Fragen zur Charakterbewertung mittels Sprachanalyse sind hier zunächst zwei Aspekte von Bedeutung: das Verbot, bestimmte Entscheidungen ausschließlich auf automatisierte Datenverarbeitungsverfahren zu stützen und das Spannungsfeld zwischen statistischen Wahrscheinlichkeitsaussagen und Einzelfallgerechtigkeit. Anschließend geht es um die Frage, ob es für den Einsatz der Software in Personalauswahlverfahren eine Rechtsgrundlage gibt.

Automatisierte Einzelentscheidungen im Sinne von § 6a Bundesdatenschutzgesetz?

Nach § 6a Bundesdatenschutzgesetz (BDSG) sind Entscheidungen mit rechtlichen Folgen oder erheblichen Beeinträchtigungen für die Betroffenen – etwa Entscheidungen zulasten von Bewerberinnen und Bewerbern – grundsätzlich unzulässig, soweit sie sich auf automatisierte Bewertungen von Persönlichkeitsmerkmalen stützen, ohne dass eine natürliche Person die entscheidungserheblichen Sachverhalte prüft und auf dieser Basis eigenständige Entscheidungen trifft. Der Gesetzgeber will damit verhindern, dass Einzelne bei solchen Entscheidungen zum bloßen Objekt einer automatisierten Persönlichkeitsbewertung werden. Daher müssen bei einer Personalauswahl die dafür Verantwortlichen nicht nur theoretisch, sondern auch faktisch in der Lage sein, trotz einer möglicher Weise ungünstigen Bewertung durch die Software eine positive Entscheidung zugunsten der bewerteten Person zu treffen.

Das Unternehmen rät eigenen Angaben zufolge dazu, die Software bei der Personalauswahl lediglich als zusätzliches Mittel der Entscheidungsfindung einzusetzen. Die faktische Wirkung eines mittels der Software vorliegenden Persönlichkeitsprofils dürfte für die Einschätzung der betroffenen Person dennoch immens sein, weil das von der Software erstellte Persönlichkeitsprofil die Einschätzung der bis zur Bewerbung unbekannten Person maßgeblich prägen wird. Dies gilt insbesondere, wenn die Personalverantwortlichen weder die Qualität der zugrunde liegenden Referenzdatei und der Wahrscheinlichkeitsaussagen nachvollziehen können, noch es eine Kontrollbewertung in Form einer herkömmlichen psychologischen Begutachtung gibt.

Um nicht schon bereits unter das Verbot automatisierter Einzelfallentscheidungen (§ 6a BDSG) zu fallen, sind daher mindes-

tens folgende Voraussetzungen zu beachten:

- Alle Bewerberinnen und Bewerber, deren Persönlichkeit mit der Software bewertet wurde, müssen zu einem Vorstellungsgespräch eingeladen werden, in dem trotz einer ungünstigen automatisierten Bewertung eine reale Chance auf eine positive Auswahlentscheidung besteht (keine Vorauswahl allein durch automatisierte Persönlichkeitsbewertung).

- Dafür benötigen die Personalverantwortlichen zum einen hinreichende Kenntnisse über die Funktionsweise, die Aussagekraft der automatisierten Persönlichkeitsbewertung und deren Grenzen. Zum anderen müssen sie die fachliche Kompetenz haben, sowohl diese Informationen zur Software als auch die Bewerberinnen und Bewerber eigenständig im Hinblick auf die abgefragten Merkmale bewerten zu können.

Statistische Persönlichkeitsbewertung versus Einzelfallgerechtigkeit?

Die Software trifft eine Aussage über die Wahrscheinlichkeit bestimmter Eigenschaften und Fähigkeiten. Diese wird abgeleitet aus den in der Referenzdatei gespeicherten Charakterprofilen von Vergleichspersonen mit ähnlichen Stimm- und Spracheigenschaften. Wie bei allen Wahrscheinlichkeitsaussagen sind treffsichere Feststellungen bestenfalls als Durchschnittswert für eine Gesamtgruppe, nicht aber für eine konkrete Person möglich. Der Einzelfall kann stets von der statistischen Regel abweichen. Die damit verbundene Ungewissheit wird nochmals erheblich verstärkt, wenn die Datenbasis unvollständig oder die Qualität und Aussagekraft der Referenzdaten unklar ist.

Weitere Einbußen sind wahrscheinlich, wenn wie im Fall der Sprachanalyse die untersuchten Merkmale lediglich Indizcharakter haben. So berücksichtigt die Software für die Bewertung berufsrelevanter Kompetenzen wie „Einsatzbereitschaft“ und „Teamfähigkeit“ nicht tatsächlich beobachtetes Verhalten (etwa in einem Rollenspiel), sondern nur sprach- und stimmliche Merkmale, die Rückschlüsse auf diese Fähigkeiten zulassen sollen. Im Ergebnis können die statistisch ermittelten Eigenschaften für den Durchschnitt der in der Referenzdatenbank hinterlegten Vergleichsgruppe aussagekräftig sein, die konkret bewertete Person hingegen aber nur unzureichend charakterisieren. Die Bewerberinnen und Bewerber wollen jedoch als individuelle Persönlichkeit und nicht als Mitglied einer statistischen Vergleichsgruppe wahrgenommen und beurteilt werden. Nicht das Einsortieren in Schubladen durch einen undurchschaubaren Algorithmus, sondern ihre tatsächlichen Fähigkeiten sollen ausschlaggebend für ihre Eignung und Befähigung sein.

§ 32 BDSG als Rechtsgrundlage für den Einsatz der Software?

Neben den aufgezeigten Problemen des Verbotes automatisierter Einzelentscheidungen und der Einzelfallgerechtigkeit statistischer Bewertungen sind beim Ein-

satz der Software in Bewerbungsverfahren vor allem die Voraussetzungen des § 32 Abs. 1 Satz 1 BDSG zu beachten. Danach sind Erhebungen und Verarbeitungen von Daten für die Personalauswahl nur zulässig, wenn sie für die Entscheidung über die Begründung eines Beschäftigtenverhältnisses erforderlich sind.

Der Einsatz der Sprachanalyse-Software zur Erstellung eines Persönlichkeitsprofils greift stärker in das Recht auf informationelle Selbstbestimmung der Bewerberinnen und Bewerber ein als herkömmliche Auswahlgespräche oder Assessment-Center-Verfahren. Bereits die Aufzeichnung der Sprachprobe ermöglicht im Unterschied zu flüchtigen, weil nicht reproduzierbaren Wahrnehmungen bei Rollenspielen, Gruppendiskussionen oder Auswahlgesprächen eine viel detailliertere und intensivere Auswertung der individuellen Sprach- und Sprechweise. Der anschließende Abgleich mit der Referenzdatei und die statistische Zuordnung von Persönlichkeitsmerkmalen verstärken den Eingriff in die informationelle Selbstbestimmung. Den Bewerberinnen und Bewerbern werden allein auf Grundlage der Sprachprobe charakterliche Eigenschaften und Kompetenzen zugewiesen oder abgesprochen, ohne dass sie durch eigene Leistungen und Darstellung ihrer Fähigkeiten einen Einfluss darauf haben.

Herkömmliche Instrumente in Bewerbungsverfahren, wie auch die Probezeit zu Beginn des Beschäftigungsverhältnisses, sind insoweit ein deutlich milderes Mittel, um die Bewerberinnen und Bewerber leistungs- und verhaltensabhängig zu beurteilen.

Im Übrigen umfasst das Recht am eigenen Wort auch Aufzeichnungen, bei denen nicht der aufgezeichnete Inhalt, sondern die Sprechweise und Stimme untersucht werden sollen. Daher ist unabhängig von der strafrechtlichen Regelung in § 201 Strafgesetzbuch bereits die Aufzeichnung der Sprachprobe ohne Einwilligung der Betroffenen grundsätzlich unzulässig.

Einwilligung der Bewerberinnen und Bewerber als Rechtsgrundlage?

Soweit die Voraussetzungen des § 32 Abs. 1 Satz 1 BDSG nicht erfüllt sind, bedarf es vor der Aufzeichnung der Sprachprobe und dem Einsatz der Software auf jeden Fall einer wirksamen, also informierten und freiwilligen Einwilligung im Sinne des § 4a BDSG. Freiwillig ist die Einwilligung nur, wenn sich die Betroffenen nicht in einer Situation befinden, die sie faktisch dazu zwingt, sich mit der Erhebung und Verwendung der von ihnen verlangten Daten einverstanden zu erklären.

Das Unternehmen weist eigenen Angaben zufolge seine Kundinnen und Kunden darauf hin, dass die Teilnahme an der Sprachanalyse nur freiwillig erfolgen darf. Im Rahmen eines Auswahlverfahrens ist allerdings eine freiwillige Teilnahme kaum vorstellbar. Denn dann müsste gewährleistet sein, dass die Bewerberinnen und Bewerber auch bei einer verweigerten Sprachanalyse ungeschmälerte Chancen

auf die ausgeschriebene Stelle haben. Andernfalls wäre die Erklärung der Einwilligung aus Sicht der Betroffenen faktische Voraussetzung für eine erfolgreiche Bewerbung – und damit unfreiwillig und unwirksam.

Die sich aus dem Einsatz der Sprachanalyse-Software ergebenden Datenschutzprobleme wurden mit dem Unternehmen eingehend erörtert. Dabei wurde deutlich gemacht, dass algorithmisch erstellte Persönlichkeitsbewertungen anhand einer Sprachprobe ein erheblicher Eingriff in die Persönlichkeitsrechte der Betroffenen sind. Das Verfahren ist daher sowohl unter dem Gesichtspunkt der Erforderlichkeit im Sinne des § 32 Abs. 1 BDSG als auch unter dem Gesichtspunkt der mangelnden Freiwilligkeit von Einwilligungen in Bewerbungsverfahren problematisch. Bis zum Ende des Berichtszeitraums stand noch nicht fest, ob Arbeitgeber in NRW die Software im Rahmen von Auswahlverfahren einsetzen.

Die mit einer Sprachanalyse-Software algorithmisch erstellten Persönlichkeitsprofile sind im Rahmen von Auswahlverfahren unter unterschiedlichen Gesichtspunkten problematisch. Sollte sich herausstellen, dass Arbeitgeber in NRW die Software in Personalauswahlverfahren einsetzen, werden wir daher aufsichtsrechtliche Maßnahmen prüfen.

9.2.3 Keine Totalüberwachung Beschäftigter durch Bondatenanalysesystem

Für Inhaber größerer Einzelhandelsbetriebe ist es häufig schwierig, Manipulationsversuche durch eigene Mitarbeiter bei Kassiervorgängen aufzudecken. Deshalb führte ein Unternehmen ein so genanntes Bondatenanalysesystem ein, das selbständig die Bondaten der einzelnen Märkte auf Unregelmäßigkeiten bei den Kassiervorgängen überprüft.

Kontrollen von Beschäftigten zur Verhinderung von Straftaten und sonstigen Rechtsverstößen können unter Beachtung der Voraussetzungen des § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) zulässig sein. Grundsätzlich kommen alle Maßnahmen im Unternehmen in Betracht, die das regelkonforme Verhalten der Beschäftigten gewährleisten. Solche Maßnahmen müssen allerdings verhältnismäßig sein. So wären beispielsweise flächendeckende verdachtsunabhängige automatisierte Abgleiche von Beschäftigtendaten (Screening) nach dem im Beschäftigtendatenschutz geltenden Verbot der Totalüberwachung unzulässig. Andererseits ist der Arbeitgeber nicht verpflichtet, stets zunächst stichprobenartige Überprüfungen in verdachtsanfälligen Bereichen durchzuführen. Sowohl die Interessen der Beschäftigten als auch die der Arbeitgeber sind im Einzelfall zu berücksichtigen.

Das hier zu prüfende Bondatenanalysesystem war zweistufig ausgestaltet.

- Auf der ersten Stufe fand zunächst eine Überprüfung der Bondaten der einzelnen Filialen auf Unregelmäßigkeiten statt. Nach Unternehmensangaben sollte eine festgestellte Unregelmäßigkeit der an der jeweiligen Kasse beschäftigten Person zuzuordnen sein.

- Soweit für einen Arbeitsbereich Auffälligkeiten festgestellt wurden, konnten in einem zweiten Schritt über die Bedienernummer die betroffenen Personen identifiziert werden.

Zulässig und zweckmäßig ist es, die Daten im ersten Schritt anonymisiert zu nutzen. Anonyme Daten lassen keine Rückschlüsse auf eine Person zu und sind damit vom Datenschutzrecht nicht erfasst. Doch oft bestehen Unklarheiten, ob Daten anonymisiert oder pseudonymisiert sind. Daten sind anonymisiert, wenn es nicht mehr möglich ist, diese auf eine bestimmte Person zurückzuführen (§ 3 Abs. 6 BDSG). Dies ist jedoch bei pseudonymisierten Daten möglich. Hier wird etwa ein Name durch eine Nummer – ein Pseudonym – ersetzt. Eine Rückführbarkeit auf eine bestimmte Person ist dann noch möglich. Bei pseudonymisierten Daten finden die Datenschutzgesetze deshalb Anwendung. Ob Daten anonymisiert oder pseudonymisiert sind, ist damit von entscheidender Bedeutung.

Das Unternehmen verwandte bereits auf der ersten Stufe pseudonymisierte, also

auf die einzelne Person zurückführbare Daten.

Wir haben dem Unternehmen daher empfohlen, im ersten Schritt – also zu einem frühen Zeitpunkt der Analyse – zunächst eine anonymisierte Datennutzung vorzusehen. Daran kann sich ggf. eine erneute Überprüfung in konkret auffällig gewordenen Bereichen mit pseudonymisierten Beschäftigtendaten (Bedienernummern) anschließen. Dieser Empfehlung folgte das Unternehmen und hat das Analysesystem entsprechend umgestellt.

Analysesysteme zur Aufdeckung von Manipulationen in Unternehmen dürfen nicht zu einer anlasslosen Totalüberwachung der Beschäftigten führen, sondern müssen verhältnismäßig sein. Sofern eine anonymisierte Überprüfung nicht ausreicht, kann bei Auffälligkeiten in bestimmten Bereichen eines Unternehmens eine personenbezogene Überprüfung im Einzelfall erfolgen. Der Fall zeigt, dass gute Ergebnisse erzielt werden können, wenn Unternehmen sich frühzeitig an uns wenden. Mögliche datenschutzrechtliche Probleme können so im Vorfeld ausgelotet und Gesetzesverstöße vermieden.

9.2.4 Betriebsinterne Veröffentlichung von Krankendaten

Ein Unternehmen veröffentlichte den Krankenstand innerhalb des Betriebs, um auf Fehlzeiten aufmerksam zu machen. Ein klarer Verstoß gegen den Datenschutz.

Der Geschäftsführer des Unternehmens versandte per E-Mail eine Grafik an die gesamte Belegschaft. Daraus ergaben sich die Fehlzeiten aller namentlich genannten Beschäftigten.

Die betriebsinterne Veröffentlichung dieser Daten stellt einen Verstoß gegen das Bundesdatenschutzgesetz (BDSG) dar. Gemäß § 43 Abs. 2 Nr. 3 BDSG handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft. Indem die jeweiligen Fehlzeiten als „Krankentage“ deklariert worden waren, ließen sich Rückschlüsse auf den Gesundheitszustand der Betroffenen ziehen. Es handelte sich insofern um Angaben über die Gesundheit und damit um besonders sensible Daten.

Außerdem unterliegen Personaldaten dem Datengeheimnis (§ 5 BDSG). Danach ist es den bei der Datenverarbeitung beschäftigten Personen – zum Beispiel in der Personalabteilung – untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.

Der Geschäftsführer des Unternehmens räumte den datenschutzrechtlichen Verstoß ein und akzeptierte das von uns festgesetzte Bußgeld. Er gab an, sich in einer erheblichen wirtschaftlichen Drucksituation befunden zu haben. Aufgrund des hohen Krankenstandes sei die termingerechte Fertigstellung von Aufträgen in Gefahr gewesen. Deshalb habe er die Belegschaft auf die Situation aufmerksam machen wollen. Im Nachgang zu diesem Vorfall haben die verantwortlichen Personen im Unternehmen gemeinsam mit dem Betriebsrat Maßnahmen erörtert, um Verstöße gegen Datenschutzvorschriften zukünftig zu vermeiden. Vereinbart wurde, Fehlzeiten künftig nur noch in einer Form auszuwerten, die keine Rückschlüsse auf Einzelpersonen zulasse. Auch hat sich der Geschäftsführer des Unternehmens bei den Beschäftigten für den Versand der E-Mail entschuldigt.

Die Weitergabe von Gesundheitsdaten in einem Betrieb durch bzw. an unbefugte Betriebsangehörige, die insofern wie Dritte zu betrachten sind, ist datenschutzrechtlich grundsätzlich unzulässig. Das Vorgehen greift erheblich in das Persönlichkeitsrecht der Betroffenen ein. Gerade die Übermittlung besonders sensibler Daten wirkt anprangernd und lässt sich auch durch wirtschaftlichen Druck nicht rechtfertigen.

9.2.5 Weitergabe von Beschäftigtendaten in Zertifizierungsverfahren

Landwirtschaftliche Produktionsbetriebe sind als Zulieferer oftmals von Handelsketten abhängig. Diese verlangen zunehmend eine Agrar-Zertifizierung. Angeboten werden solche Qualitätssicherungs- und Qualifizierungssysteme von privaten Organisationen für die Landwirtschaft. Gerade bei der Feststellung der Sozialkriterien der Beschäftigten ist ihr Recht auf informationelle Selbstbestimmung zu wahren.

Die Zertifizierung soll nachhaltige Produktionsmethoden, eine verantwortungsvolle Nutzung von Wasser und die Rücksicht auf das Wohlergehen der Beschäftigten fördern. In einem Teil des Zertifizierungsverfahrens werden Detailangaben zu den Beschäftigten der Produktionsbetriebe erhoben und verarbeitet. Das weltweit drittgrößte Zertifizierungs-System wird von einem Unternehmen in NRW angeboten. Ein Zusatzmodul dieses Systems erfasst Sozialkriterien der Beschäftigten, insbesondere im Hinblick auf spezifische Aspekte der Arbeitssicherheit und des Gesundheitsschutzes. Akkreditierte Zertifizierungsstellen prüfen für das zertifizierende Unternehmen die Agrar-Unternehmen vor Ort.

Im Rahmen des Zertifizierungsverfahrens bei den Agrar-Unternehmen wurde dort unter anderem Einsicht in die Arbeitsverträge genommen. Daneben bestand die Möglichkeit einer Übermittlung von Beschäftigtendaten auf der Basis einer Einwilligung zum Zweck der Aufnahme in die Zertifizierungsdatenbank. Das zertifizierende Unternehmen stellte hierzu auf seiner Homepage das Muster einer entsprechenden datenschutzrechtlichen Einwilligungserklärung bereit. Betroffen waren die folgenden Beschäftigtendaten: Vor- und Nachname, Beginn und Ende des Arbeitsverhältnisses, Lohnkategorie laut Arbeitsvertrag, vereinbarter Bruttolohn, vereinbarte und geleistete Arbeitszeiten.

Für das Übermitteln dieser Beschäftigtendaten an die Zertifizierungsstellen oder das zertifizierende Unternehmen gibt es keine Rechtsgrundlage. Es besteht insofern weder eine Erforderlichkeit für die Durchführung des Arbeitsverhältnisses gemäß § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) noch für die Verfolgung eigener Geschäftszwecke der Arbeitgeber im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Eine Einwilligung der Beschäftigten kommt nicht in Betracht, weil die Landwirte sich den Forderungen der Zertifizierungsstellen zur Angabe der Daten nicht entziehen können – und sich dieser Druck auch auf die Beschäftigten fortsetzt. Diese stehen regelmäßig in einem Über-/ Unterordnungsverhältnis zu ihren Arbeitgebern mit der Folge eines strukturellen Ungleichgewichts. Die Einwilligungen der Beschäftigten beruhen daher nicht auf einer autonomen und freiwilligen Entscheidung und sind damit unwirksam.

Wir haben das zertifizierende Unternehmen deshalb darauf hingewiesen, dass vor der Einsichtnahme in Arbeitsverträge die Beschäftigtendaten durch die Agrar-Unternehmen zu anonymisieren sind. Alternativ können die erforderlichen Daten im Rahmen der Zertifizierung auch durch einen vertrauenswürdigen Dritten kontrolliert werden, etwa Wirtschaftsprüfer und Steuerberater (Testatlösung) oder Buchprüfer. Das hieraus resultierende anonymisierte Ergebnis sollte in die Checklisten zur Zertifizierung und Evaluierung des jeweiligen Agrarbetriebes übernommen werden.

Bei der Zertifizierung von Betrieben sind die schutzwürdigen Belange der Beschäftigten zu beachten. Für die Datenübermittlung ist weder eine Rechtsgrundlage gegeben noch eine wirksame Einwilligung anzunehmen. Das Zertifizierungsverfahren sollte deshalb ausschließlich auf der Grundlage anonymisierter Beschäftigtendaten durchgeführt werden. Der Zweck des Zertifizierungsverfahrens wird dadurch nicht gefährdet.

10. Gesundheit und Soziales

10.1 Neues Landeskrebsregistergesetz

Am 1. April 2016 trat das neue Landeskrebsregistergesetz in Kraft. Zur weiteren Verbesserung der Krebsbekämpfung als einem der vorrangigen Gesundheitsziele enthält es strukturelle Neuregelungen und löst das bisherige Krebsregistergesetz ab. Vorausgegangen waren umfangreiche Beratungen mit dem Ergebnis einer angemessenen Beachtung des Rechts auf informationelle Selbstbestimmung.

Hintergrund für die Gesetzesänderung ist eine Vorgabe des Bundes. Die Länder sind demnach verpflichtet, klinische Krebsregister nach § 65c Sozialgesetzbuch V (SGB V) zu errichten bzw. anzupassen. NRW setzt dies durch die Gründung eines Landeskrebsregisters mit den Aufgabenbereichen der epidemiologischen und der klinischen Krebsregistrierung um. Während bei der epidemiologischen Krebsregistrierung Daten zum Auftreten von Krebserkrankungen sowie die Art der Primärtherapie bei Personen erfasst werden, erstreckt sich die klinische Krebsregistrierung auf die Erfassung von Daten über das Auftreten, den Verlauf und die Behandlung von Krebserkrankungen bei Personen, die behandelt werden oder wurden. Bei der epidemiologischen Auswertung stehen Fragen zu der zeitlichen und räumlichen Verteilung und Häufigkeit bestimmter Krebserkrankungen und deren möglichen Ursachen im Fokus. Die klinische Auswertung dient primär der Qualitätssicherung und Darstellung der Ergebnisqualität des gesamten Behandlungsverlaufs von Krebspatientinnen und -patienten. Die Daten können zudem unter bestimmten Voraussetzungen für die Forschung zur Verfügung gestellt werden.

Im Krebsregister werden besonders sensible Gesundheitsdaten verarbeitet. Vor diesem Hintergrund haben wir das Ministerium für Gesundheit, Emanzipation, Pflege und Alter des Landes NRW im Vorfeld des Gesetzgebungsverfahrens beraten. Das Gesetz ist das Ergebnis einer tragbaren Rechtsgüterabwägung zwischen dem Recht der einzelnen Person auf informationelle Selbstbestimmung, den Rechtspositionen der meldepflichtigen Personen und dem Allgemeininteresse an einer umfassenden Krebsregistrierung.

Eine zentrale Neuregelung ist die nunmehr nachvollziehbar begründete umfassende Pflicht der Leistungserbringer (insbesondere Ärzte und Krankenhäuser), Krebserkrankungen, ihren Verlauf und den Therapieverlauf anzugeben. Damit kann eine durch den Bundesgesetzgeber vorgezeichnete, möglichst vollständige Registrierung von Krebserkrankungen erreicht werden. Entscheidendes Gewicht ist dem Umstand beizumessen, dass die Ursachen von Krebserkrankungen nur durch entsprechende medizinische Informationen

über große Teile der Bevölkerung weiter erforscht und gefördert werden können. Eine umfassende Krebsregistrierung dürfte insofern einen erheblichen und wertvollen Beitrag für die Krebsforschung sowie die möglichen beeinflussenden Faktoren für diese Erkrankung leisten, was aus datenschutzrechtlicher Sicht ein tragendes Argument im Rahmen der Güterabwägung ist

Zwar bedeuteten umfassende Meldepflichten der Leistungserbringer einen nicht unerheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Patientinnen und Patienten. Datenschutzrechte der Betroffenen sind jedoch angemessen berücksichtigt.

Patientinnen und Patienten haben das Recht, der dauerhaften Speicherung von Teilen ihrer personenbezogenen Daten (so genanntes Identitäts-Chiffrats, § 2 Abs. 14 LRKG NRW) zu widersprechen. Über ihr Widerspruchsrecht nach § 13 Abs. 1 LRGK NRW sind sie umfänglich aufzuklären.

Zudem wird durch technisch-organisatorische Maßnahmen sichergestellt, dass im Rahmen der Registerführung nur die Daten verarbeitet werden, die für die jeweilige Aufgabe erforderlich sind (§ 3 LKRG NRW). Hierzu sind unter anderem Pseudonymisierungs- und Verschlüsselungsverfahren vorgesehen.

Auch Fragen zum Inhalt der Meldepflicht waren zu bewerten. Im Ergebnis halten wir es für zulässig, dass neben dem Tod der betroffenen Person ebenfalls die Todesursache anzugeben ist, auch wenn sie nicht die Krebserkrankung ist (§ 14 Abs. 1 Nr. 5 LKRG NRW). Die genaue Todesursache könnte bei der Krebsforschung auch dann ein relevantes Kriterium sein, wenn sie nach erstem Anschein nicht in unmittelbarem Zusammenhang mit einer Krebserkrankung steht.

Erfreulicherweise sieht das Landeskrebsregistergesetz die in der Vorläuferfassung des Gesetzentwurfs noch enthaltene Erlaubnis, Datenauswertungen mit Namen und Anschriften von Leistungserbringern sowie Bezeichnungen von Arzneimitteln, Wirkstoffen und Therapien zu veröffentlichen, nicht mehr vor.

Bei allgemeinen Auskünften oder Auskünften für Forschungsvorhaben ist darauf zu achten, dass bei den herausgegebenen Informationen keine Rückschlüsse auf betroffene Personen möglich sind (§ 22 Abs. 1 Satz 2, Abs. 2 Satz 4 LKRG NRW).

Zu begrüßen wäre allerdings eine gesetzliche Verpflichtung gewesen, wonach die betroffenen Patientinnen und Patienten ausführlich von den meldepflichtigen Personen selbst zu unterrichten sind und eine Übertragung der Unterrichtungspflicht auf nichtärztliches Personal ausgeschlossen ist. Eine solche, noch in der Vorläuferfassung des Gesetzes vorgesehene Unterrichtung würde die Patientinnen und Patienten in ihrer schwierigen persönlichen Lebenssituation besser in die

Lage versetzen, über das Für und Wider der vorgesehenen Datenspeicherung im Landeskrebsregister zu entscheiden. Da insoweit über Daten aufzuklären ist, die der ärztlichen Diagnostik und Behandlung zuzuordnen sind, wäre es konsequent gewesen, insoweit eine ärztliche Aufklärung über die Vor-und Nachteile einer entsprechenden Entscheidung vorzusehen. Nunmehr ist geregelt, dass die Pflicht der meldepflichtigen Personen zur Unterrichtung zwar übertragen werden kann, wobei insoweit jedoch ausschließlich entsprechend qualifiziertes nichtärztliches Personal in Betracht kommt (§ 13 Abs. 2 LKRG NRW).

Die Neuregelungen im Landeskrebsregistergesetz können zur weiteren Verbesserung medizinischer Erkenntnisse für die betroffenen Patientinnen und Patienten führen. Die meldepflichtigen Personen sollten die dem Landeskrebsregister zu meldenden Daten lückenlos und sorgfältig zusammengestellt übertragen. Dabei sollte insbesondere darauf geachtet werden, dass die Betroffenen über die Verarbeitung ihrer sensiblen Daten im Landeskrebsregister und ihr Widerspruchsrecht nach § 13 Abs. 1 LKRG NRW umfänglich aufgeklärt werden.

10.2 Einwilligungs- und Schweigepflichtentbindungserklärung in der Haftpflichtversicherung

Die Praxis der Haftpflichtversicherungen, Angaben zu Vorerkrankungen des Unfallopfers zu erheben, die nicht im unmittelbaren Zusammenhang mit dem Unfallereignis stehen, kann datenschutzrechtlichen Bedenken begegnen.

Kfz-Haftpflichtversicherungen dürfen Gesundheitsdaten bei Ärztinnen und Ärzten erheben, soweit dies zur Prüfung von Schadensersatzansprüchen nach Unfällen erforderlich ist, und die betroffene Person eine Schweigepflichtentbindungserklärung abgegeben hat. Die Versicherungen sind darüber hinaus auch daran interessiert, das Vorliegen einer Anfälligkeit der Betroffenen für eine bestimmte Erkrankung (Prädisposition) im Hinblick auf die unfallbedingt erlittenen Beeinträchtigungen zu prüfen. Außerdem möchten die Versicherungen ausschließen, dass Vorschäden über die Haftpflichtversicherung mitreguliert werden, die nicht durch den Unfall verursacht wurden. Die in der Versicherungswirtschaft eingesetzten Erklärungsvordrucke wurden zu diesem Zweck auf Vorerkrankungen ausgedehnt, welche für die Beurteilung des Gesundheitsschadens von Bedeutung sein könnten.

Die Kenntnis über Vorerkrankungen ist jedoch erst dann erforderlich, wenn konkrete Zweifel an der Berechtigung der geltend gemachten Ansprüche bestehen. Erst dann sollte von der Einwilligungs- und Schweigepflichtentbindungserklärung zu Vorerkrankungen Gebrauch gemacht werden. Zudem haben sich Versicherungen im Verhaltenskodex dem Grundsatz der Erforderlichkeit verpflichtet. Dies würde zu einem zweistufigen Verfahren führen: Im ersten Schritt wird allein der Schaden abgefragt. Bei Erforderlichkeit dürfen im zweiten Schritt die Vorerkrankungen aufgrund der bereits im Vorfeld eingeholten Einwilligung abgefragt werden. Wer die Entscheidung über die Bedeutung von Vorerkrankungen für den geltend gemachten Schaden nicht der behandelnden Ärztin oder dem Arzt überlassen möchte, hat in dieser Phase des Verfahrens die Möglichkeit, die erforderlichen Gesundheitsdaten zum Nachweis des Schadens selbst direkt an die Versicherung zu senden.

Gemeinsam mit den Datenschutzaufsichtsbehörden der übrigen Länder werden wir im Dialog mit der Versicherungswirtschaft darauf hinwirken, dass der Grundsatz der Erforderlichkeit auch in diesen Fallkonstellationen gewährleistet wird.

10.3 Getrennte Datenhaltung innerhalb eines Gesundheitsamtes

Die in Gesundheitsämtern erhobenen Gesundheitsdaten sind sensibel. Auch innerhalb des Gesundheitsamtes ist deshalb eine strikte Trennung der Gesundheitsdaten erforderlich. Ein Zugriff von Beschäftigten des einen Bereichs auf die personenbezogenen Daten eines anderen Sachgebietes ist auszuschließen.

In einem Gesundheitsamt sollte eine neue Software personenbezogene Daten einzelner Arbeitsbereiche zentral verwalten. Ziel war es, durch eine zentrale Personendatenverwaltung Doppelerfassungen aus den unterschiedlichen Sachgebieten, wie zum Beispiel Amtsarzt oder kinderärztlicher- und sozialpsychiatrischer Dienst, zu verhindern.

Ein Zugriff von Beschäftigten des einen Bereichs auf die personenbezogenen Daten eines anderen Sachgebietes ist jedoch datenschutzrechtlich unzulässig. Dies gilt auch für den Zugriff auf zentral gespeicherte Personendaten („Stammdatensatz“) oder Terminkalender anderer Sachgebiete. Datenweitergaben zwischen den Bereichen eines Gesundheitsamtes sind gemäß § 23 Abs. 2 in Verbindung mit § 5 Abs. 1 Gesundheitsdatenschutzgesetz NRW (GDSG NRW) nur unter den Voraussetzungen zulässig, die für Datenübermittlungen an Dritte zu beachten sind. Diese liegen jedoch nicht vor, soweit Patientendaten durch Zugriffe auf einen gemeinsamen Stammdatensatz amtsintern weitergegeben werden.

Durch das GDSG NRW werden alle personenbezogenen Daten ohne Rücksicht auf die Art der Datenträger geschützt. Als Beispiele nennt die Gesetzesbegründung (LT-Drs. 11/5705 S. 28) alle Angaben zur Person der Patientin oder des Patienten (insbesondere Name, Anschrift und Geburtsdatum), alle Aufzeichnungen über frühere Erkrankungen (insbesondere Arztberichte und Befunde) sowie alle Feststellungen und Aufzeichnungen, die durch Diagnose und Therapie gewonnen werden (zum Beispiel Laborbefunde, Ergebnisse bildgebender Verfahren, OP-Berichte). Danach stellen bereits Informationen zur Terminierung von Untersuchungen oder über Einladungen zu solchen für einzelne Bereiche des Gesundheitsamtes ein gesetzlich besonders geschütztes Patientendatum dar. So könnte etwa die Kenntnis von einer Ladung zur Begutachtung durch den sozialpsychiatrischen Dienst Rückschlüsse auf die Verfassung einer Patientin oder eines Patienten zulassen. Die strikte Trennung von Patientendaten, die in verschiedenen Sachgebieten eines Gesundheitsamtes verarbeitet werden, verlangt auch die ärztliche Schweigepflicht.

Dem Gesundheitsamt haben wir deshalb geraten, die Software so zu gestalten, dass ausschließlich berechtigte Personen Zugriff auf die Daten der einzelnen Sach-

gebiete erhalten – etwa durch ein Rechte- und Rollenkonzept.

Das Gesundheitsdatenschutzgesetz NRW und die ärztliche Schweigepflicht verbieten einen Zugriff auf Patientendaten durch verschiedene Sachgebiete eines Gesundheitsamtes.

10.4 Dokumentationspflicht in der Arztpraxis

Die Dokumentationspflicht bei Patientenakten umfasst auch die Pflicht, Änderungen kenntlich zu machen.

Im Rahmen unserer Beratungstätigkeit bestand Anlass darauf hinzuweisen, dass auch Berichtigungen und Änderungen von Eintragungen in elektronisch oder in Papierform geführten Patientenakten transparent und nachvollziehbar sein müssen. Mit dem Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten vom 20.02.2013 wurde die Dokumentationspflicht von Behandelnden bei den Regelungen zum Behandlungsvertrag im Bürgerlichen Gesetzbuch (BGB) verankert. Diese verpflichten auch zur Revisionssicherheit und entsprechen einer allgemeinen Datensicherheitsanforderung, die sich zum Beispiel auch im Handelsgesetzbuch oder in der Abgabenordnung findet. Auch die Bundesärztekammer verweist in ihrer Informationsschrift „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ (Deutsches Ärzteblatt 2014, Seite 963, 965) darauf, dass die Revisionssicherheit zu gewährleisten ist.

§ 630f BGB als (auch) datenschutzrechtlich relevante Regelung dient insbesondere dem Schutz der Patienteninnen und Patienten vor nachträglich vorgenommenen Änderungen der ärztlichen Dokumentation, etwa aus Anlass eines im Raum stehenden Haftungsanspruchs wegen des Vorwurfs einer fehlerhaften Behandlung. Die Behandelnden sind gehalten, die Patientenakten revisionssicher zu führen und das EDV-Praxisverwaltungssystem bei elektronisch geführten Patientenakten so einzurichten, dass neben dem Zeitpunkt einer Änderung der Dokumentation auch ihr ursprünglicher Inhalt erkennbar bleibt.

Hinweise und Erläuterungen zur Revisionssicherheit finden sich nunmehr auch in den Publikationen der regionalen Ärztekammern in NRW.

10.5 Wearable Computing – ein fragwürdiges Konzept für die Berufsunfähigkeits-, Lebens- und Krankenversicherung

Fitness-Armbänder und andere am Körper getragene Kleincomputer und Sensoren (so genannte Wearables) etablieren sich weiter auf dem Markt. Wie zukunftsweisend Geschäftsmodelle sind, die auf der Basis von Wearable Computing in Verbindung mit Gesundheits-Apps Daten von Versicherten nutzen und für Berufsunfähigkeits-, Lebens- und Krankenversicherungen verschiedene Vergünstigungen gewähren, ist auch eine Frage des Datenschutzes.

Mit der Entwicklung des Wearable Computing hat sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in der Entschließung „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ vom 6./7. April 2016 kritisch auseinandergesetzt. Die Entschließung ist im Anhang abgedruckt und auf unserer Internetseite www.ldi.nrw.de abrufbar.

Auch wenn die Sammlung und Auswertung der eigenen Gesundheitsdaten nützliche Informationen zur besseren Vorsorge bieten und zu einem Zugewinn an persönlicher Lebensqualität beitragen kann, sind damit Risiken für das Persönlichkeitsrecht verbunden.

So stellte die Konferenz insbesondere fest, dass in Beschäftigungs- und Versicherungsverhältnissen Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen den Verwendern und den betroffenen Personen zustande kommen, unwirksam sind und keine Rechtsgrundlage für Datenverarbeitungen liefern. Auch zahlreiche andere Stellen, etwa die Verbraucherzentrale (Bundesverband), üben Kritik an Geschäftsmodellen von Versicherungen, die die Gewährung von Vergünstigungen für die Versicherten an bestimmte durch Gesundheits-Apps generierte Informationen knüpfen. Im Jahresbericht 2015 des Deutschen Ethikrates wird im Abschnitt „Big Data“ im Zusammenhang mit Wearables zentral die Kernfrage hervorgehoben: Wo sollten aus Sicht des Individuums oder gar aus der Sicht des regulierenden Staates Grenzen für die Erhebung, Verknüpfung und Nutzung von Daten gezogen werden? Dargestellt werden im Versicherungswesen und im sozialen Miteinander bewusst oder unbewusst eintretende Entsolidarisierungsdynamiken, die in die Feststellung münden: Der Prämienvorteil des einen sei der Prämiennachteil für den anderen. Der Deutsche Ethikrat hat eine Stellungnahme angekündigt, in der hierzu erste ethische und rechtliche Standards gesetzt werden sollen.

Diese problematischen Entwicklungstendenzen werden an einem uns bekannt gewordenen Geschäftsmodell einer über-

regionalen Versicherungsgesellschaft deutlich. Um gesundheitsbewusstes Verhalten von Versicherten mit rabattierten Versicherungsprämien und sonstigen Vergünstigungen zu belohnen, werden Daten der Betroffenen unter Verwendung von Fitness-Armbändern oder ähnlichen Geräten turnusmäßig an das Versicherungsunternehmen übermittelt. Die Daten offenbaren Informationen zu den Lebensumständen und zum Gesundheitszustand der Versicherten. Neben der datenschutzrechtlichen Kritik an der Freiwilligkeit der Einwilligungen haben auch wir erhebliche Zweifel, ob das Geschäftsmodell den Vorgaben des Versicherungsvertragsgesetzes entspricht und mit dem Solidarprinzip in der Versichertengemeinschaft vereinbar ist. Daher haben wir die Bundesanstalt für Finanzdienstleistungen um eine versicherungsaufsichtsrechtliche Prüfung gebeten.

Die Sichtweise von Befürwortern solcher Geschäftsmodelle, die Versichertengemeinschaft werde durch Bonusprogramme für Versicherte, die sich um ihre Gesundheit kümmern, gestärkt, bleibt einseitig. Personen, die wegen ihrer Konstitution nicht in der Lage sind, an derartigen Programmen teilzunehmen, werden nämlich von vornherein ausgegrenzt.

Aufgrund der dargestellten Risiken sollte der Gesetzgeber für den Einsatz von Wearables und Gesundheits-Apps im Bereich der Berufsunfähigkeits-, Lebens- und Krankenversicherungen einen klaren rechtlichen Rahmen schaffen.

10.6 Mängel bei Wearables

Zusammen mit anderen Datenschutzaufsichtsbehörden haben wir mehrere Wearables geprüft und etwa 70 Prozent des Marktanteils in Deutschland abgedeckt. Die Ergebnisse der Prüfung zeigen etliche Mängel auf.

Bereits im Bericht 2015 unter 5.2 haben wir einen ersten Überblick über die auf dem Markt angebotenen Wearable Computer gegeben– wie Smart Watches, Fitness-Armbänder und Activity-Tracker. Aufgrund der besonderen Gefährdungen für die Privatsphäre der Nutzerinnen und Nutzer sowie Dritter durch diese Computer und Sensoren haben wir gemeinsam mit weiteren Datenschutzaufsichtsbehörden 16 Wearables geprüft. Einbezogen wurden auch die Hersteller-Apps für die Betriebssysteme iOS und Android.

Aus den Aufzeichnungen der Wearable Computer können umfangreiche Schlüsse gezogen werden. Deshalb ist Transparenz von besonderer Bedeutung. Nutzerinnen und Nutzer müssen auf einen Blick erkennen können, ob sie Herr ihrer Daten bleiben. Insbesondere muss klar sein, welche Daten Wearables erheben und ob die Daten an Dritte weitergegeben werden. Auch grundlegende Datenschutzrechte, wie zum Beispiel Auskunfts- und Löschungsansprüche, müssen gewährleistet sein. Diesen Anforderungen werden nicht alle Wearables gerecht.

■ Mangelhafte Datenschutzbestimmungen

Bereits die Datenschutzbestimmungen erfüllen meistens nicht die gesetzlichen Anforderungen. Sie sind in der Regel viele Seiten lang, schwer verständlich und enthalten nur pauschale Hinweise zu essentiellen Datenschutzfragen. Teilweise sind sie nicht einmal in deutscher Sprache erhältlich. Die Hersteller und Betreiber geben sich keine Mühe, Licht in das Dickicht aus Hardware-Hersteller, App-Betreiber, App-Shop-Anbieter und zahlreichen Dienstleistern zu bringen. So erfahren Nutzerinnen und Nutzer oftmals nicht im ausreichenden Maße, wer konkret Zugriff auf die Daten hat und wie lange sie gespeichert werden. Beunruhigend sind auch die Aussagen zur Datenweitergabe. Einige Hersteller stellen ausdrücklich klar, dass sie die Fitness-Daten der Nutzerinnen und Nutzer für eigene Forschungszwecke und Marketing verwenden und an verbundene Unternehmen weitergeben. Nutzerinnen und Nutzer erfahren weder, um wen es sich dabei handelt, noch gibt es eine Möglichkeit zu widersprechen.

■ Datenübermittlung in die ganze Welt

Fast alle Hersteller setzen Tracking-Tools US-amerikanischer Unternehmen ein. Mithilfe dieser Tools können Hersteller erfassen, wie die Geräte oder Apps genutzt werden, um die Benutzerfreundlichkeit zu verbessern. Die Daten sind aber auch für Werbezwecke und zur Profilbildung interessant. Zwar wird oft angegeben, dass

hierzu nur anonyme Daten verwendet werden würden. Den Nachweis bleiben die Hersteller jedoch schuldig. Die Erfahrung zeigt, dass in der Regel in solchen Fällen weiterhin bei vielen Daten ein Personenbezug hergestellt werden kann.

■ Gefahr bei Verlust oder Weiterverkauf

Viele Geräte bieten keine Möglichkeit, Daten selbstständig vollständig zu löschen. Weder im Gerät selbst noch im Nutzerkonto gibt es eine Löschfunktion. Einige Hersteller weisen sogar darauf hin, dass eine Löschung nicht möglich ist. Wie lange die Hersteller die Daten speichern, bleibt verborgen. Der Verlust oder Weiterverkauf von Wearables birgt daher ein enormes Risiko.

Auf der Grundlage der gewonnen Erkenntnisse werden nun weitere Schritte eingeleitet. Einige Mängel ließen sich problemlos dadurch beheben, dass die Fitnessdaten der Wearables lediglich auf das Smartphone weitergeleitet und lokal verarbeitet werden. Eine permanente Übermittlung aller Daten vom Smartphone an Server der Hersteller ist aus unserer Sicht in der Regel mit Risiken verbunden. Indem die Hersteller jedoch alle Daten von der App weiterleiten, signalisieren sie ein eigenes Interesse an den sensiblen Daten.

Auf der Grundlage der gewonnen Erkenntnisse werden nun weitere Schritte eingeleitet. Hersteller und Anbieter sollten bereits bei der Entwicklung neuer Wearables den Datenschutz beachten.

11. Finanzverwaltung und Statistik

11.1 Einsichtsrecht Steuerpflichtiger in die eigene Steuerakte

Das Einsichtsrecht Steuerpflichtiger in die eigene Steuerakte ist nach wie vor gesetzlich nicht verankert. Bereits im Jahr 2009 haben die Datenschutzbeauftragten des Bundes und der Länder einen gesetzlichen Auskunftsanspruch gefordert. In den jüngsten Gesetzesänderungen wurde diese Forderung nicht berücksichtigt.

Finanzämter verweigern Bürgerinnen und Bürger zuweilen immer noch die Einsicht in ihre Steuerakten. Leider müssen wir dann darauf hinweisen, dass es nach wie vor kein gesetzliches Einsichtsrecht gibt.

In einem gemeinsamen Konzept von Bund und Ländern wurde zwischenzeitlich zwar ein Diskussionsentwurf „Modernisierung des Besteuerungsverfahrens“ vorgelegt, der auch Vorschläge für ein Auskunftsrecht und für sonstige Betroffenenrechte in der Abgabenordnung enthält. Diese sind jedoch in datenschutzrechtlicher Hinsicht noch verbesserungsbedürftig. So sind etwa die vorgesehenen Ausschlussgründe für eine Auskunftserteilung oder für eine Unterrichtung der Betroffenen über ohne ihre Kenntnis erhobene Daten zu unbestimmt. Das birgt das Risiko einer uferlosen Auslegung zulasten der Steuerpflichtigen.

Die Bundesbeauftragte für Datenschutz und Informationsfreiheit hat die Kritikpunkte dem Bundesministerium der Finanzen im Frühjahr 2015 mitgeteilt. Bedauerlicherweise ist die Diskussion nicht weiter vorangekommen. Im Gegenteil: Die im Konzept noch vorgesehenen Regelungen wurden in das Gesetz zur Modernisierung des Besteuerungsverfahrens vom 18. Juli 2016 (BGBl. I 2016 S. 1679) nicht aufgenommen.

Gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder werden wir uns weiter dafür einsetzen, dass die Auskunftsansprüche der Steuerpflichtigen zügig und angemessen gesetzlich geregelt werden. Auch das Finanzministerium NRW sollte sich konsequent hierfür einsetzen. Damit sollten Eingaben zu diesen Fragen bald der Vergangenheit angehören.

11.2 Kleine Volkszählung – Neufassung des Mikrozensusgesetzes

Mit dem Mikrozensus sammelt der Staat Informationen über die Bevölkerung, den Arbeitsmarkt sowie die Wohnsituation der Haushalte. Zur Fortführung des Mikrozensus ab dem Jahr 2017 werden verschiedene Haushaltsstatistiken reformiert und an Vorgaben mehrerer EU-Verordnungen angepasst. Das novellierte Mikrozensusgesetz soll Synergieeffekte zur Kostendämpfung des Erhebungsaufwands erzeugen und die Befragungsbelastung der Betroffenen verringern.

In NRW führt der Landesbetrieb Information und Technik NRW den Mikrozensus durch. Bürgerinnen und Bürger erhalten vorab Schreiben, die die Befragung ankündigen. Diese Informationen werfen immer wieder Fragen auf, mit denen sich die Betroffenen an uns wenden. Dabei haben wir festgestellt, dass Unklarheiten zu Lasten der Akzeptanz gehen. Zum Gesetzentwurf zur Neuregelung des Mikrozensus und zur Änderung weiterer Statistikgesetze haben wir gemeinsam mit weiteren Datenschutzbeauftragten der Länder und der Bundesbeauftragten für Datenschutz Stellung genommen.

Konkretisierungen des Gesetzentwurfs wurden begrüßt, aber auch transparentere Regelungen angeregt, etwa zur Bestimmung der Erhebungseinheiten und zum Kernprogramm der Erhebungsmerkmale. Weitere Vorschläge waren:

- Trennung einiger auf europäischen Rechtsakten beruhender Angaben mit Auskunftspflicht gegenüber freiwilligen Angaben der Betroffenen.

- Präzisierung einiger Erhebungsmerkmale, die sich auf Wohnverhältnisse und die persönliche Lebenssituation Auskunftspflichtiger beziehen.

- Orientierung des gesetzlichen Erhebungsumfangs an den in der Gemeinschaftsstatistik über Einkommens- und Lebensbedingungen (EU-SILC) festgelegten Erhebungsmerkmalen.

- Auskunftspflichten, die neben Volljährigen und alle einen eigenen Haushalt führenden Minderjährigen auch sonstige minderjährige Haushaltsmitglieder treffen sollten entweder konkretisiert werden oder entfallen.

- Durch die gemeinsame Durchführung von Stichprobenerhebungen nach § 7 Bundesstatistikgesetz (BStatG) mit dem Mikrozensus soll das Erhebungsmanagement verschlankt und kostensparender werden. Bei einer gemeinsamen Durchführung wären zwar weniger Personen betroffen. Auf diese geringere Anzahl Betroffener werden allerdings bei einer kumulierten statistischen Erhebung umfangreichere Datenerfassungen zukommen. Daher hatten wir angeregt zu prüfen, ob von

einer gemeinsamen Durchführung abgesehen werden kann.

Nur ein die datenschutzrechtlichen Anforderungen berücksichtigendes Gesetz wird auf die notwendige Akzeptanz der Auskunftspflichtigen stoßen und damit ordnungsgemäße statistische Erhebungen gewährleisten. Die vorgeschlagenen Änderungen wurden in dem zwischenzeitlich in Kraft getretenen Mikrozensusgesetz vom 7. Dezember 2016 (BGBl. I S. 2826) in den wesentlichen Punkten leider nicht berücksichtigt.

12. Internet und Medien

12.1 Änderung des WDR-Gesetzes

Mit dem 15. Rundfunkänderungsgesetz vom 2. Februar 2016 wurde das WDR-Gesetz reformiert. Die Änderung betrifft auch die Stellung der bzw. des Datenschutzbeauftragten des Westdeutschen Rundfunks und die Anwendbarkeit des Informationsfreiheitsgesetzes.

Die Änderung des WDR-Gesetzes trat am 13. Februar 2016 in Kraft. Seitdem darf die oder der Datenschutzbeauftragte des Westdeutschen Rundfunks (WDR) während dieser Tätigkeit keine weiteren Aufgaben innerhalb der Anstalt mehr übernehmen. In unserer Stellungnahme an den Landtag haben wir diese Änderung als einen Schritt hin zur Verselbständigung der Datenschutzaufsicht beim WDR begrüßt.

Kritisch sehen wir die Regelung, die die Prüfergebnisse des Landesrechnungshofs (LRH) beim WDR vom Anwendungsbereich des Informationsfreiheitsgesetzes ausnimmt. Neben den journalistisch-redaktionellen Informationen werden nun generell auch Prüfergebnisse des LRH dem Informationsanspruch nach dem Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) entzogen. Im Einzelfall mögen Ablehnungsgründe nach dem IFG die Verweigerung der Information rechtfertigen. Aber besondere sachliche Gründe für eine solche Privilegierung des WDR gegenüber anderen vom LRH geprüften öffentlichen Stellen sind nicht erkennbar und wurden in der Gesetzesbegründung auch nicht dargelegt.

Das Gesetzgebungsverfahren haben wir zugleich zum Anlass genommen, gegenüber dem Landtag auf eine seit 2007 bestehende Diskrepanz zwischen dem Rundfunkstaatsvertrag und dem WDR-Gesetz hinzuweisen, die die Regelungen der Datenschutzkontrolle bei Telemedien betrifft. Regelungsziel des Rundfunkstaatsvertrags ist es, die Datenschutzaufsicht für Telemedien zu bündeln. So soll auch beim öffentlich-rechtlichen Rundfunk außerhalb des journalistisch-redaktionellen Bereichs für Telemedien die allgemeine Datenschutzaufsichtsbehörde zuständig sein. Nach dem WDR-Gesetz verläuft die Trennlinie der Datenschutzkontrolle jedoch an anderer Stelle. Dieses Gesetz nimmt den WDR insgesamt von unserem Zuständigkeitsbereich aus.

Diese Ungereimtheiten mögen bei der Formulierung des Rundfunkstaatsvertrages den unterschiedlichen Rechtslagen in den Ländern geschuldet sein. In der Praxis wird angenommen, dass das WDR-Gesetz vorgeht. Der Gesetzgeber hat das 15. Rundfunkänderungsgesetz leider nicht für eine Klarstellung genutzt.

Über die Struktur der Datenschutzaufsicht im Bereich des öffentlichen Rundfunks sollte neu nachgedacht werden, um bestehende Ungereimtheiten zu beseitigen.

12.2 Rundfunkfinanzierung: Erneuter Meldeabgleich

Seit 2013 basiert die Finanzierung des öffentlich-rechtlichen Rundfunks auf dem Rundfunkbeitrag, einer allgemeinen Abgabe für Wohnungen, Betriebsstätten und gewerbliche Kraftfahrzeuge. Damit wird sie unabhängig von dem Besitz eines Rundfunkempfangsgerätes erhoben. Im Zuge der Umstellung haben die Meldeämter in den Jahren 2013 und 2014 rund 70 Millionen Meldedatensätze an die Rundfunkanstalten übermittelt, um einen, wie es hieß, „einmaligen Meldedatenabgleich" durchzuführen. Die Datenschutzbeauftragten des Bundes und der Länder hatten sich dagegen ausgesprochen (siehe Bericht 2011 unter 15.4). Der „einmalige" millionenfache Meldedatenabgleich soll nunmehr im Jahr 2018 erneut durchgeführt werden. Wird die Ausnahme jetzt zur Regel?

Anfragen zu diesem Verfahren zeigen: Bürgerinnen und Bürger machen sich Gedanken darüber, ob die umfangreichen Datenübermittlungen der Meldeämter an den Beitragsservice der öffentlich-rechtlichen Rundfunkanstalten rechtsstaatlich korrekt sind.

Die datenschutzrechtliche Dimension des Eingriffs ist erheblich. Auch wenn die übermittelten Datensätze nicht alle Angaben aus dem Melderegister enthalten, entsteht aus der Datenmenge dennoch ein umfassendes Bild über die Wohnverhältnisse der Gesamtbevölkerung. Während bei der Reform des Melderechts im Jahr 2015 nicht zuletzt aus Datenschutzgründen auf die Einrichtung eines bundesweiten zentralen Melderegisters verzichtet wurde, entsteht durch die Zusammenführung der dezentralen Melderegister bei den Rundfunkanstalten ein umfassendes Register bei einer Institution mit ganz anderer Aufgabenstellung.

Im Zuge der Umstellung von der Gebührenfinanzierung auf das jetzige Beitragssystem war dies zunächst als einmalige Maßnahme gedacht. Die Gerichte haben verfassungsrechtliche Bedenken gegen eine derartig umfangreiche Datenübermittlung an die Rundfunkanstalten gesehen. Gleichwohl haben sie sie als einmaligen und systemwechselbedingten Vorgang als verhältnismäßig und rechtmäßig bewertet (vgl. Bayerischer Verfassungsgerichtshof, Entscheidung vom 14. Mai 2014, Vf. 8 – VII – 12, Vf. 24 – VII – 12).

Mit der aktuellen Änderung des Rundfunkbeitragsstaatsvertrages, die am 1. Januar 2017 in Kraft getreten ist, wird „zur Sicherstellung der Aktualität des Datenbestandes" im Jahr 2018 ein erneuter kompletter Meldedatenabgleich geregelt, der nach seiner Durchführung evaluiert werden soll.

Vorausgegangen war unter anderem eine Anhörung vor der Rundfunkkommission, in der der Vertreter des Arbeitskreises Medien der Datenschutzbeauftragten des Bundes und der Länder erhebliche und grundlegende Bedenken vorbrachte, vor

allem gegen die geplante erneute Übermittlung von Meldedaten der gesamten erwachsenen Bevölkerung an die Rundfunkanstalten vorbrachte.

Zusätzlich haben wir uns vor der Unterzeichnung des Staatsvertrags gegenüber der Landesregierung für eine Streichung dieser Maßnahme eingesetzt. Wir haben deutlich gemacht, dass aus unserer Sicht die Erforderlichkeit dieser massenhaften Datenübermittlung nach der Evaluierung nicht begründet ist. Sie beinhaltet vielmehr die Weitergabe vieler nicht benötigter Informationen: So stehen den rund 70 Millionen Erwachsenen nur etwa 40 Millionen Haushalte gegenüber. Zudem besteht längst nicht in allen Haushalten eine Beitragspflicht, und die ganz überwiegende Zahl der Beitragspflichtigen ist schon erfasst. In erster Linie sind die Betroffenen ohnehin selbst zur Anzeige verpflichtet. Bei Bedarf bestehen verschiedene Nachforschungsmöglichkeiten der Rundfunkanstalten, und bei Änderungen im Meldedatenbestand sind die Meldebehörden zur Datenübermittlung befugt. Vor diesem Hintergrund war auch das für die Rundfunkanstalten erstellte Rechtsgutachten, das 2010 die Verfassungsmäßigkeit eines einmaligen Meldeabgleichs zum Ergebnis hatte, davon ausgegangen, dass künftig keine massenhafte Übermittlung mehr nötig sein würde.

Die Wiederholung des Meldedatenabgleichs, zumal innerhalb eines so kurzen Zeitraums, erscheint nach alldem weder erforderlich noch angemessen.

Begründet wird der erneute Meldedatenabgleich in 2018 damit, dass die pflichtgemäße zeitnahe Löschung der Daten der in der Wohnung mit dem Beitragsschuldner wohnenden Personen zu erheblichen Informationsverlusten beim Beitragsservice geführt habe. Deshalb ist zu erwarten, dass auch nach dem Meldedatenabgleich im Jahr 2018 das Bedürfnis nach weiteren Abgleichen geäußert werden wird.

Zur Datenschutzaufsicht beim Beitragsservice ist anzumerken, dass der Beitragsservice die Datenverarbeitung im Auftrag der Rundfunkanstalten vornimmt, und deshalb die gleichen materiellen Vorschriften – also in der Regel die Datenschutzgesetze der Länder – wie bei den Rundfunkanstalten selbst gelten. Allerdings sind die Rundfunkanstalten in den meisten Ländern, so auch in NRW, unter Berufung auf die Staatsferne des Rundfunks der Kontrolle durch die Landesbeauftragten entzogen. Dies betrifft nicht nur die Programmgestaltung und die journalistische Arbeit, sondern alle Datenverarbeitungen – auch die des Beitragsservice.

Zusammen mit den Datenschutzbeauftragten des Bundes und der anderen Länder werden wir uns auch künftig gegen eine erneute oder sogar regelmäßige Durchführung der massenhaften Datenübermittlung von den Meldebehörden an den Beitragsservice wenden.

12.3 Smart-TV

Internetfähige Smart-TV-Geräte werden immer beliebter. Die Risiken für die Privatsphäre der Nutzerinnen und Nutzer sind aber noch nicht ausgeräumt.

Die wesentlichen datenschutzrechtlichen Probleme, die bei der Nutzung von Smart-TV-Geräten bestehen, wurden im Bericht 2015 unter 4.1 dargestellt. In einer vom Bayerischen Landesamt für Datenschutzaufsicht koordinierten und organisierten gemeinsamen technischen Prüfung wurden Ende 2014 Smart-TV-Geräte maßgeblicher Hersteller untersucht. Gegenstand der Untersuchung war insbesondere, welche Datenflüsse stattfinden, wenn die Geräte mit dem Internet verbunden werden.

Auf Basis der gewonnenen Erkenntnisse haben die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich eine gemeinsame Orientierungshilfe erarbeitet und im Herbst 2015 veröffentlicht. Die Orientierungshilfe ist auf unserer Homepage www.ldi.nrw.de abrufbar. Darin werden die wesentlichen technischen Abläufe erklärt und die datenschutzrechtlichen Anforderungen sowie Empfehlungen an die verschiedenen Akteure im Bereich des Smart-TV zusammengestellt. Sie richtet sich an Gerätehersteller, Portalbetreiber, App-Anbieter und insbesondere auch an die Anbieter von Hybrid broadcast broadband TV (HbbTV). HbbTV nutzt sowohl das Rundfunksignal (Broadcasting) als auch das Breitbandinternet (Broadband), um neben der Fernsehsendung auch zahlreiche weitere Zusatzinformationen anzubieten.

Neben der Konkretisierung, welche Informationspflichten bestehen und wann die Einwilligung der Betroffenen eingeholt werden muss, liegt ein besonderer Fokus der Orientierungshilfe auf der Frage, wann Nutzungsdaten über den Rückkanal an den Anbieter eines Web-Dienstes fließen dürfen. Die Aufsichtsbehörden haben verdeutlicht, dass Diensteanbieter über das Internet erst dann Daten von Fernsehzuschauerinnen und Fernsehzuschauern erheben dürfen, wenn diese die Dienste bewusst in Anspruch nehmen wollen. Diese Inanspruchnahme zeigt sich zum Beispiel dadurch, dass die Fernsehzuschauerinnen und Fernsehzuschauer den so genannten „Red Button“ aktivieren, um die Verbindung zu einem Web-Dienst herzustellen, der über HbbTV angeboten wird. In Gesprächen mit HbbTV-Anbietern haben diese sehr massiv ihr Interesse verdeutlicht, bestimmte Nutzerdaten unabhängig davon zu erhalten, ob diese sich für die Inanspruchnahme ihres Dienstes entscheiden. Nur so könne der Dienst hinreichend spezifische Angebote bereitstellen. Demgegenüber haben die Aufsichtsbehörden verdeutlicht, dass die Bildung von Nutzungsprofilen vor dem Drücken des „Red Button“ nicht hingenommen werden kann.

Das Landgericht Frankfurt hat einer Unterlassungsklage der Verbraucherzentrale

NRW im Wesentlichen stattgegeben, die darauf abzielte, dass Smart-TV-Geräte nicht ohne die eingehende Information über die mit der Nutzung verbundenen Datenflüsse vertrieben werden dürfen (Urteil vom 10. Juni 2016, Az. 2-03 O 364/15, bei Drucklegung noch nicht rechtskräftig). Maßgeblich für das Verfahren waren Fragen des Wettbewerbsrechts, indirekt spielte das Datenschutzrecht für die Entscheidung aber eine große Rolle. Das Landgericht hat die Bedeutung der Datenschutzfragen für die Kundinnen und Kunden deutlich hervorgehoben.

Die Thematik wird von uns gegenüber den in NRW ansässigen Anbietern der Smart-TV-Dienste weiterverfolgt. Im Sinne der Durchsetzung des Datenschutzes stehen wir auch bei diesem Thema in engem Kontakt mit der Verbraucherzentrale NRW.

12.4 Google

Das Unternehmen Google bietet neben der Suchmaschine viele weitere Dienste an, meist als Marktführer. Zwar ist die Landesbeauftragte für Datenschutz NRW nicht die örtlich zuständige Aufsichtsbehörde für den Anbieter Google, dennoch haben wir den Nutzerinnen und Nutzern von Google-Diensten einige Hinweise und Ratschläge geben können.

Suchmaschine

Google hat die Website seiner Suchmaschine mit dem Ziel geändert, die Verarbeitung der personenbezogenen Daten der Nutzerinnen und Nutzer auf eine neue Rechtsgrundlage zu stellen. Nach mehrmaligem Aufruf der Seite wird derzeit deren weitere Nutzung von der Abgabe einer Einwilligungserklärung abhängig gemacht. Im Rahmen der Datenschutzbestimmungen wird man aufgefordert, der Verwendung der Nutzerdaten für andere Zwecke als die der Suchmaschine sowie der Zusammenführung der Daten verschiedener Dienste des Anbieters Google zuzustimmen. Solange keine entsprechende Einwilligungserklärung abgegeben wird, wird der Nutzungsvorgang unterbrochen.

Auch wenn eine solche Einwilligungserklärung im Hinblick auf den gesetzlichen Erlaubnistatbestand des § 15 Abs. 1 Telemediengesetz (TMG) für die Erhebung und Verwendung von Nutzungsdaten für das Angebot der Suchmaschine gar nicht erforderlich wäre, ist Google rechtlich nicht daran gehindert, für das Angebot eine Einwilligung einzuholen. Allerdings kann durch regelmäßiges Löschen der Browser-Cookies auch eine Einwilligung vermieden werden, so dass das Angebot dann weiter aufgerufen werden kann. Auf diese Weise lässt sich derzeit das von Google gewählte und von vielen als belästigend empfundene Verfahren umgehen. Wer den Browser so eingestellt hat, dass er beim Schließen alle Cookies automatisch löscht, wird die besondere Einwilligungsaufforderung noch nie gesehen haben, bekommt aber den allgemeinen Hinweis auf die Einwilligungserklärung angezeigt.

Nur am Rande sei bemerkt: Alternative Suchmaschinenanbieter machen ihre Nutzung nicht von der Abgabe einer Einwilligungserklärung abhängig und gehen mit den persönlichen Daten der Nutzerinnen und Nutzer datensparsamer um. Hierüber informieren wir auf unserer Homepage www.ldi.nrw.de.

Google Analytics

Mithilfe von Google Analytics können Betreiber von Internetseiten das Nutzungsverhalten der Besucherinnen und Besucher, etwa deren geographische Herkunft oder Verweildauer auf einzelnen Seiten, auswerten, um herauszufinden, was ihre Kundinnen und Kunden interessiert, und um dementsprechend ihr Angebot zu gestalten. In vielen Fällen konnten wir feststellen, dass die Betreiber die rechtlichen Vorgaben des TMG nicht einhalten.
Wir haben in diesen Fällen darauf hinge-

wirkt, dass die Seitenbetreiber die Rechtsverstöße abstellen. Folgende Verstöße wurden festgestellt:

- In der Datenschutzerklärung wurde nicht auf die Verwendung von Google-Analytics hingewiesen.

- Es wurde unzutreffend über die Verwendung personenbezogener Daten informiert. Beispiel: „Google führt Ihre Daten nicht mit anderen Daten zusammen". Google führt aber nach der letzten Änderung der Nutzungsbestimmungen sehr wohl die Daten verschiedener Dienste zusammen und lässt sich hierzu die Einwilligung erteilen.

- Die Datenschutzerklärung enthielt keine Hinweise, wie der Weitergabe der Daten an Google widersprochen werden kann.

- Die IP-Adresse der Besucherin oder des Besuchers der Internetseite wurde nicht vor der Weitergabe an Google gekürzt.

- Für die Weitergabe der Daten der Nutzerinnen und Nutzer in die USA beriefen sich Seitenbetreiber weiterhin auf die Grundsätze von Safe Harbor, obwohl dieses Instrument nach dem Urteil des Europäischen Gerichtshofes (EuGH) nicht mehr wirksam war. Derzeit beruft sich Google stattdessen auf die Grundsätze des EU-US Privacy Shield.

Zum EU-US Privacy Shield hat die EU-Kommission im Juli 2016 festgestellt, dass unter dessen Regelungen ein angemessenes Datenschutzniveau für Datenübermittlungen in die USA besteht (siehe hierzu unter 4.). Ob und wie sich das EU-US Privacy Shield bewährt hat, wird bei der ersten gemeinsamen jährlichen Überprüfung der Regelungen im Jahr 2017 beurteilt werden.

„Recht auf Vergessenwerden"

Mit Urteil vom 13. Mai 2014 (Az. C-131/12) hat der EuGH auf der Grundlage der Europäischen Datenschutzrichtlinie das grundsätzliche Recht von Betroffenen anerkannt, bei Suchanfragen zu ihrem Namen vom Betreiber der Suchmaschine die Löschung eines Treffers zu verlangen (siehe Bericht 2015 unter 3.4). Nach Bekanntwerden des Urteils haben sich viele Betroffene mit der Bitte an uns gewandt bestimmte Suchergebnisse zu ihren Namen löschen zu lassen. In diesen Fällen verweisen wir auf das Löschformular, das Google auf seiner Seite zur Geltendmachung seiner Rechte bereitstellt, sowie auf die Zuständigkeit der Hamburgischen Datenschutzaufsichtsbehörde, die sich aus dem Sitz der deutschen Google-Niederlassung ergibt.

Google beschäftigt die Datenschutzaufsichtsbehörden in ihrer täglichen Arbeit unabhängig von der direkten Zuständigkeit für das Unternehmen. Nutzerinnen und Nutzer beraten wir dabei zu allgemeinen Fragen. Soweit Betreiber von Internetseite aus NRW Google-Dienste eigenverantwortlich nutzen, wirken wir auf den datenschutzgerechten Einsatz hin.

12.5 Facebook

Soziale Netzwerke im Internet können Menschen verbinden und die Kommunikation über zeitliche und räumliche Grenzen hinweg vereinfachen. Auch wenn für die Nutzung kein Entgelt verlangt wird, werden sie nicht wirklich ohne Gegenleistung gewährt: Die über die Mitglieder gewonnenen Erkenntnisse werden vermarktet, um den Dienst zu finanzieren und Gewinne zu erzielen. Es liegt auf der Hand, dass hier Konflikte mit der informationellen Selbstbestimmung der Betroffenen entstehen. Facebook steht als größtes Netzwerk im besonderen Fokus der Aufsichtsbehörden.

Aufgrund der deutschen Niederlassung von Facebook in Hamburg, ist der dortige Landesbeauftragte für Datenschutz zuständige Aufsichtsbehörde. Aber auch in NRW gab es einigen Anlass, in Sachen Facebook tätig zu werden.

Unter unserer Beteiligung wurden die im Bericht 2015 unter 4.2. erwähnten Gespräche zwischen der Innenministerkonferenz (IMK) und Facebook fortgesetzt. Leider drängt sich der Eindruck auf, Facebook verschleppe die Angelegenheit. Die unpräzisen Antworten machten viele Nachfragen erforderlich und auch am Ende blieb noch vieles im Unklaren. Während der Abschlussbericht der IMK noch aussteht, hat sich zwischenzeitlich die untersuchte Praxis einschließlich der verwendeten Nutzungsbedingungen gegenüber dem Ausgangssachverhalt mehrfach geändert.

Vor diesem Hintergrund haben wir unsere bisherige Praxis fortgesetzt, öffentlichen Stellen von der Errichtung von Fanpages abzuraten (siehe Bericht 2015 unter 4.2). Öffentliche Stellen sollten ihre Vorbildfunktion wahrnehmen. Bei einer Veranstaltung der Polizeipräsidien und Kreispolizeibehörden haben wir darauf hingewiesen, wie problematisch es aus unserer Sicht ist, wenn öffentliche Stellen in die Datenverwendungspraxis bei Facebook einbezogen werden. Obwohl das Innenministerium NRW diese Möglichkeit der Kontaktaufnahme mit Bürgerinnen und Bürgern bewirbt, hat erfreulicherweise ein großer Teil der Kreispolizeibehörden sich gegen die Errichtung einer eigenen Profilseite entschieden.

Mit der Nutzung von Facebook verbunden sind auch Datenübermittlungen an den Hauptsitz des Unternehmens in die USA. Die Datenverwendung in den USA entspricht nach der Safe-Harbour-Entscheidung des Europäischen Gerichtshofes (EuGH) jedoch in verschiedenen Punkten wohl nicht dem europäischen Datenschutzstandard und die Betroffenen sind oft schutzlos gestellt. Auch mit dem neuen Privacy Shield nach dem sich Facebook Inc. bereits im September 2016 hat zertifizieren lassen, ist weiterhin fraglich, ob die Probleme ausgeräumt sind.

Einen anderen Aspekt der Facebook-Nutzung betrifft die verbreitete Einbindung von Social Plugins, den so genannten Fa-

cebook-Like-Buttons, auf Websites von Unternehmen. Plugins können beim Aufruf der Internetseite Daten an den Anbieter des Plugins übertragen.

Hier war die Verbraucherzentrale NRW aktiv. Sie hat im März 2016 ein Urteil des Landgerichts Düsseldorf (Urteil vom 9. März 2016, Az. 12 O 151/15) gegen ein nordrhein-westfälisches Unternehmen erstritten, das diesen Like-Button als iFrame auf seiner Website eingebunden hatte.

Die Einbindung als iFrame bedeutet, dass diejenigen Kundinnen und Kunden, die die Website eines Unternehmens aufrufen, damit automatisch und ohne eigenes Wissen zugleich eine Verbindung zum Server von Facebook aufbauen. So erhält der Betreiber des Plugin zugleich die Information über den Aufruf der Seite und die Möglichkeit, im Browser der Nutzerin oder des Nutzers ein Cookie zu setzen. Dadurch sind diese bei späteren Aufrufen identifizierbar. Das Landgericht hat entschieden, dass der Button nicht einfach durch einen iFrame in die Website eingebunden werden darf, weil dann bereits vor Aktivieren des Button durch die Nutzerin oder den Nutzer die Daten an Facebook fließen.

Noch während des erstinstanzlichen Verfahrens hat das betroffene Unternehmen die Einbindung des Plugins geändert. Es verwendet nun eine Zweiklicklösung, bei der das Plugin erst aktiviert wird, wenn die Nutzerin oder der Nutzer den entsprechenden Button betätigt hat. Dennoch hat das Unternehmen Berufung gegen das Urteil des Landgerichts eingelegt. Facebook stellt das Plugin bereit und ist auf Seiten des Websitebetreibers dem Streit beigetreten, da das Unternehmen ein starkes Interesse daran haben dürfte, ein rechtskräftiges Verbot der Einbindung seiner Like-Buttons als iFrame zu verhindern.

Das Oberlandesgericht (OLG) Düsseldorf hat uns im Berufungsverfahren gemäß § 12a des Unterlassungsklagegesetzes Gelegenheit zur Stellungnahme gegeben. Diese Regelung, nach der der zuständigen Aufsichtsbehörde Gelegenheit zur Äußerung eingeräumt wird, besteht seit April 2016 und bezieht sich auf Fragen der Unzulässigkeit von Datenverwendungen. In unserer Stellungnahme haben wir erläutert, dass die Einbindung des Buttons als iFrame eine unerlaubte Datenübermittlung des Websitebetreibers an Facebook darstellt.

Mit Beschluss vom 19. Januar 2017 (Az. I-20 U 40/16) hat das (OLG) Düsseldorf die entscheidungserheblichen Rechtsfragen, die die Auslegung europäischer Datenschutzvorgaben betreffen, dem EuGH vorgelegt. Dieser kann nun im Vorabentscheidungsverfahren verbindlich festlegen,

- ob das europäische Datenschutzrecht es zulässt, dass deutsche Verbraucherzentralen in Datenschutzfragen ein Verbandsklagerecht besitzen,

- wer bei Einbindung von Plugins als datenschutzrechtlich verantwortliche Stelle anzusehen ist,

- wem gegenüber etwa eine Einwilligung der betroffenen Personen zu erteilen wäre und

- welche Informationspflichten den Websitebetreiber treffen.

Erfahrungsgemäß ist eine Entscheidung des EuGH frühestens Anfang des Jahres 2018 zu erwarten.

Weiterhin raten wir verantwortlichen Stellen davon ab, soziale Netzwerke zu nutzen, die die datenschutzrechtlichen Anforderungen nicht erfüllen. Wir werden uns auch künftig dafür einsetzen, die Risiken der Nutzung zu minimieren. Unabhängig davon sollten sich Bürgerinnen und Bürger umfassend informieren und bewusst entscheiden, ob sie ein soziales Netzwerk nutzen wollen.

12.6 WhatsApp

Der Messenger-Dienst WhatsApp hat mit weltweit über einer Milliarde Nutzerinnen und Nutzern eine marktbeherrschende Stellung. Seine Nutzung ist allerdings mit Risiken für die Privatheit verbunden.

Positiv an WhatsApp ist grundsätzlich, dass die Inhalte der Kommunikation verschlüsselt werden. Die Schlüssel sind dabei in den Endgeräten der Nutzerinnen und Nutzer gespeichert (so genannte Ende-zu-Ende-Verschlüsselung). So sollen weder WhatsApp noch Dritte bei der Übertragung der Inhalte auf diese zugreifen können. Presseberichte weisen allerdings darauf hin, dass WhatsApp in der Lage sei, für einen Kommunikationspartner neue Schlüssel zu generieren und sich auf diese Weise trotz Verschlüsselung Zugriff auf Inhalte verschaffen könne. Ob ein solches Verfahren von WhatsApp tatsächlich genutzt wird, ist uns nicht bekannt.

Mit der Verschlüsselung von Inhalten ist noch keine Aussage darüber getroffen, wie WhatsApp mit Verkehrsdaten (Wer kommuniziert wann mit wem?) und Bestandsdaten (Wer ist als Nutzerin oder Nutzer des Dienstes angemeldet?) verfährt. Hier ist datenschutzrechtlich einiges zu hinterfragen.

Im August 2016 hatte sich herausgestellt, dass der Telekommunikationsdienst WhatsApp, der zum Facebook-Konzern gehört, nach einer Änderung der Nutzungsbedingungen Daten der Nutzerinnen und Nutzer an Facebook weitergeben möchte. Zwar sollte es möglich sein, der Weitergabe für Werbezwecke zu widersprechen, jedoch nur für eine bestimmte Zeit. Der Weitergabe zu anderen Zwecken konnte nicht widersprochen werden.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der für die deutsche Niederlassung von Facebook zuständig ist, hat daraufhin dem Unternehmen die Speicherung der von WhatsApp weitergegebenen Daten deutscher Nutzerinnen und Nutzer untersagt. Facebook hat hiergegen Rechtsmittel eingelegt. Die Vorsitzende der Artikel-29-Arbeitsgruppe, in der die europäischen Datenschutzbehörden zusammenarbeiten, hat WhatsApp aufgefordert, bis zur Klärung keine Daten an Facebook zu übermitteln. Facebook hat erklärt, bis zur Klärung der Rechtslage keine Daten von WhatsApp zu erheben und zu speichern.

Ein weiterer Kritikpunkt: WhatsApp liest bei der Installation Telefonnummern und weitere Datenkategorien aus, die im Adressbuch auf dem Gerät der Nutzerinnen und Nutzer gespeichert sind. Anschließend erfolgt ein Abgleich dieser Daten mit der Datenbank aller durch WhatsApp gespeicherten Bestandsdaten. Dies geschieht unabhängig davon, ob die Telefonnummern anderen WhatsApp-Nutzerinnen und -Nutzern gehören und ob diese damit einverstanden sind oder da-

von überhaupt auch nur wissen. Besonders brisant dabei ist: Für die Weitergabe dieser Daten sind die Nutzerinnen und Nutzer von WhatsApp datenschutzrechtlich verantwortlich. Über die Nutzung für rein private oder familiäre Zwecke hinaus wären, mangels einer gesetzlichen Erlaubnis für die Weitergabe der Daten, grundsätzlich die Einwilligungen aller Personen einzuholen, deren Telefonnummern im Adressbuch gespeichert sind. Wenn die Nutzerinnen und Nutzer dies nicht können, dann sollten sie bei der Installation der App zumindest darauf achten, dass der App, soweit dies technisch möglich ist, keine Zugriffsrechte auf das Adressbuch des Endgerätes eingeräumt werden. Alternativ sollten Nutzerinnen und Nutzer ein Endgerät oder ein Benutzerprofil auf ihrem Endgerät verwenden, in dessen Adressbuch außer der eigenen Telefonnummer keine weiteren vorhanden sind.

Zum Schluss sei darauf hingewiesen: WhatsApp ist nach Auffassung der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein Telekommunikationsdienst. Damit fällt es in die sachliche Zuständigkeit der Bundesbeauftragten für den Datenschutz.

Bei der Nutzung von WhatsApp bestehen viele Rechtsunsicherheiten, insbesondere was das Hochladen der Adressbuchdaten unbeteiligter Dritter an WhatsApp und die Weitergabe von Kundinnen- und Kundendaten an Facebook betrifft. Am Markt gibt es Alternativen, die ebenfalls Ende-zu-Ende-Verschlüsselung anbieten, jedoch keine Daten ihrer Nutzerinnen und Nutzer an Dritte weitergeben, und deren Programmcode frei einsehbar und auf Schwachstellen überprüfbar ist.

12.7 „Hassmails“ – Vorsicht bei Veröffentlichung

Hassmails sind schnell geschrieben, im Ton verletzend und der Inhalt oft falsch. Als Reaktion würden einige Empfänger gerne die E-Mails veröffentlichen – im Bereich der Politik oft um eine öffentliche Diskussion anzuregen, teilweise aber auch, um die Absenderin oder den Absender bloßzustellen. Doch ist eine Veröffentlichung im Internet zulässig?

Grundsätzlich dürfen personenbezogene Daten im Internet nur mit Einwilligung der oder des Betroffenen veröffentlicht werden. Das Veröffentlichen von personenbezogenen Informationen und Meinungen im Internet stellt einen besonders intensiven Eingriff in die Rechte der Betroffenen dar, weil die Daten – einmal online – nicht wieder zurückgeholt werden können. Sie können noch Jahrzehnte später weltweit abgerufen und für heute nicht absehbare Zwecke verwendet werden.

Dies gilt auch für Hassmails. Soweit eine Hassmail von der Verfasserin oder dem Verfasser noch nicht veröffentlicht wurde und die E-Mail Angaben zu dritten Personen enthält oder Rückschlüsse auf die Absenderin oder den Absender zulässt, darf sie grundsätzlich nur mit deren Einwilligung veröffentlicht werden. Für den Zweck, mit der Veröffentlichung eine politische Diskussion anzuregen, ist grundsätzlich auch keine Nennung der Verfasserin oder des Verfassers erforderlich. Wer die Absenderin oder den Absender wegen des Inhalts der E-Mail anklagen will, sollte sich an die Staatsanwaltschaft wenden statt die Mail ins Internet zu stellen. Während selbst Haftstrafen zeitlich befristet sind und selbst Eintragungen im Strafregister nach einer gewissen Frist gelöscht werden, können Eintragungen im Internet die betroffene Person lebenslänglich verfolgen – mit unvorhersehbaren Folgen für das künftige berufliche oder private Leben. Die im Strafrecht gewährte zweite Chance ist bei einer einmal im Internet veröffentlichten E-Mail weder gegeben noch sicherzustellen.

Datenschutzrechtlich unproblematisch ist es hingegen, wenn vor einer Veröffentlichung jeglicher Personenzug entfernt wird. Dies betrifft nicht nur den Namen der Absenderin oder des Absenders oder sonstiger Personen. Auch der Rückschluss auf bestimmte Personen durch weitere Informationen etwa aus dem Inhalt muss ausgeschlossen sein.

Die Veröffentlichung von Schreiben und E-Mails mit Personenbezug im Internet ist grundsätzlich unzulässig. Eine Veröffentlichung in anonymisierter Form ist dagegen möglich und wird in der Regel allen Interessen gerecht.

13. Datensicherheit

13.1 Das Standard-Datenschutzmodell

Welche technischen und organisatorischen Maßnahmen sind erforderlich, um die datenschutzrechtlichen Anforderungen zu erfüllen? Diese Frage stellen sich viele Unternehmen, Behörden und sonstige verantwortliche Stellen – aber auch die Aufsichtsbehörden, die diese Stellen beraten und kontrollieren. Mit dem Standard-Datenschutzmodell (SDM) wollen die Datenschutzaufsichtsbehörden nun eine einheitliche Prüfmethode entwickeln und etablieren, die es erlaubt, die Frage systematisch und nachvollziehbar zu beantworten.

Das SDM soll einen praktikablen Weg eröffnen, rechtliche Vorgaben des geltenden Datenschutzrechts und zukünftig auch der DS-GVO in angemessene technische und organisatorische Maßnahmen umzusetzen. Dazu wurden zunächst die datenschutzrechtlichen Anforderungen verschiedener Datenschutzgesetze in einen einheitlichen Katalog elementarer Schutzziele (Gewährleistungsziele) überführt. Das sind zum einen die klassischen Schutzziele der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit. Diese werden ergänzt um die speziell datenschutzbezogenen Anforderungen Datenminimierung, Transparenz, Intervenierbarkeit und Nichtverkettung. Nichtverkettung bezeichnet die Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben wurden.

Im Rahmen einer Prüfung wird der Schutzbedarf der verarbeiteten Daten hinsichtlich der Gewährleistung dieser Ziele ermittelt. Maßstab dafür ist die Eingriffsintensität der Datenverarbeitung aus Sicht der einzelnen Betroffenen. Aus der Analyse des Schutzbedarfs folgt dann, welche standardisierten Schutzmaßnahmen erforderlich sind. Die insoweit als erforderlich erkannten technischen oder organisatorischen Sicherungsmaßnahmen lassen sich einem standardisierten Maßnahmenkatalog entnehmen, der als Anhang zum SDM konzipiert ist. In einer abschließenden Risikoanalyse werden eventuell noch darüber hinaus gehende Sicherungsbedarfe ermittelt.

Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) hat im November 2016 das Handbuch mit der allgemeinen Prüfsystematik des SDM in einer Erprobungsfassung veröffentlicht. Der Katalog mit den konkreten, standardisierten Schutzmaßnahmen wird derzeit vom Arbeitskreis Technik (AK Technik), einem Arbeitsgremium der DSK, entwickelt. Das SDM soll sowohl in der Kontroll- und Beratungspraxis der Datenschutzaufsichtsbehörden als auch bei der Planung und beim Betrieb von Datenverarbeitungen durch verantwortli-

che Stellen im öffentlichen und nicht-öffentlichen Bereich erprobt werden. Es wird vom AK Technik laufend fortentwickelt.

Das Modell soll zu einer einheitlichen und transparenten Prüfpraxis der Datenschutzaufsichtsbehörden beitragen. Gleichzeitig will es verantwortliche Stellen in die Lage versetzen, aus rechtlichen Anforderungen systematisch die erforderlichen Schutzmaßnahmen abzuleiten. Gelingt dies, dürfte das Modell vor dem Hintergrund der DS-GVO auch über die Grenzen Deutschlands hinweg Anwendung finden.

13.2 Anonymität in Zeiten von Big Data

Wir hinterlassen immer mehr digitale Spuren – nicht nur im Internet. Gleichzeitig werden Werkzeuge und Techniken zur Auswertung von Daten in Computersystemen effizienter. Die Verknüpfung personenbeziehbarer Datenspuren zu Persönlichkeitsprofilen birgt Risiken für die Privatheit. Deshalb gilt es, wirksame Methoden zu etablieren, die eine unzulässige Gewinnung personenbeziehbarer Daten verhindern oder zumindest erheblich erschweren.

Wir hinterlassen Daten beim Online Banking, bei Online-Einkäufen oder in sozialen Netzwerken. Aber auch als Standortdaten von Smartphones, etwa in Form von Vitaldaten durch Apps, in Webprotokollen beim Surfen und in vielen anderen Zusammenhängen. Je mehr Daten wir hinterlassen, desto größer ist die Gefahr, dass Persönlichkeitsprofile erstellt werden, die undifferenziert und sogar unrichtig sein können. Verhaltensweisen werden prognostizierbar. Prognosen, ob zutreffend oder nicht, beeinflussen und beeinträchtigen die künftigen Handlungsmöglichkeiten der Betroffenen. Außerdem kann Big Data mit seinen Möglichkeiten zur Verknüpfung und Analyse riesiger Datenmengen den Alptraum des gläsernen Menschen, der Totalüberwachung, ja der „smarten Diktatur“ wahr werden lassen.

Big Data ist jedoch nicht insgesamt zu verdammen. Das sinnvolle Potential liegt auf der Hand: In der Wirtschaft für bessere Vorhersagen von Konjunkturzyklen und Veränderungen in Märkten für Produktentwicklungen und Marketingstrategien. In der Medizin können auf der Grundlage von bereits vorliegenden Daten zu erfolgreichen Behandlungen Hilfestellungen für Therapien erfolgen. Ziel muss es deshalb sein, Wege aufzuzeigen Big Data unter Wahrung der Privatheit der betroffenen Personen nutzbar zu machen. Dabei gilt es zu berücksichtigen: Die Verknüpfung von personenbezogenen Daten, die aus unterschiedlichen Anwendungszusammenhängen stammen, sowie die Analyse personenbezogener Daten mit Analysemethoden des Big Data sind grundsätzlich unzulässig. Ein Ausweg aus den durch die Datenschutzregelungen definierten engen Grenzen wird in der Anonymisierung gesehen. Denn anonymisierte Daten sind keine personenbezogenen Daten mehr und unterliegen damit nicht den Datenschutzgesetzen. Der Weg dorthin ist jedoch mit Fallstricken versehen. Einige wenige charakteristische Merkmale einer Person reichen oft schon aus, um diese zu bestimmen. Sind etwa Geburtsdatum, Geschlecht und Postleitzahl bekannt, reichen diese Daten aus, um 87% der US-amerikanischen Bevölkerung zu identifizieren, so eine Studie von L. Sweeney der Carnegie Mellon University. Das Erstaunliche ist, dass es sich um drei nicht personenspezifische Merkmale handelt, die für sich genommen also keine Identifikation erlauben. Durch die Verknüpfung mit korrelierendem Wissen wird jedoch eine Persone-

nidentifikation möglich. Solche Merkmale werden als Quasi-Identifikatoren bezeichnet. Das korrelierende Wissen entsteht durch eine Zusammenführung von Daten aus unterschiedlichen Anwendungszusammenhängen. Die zur Verfügung stehenden Analysemethoden ermöglichen dann die Identifikation von Personen.

Vor diesem Hintergrund stellt sich die Frage: Wie können personenbezogene Daten anonymisiert werden?

Nicht mehr ausreichend ist es, die direkt identifizierenden Daten in einem Datensatz zu einer Person zu löschen (Name, Vorname, Wohnanschrift). Zusätzlich sind die Daten zu betrachten, die indirekt, also durch Analyse von Zusatzwissen, zu einer Identifikation einer Person führen können. Hierzu hat die Wissenschaft verschiedene Methoden entwickelt.

k-Anonymität

Die wichtigste Methode ist die so genannte k-Anonymität. Der k-Anonymität liegt die Idee zu Grunde, die zu den Quasi-Identifikatoren gehörenden Daten zu Gruppen mit gleichem Informationsgehalt zusammenzufassen. Damit sind die hinter den Daten stehenden Individuen nicht mehr unterscheidbar und ein Verknüpfen mit korrelierendem Wissen ist nicht mehr eindeutig möglich. Anonymität gewährleistet damit die Gruppe. Je größer die Gruppe, desto größer ist das Maß an Anonymität. Mit der Größe der Gruppe sinkt die Wahrscheinlichkeit einen konkreten Angehörigen einer Gruppe mit bestimmten Merkmalen zu identifizieren.

Daraus folgt: Anonymität ist eine mit Wahrscheinlichkeiten behaftete Größe. Der Parameter k definiert bei der k-Anonymität die Mindestgröße der Gruppen. Er ist damit gleichzeitig das Maß der Anonymität. In einer Gruppe von k Individuen liegt die Wahrscheinlichkeit bei 1/k ein einzelnes Individuum korrekt zu identifizieren. Also beispielsweise liegt die Trefferquote in einer Gruppe mit 100 Individuen bei 1 Prozent.

Es gibt verschiedene Ansätze, um k-Anonymität zu erreichen:

1. Dummy-Datensätze hinzufügen

2. Unterdrücken von Informationen durch Löschen

3. Vertauschen von Daten

4. Verallgemeinern von Daten.

Die an dem Thema Anonymisierung interessierten Leserinnen und Leser möchten wir auf die Langfassung dieses Beitrags auf unserer Homepage www.ldi.nrw.de hinweisen, mit weiteren Informationen zu den rechtlichen Aspekten sowie eine detailliertere Beschreibung weiterer Methoden zur Anonymisierung, wie etwa die l-Diversität und der t-Closeness. Die Methoden erläutern wir anhand eines konkreten Beispiels mit personenbezogenen Datensätzen.

In Zeiten von Big Data ist Anonymisierung entscheidend für die Wahrung der Privatheit. Die Schwierigkeit besteht allerdings in dem Spagat ein akzeptables Anonymitätsmaß zu erreichen und gleichzeitig einen Informationsgehalt zu wahren, der noch verwertbare Analyseergebnisse zulässt.

13.3 Zu Risiken und Nebenwirkungen des Internet der Dinge

Das Internet der Dinge, englisch: Internet of Things (IoT), hält inzwischen auch Einzug in Haushalte. Zunehmend sind die unterschiedlichsten Dinge mit dem Internet verbunden. Dies bleibt nicht ohne Auswirkungen auf den Datenschutz.

Im Heimbereich ist der Trend zur Vernetzung bei Fernsehern am offensichtlichsten: Nahezu alle aktuellen Fernseher können Videos aus Online-Videotheken wiedergeben. Kühlschränke sind mit eingebauter Webcam im Innenraum lieferbar, Waschmaschinen melden über eine App, dass die Wäsche fertig ist. Heizung und Beleuchtung lassen sich über das Internet steuern („Smart Home"). Vernetzte Zähler, so genannte Smart Meter, vor allem für den Stromverbrauch sind bereits verbreitet. Ihr Einsatz wird sich aufgrund gesetzlicher Regelungen in den nächsten Jahren beschleunigen. Personenwaagen, Blutdruckmessgeräte oder auch so genannte Wearables messen konstant die körperliche Aktivität und den Puls. Die Messwerte können über einen beliebigen Zeitraum über eine App oder in der Cloud ausgewertet werden. In zunehmendem Maße breitet sich das Internet der Dinge auch im Kinderzimmer aus. Schon seit einigen Jahren lassen internetfähige Spielkonsolen weltweite Spielergemeinschaften entstehen. Inzwischen werden jedoch nicht mehr nur elektronische Spielzeuge wie ferngesteuerte Autos oder Modelleisenbahnen vernetzt. Auch traditionelle Spielzeuge gehen schon ins Netz. Die „Happy Barbie" überträgt Tonaufnahmen in die Cloud, und kann dann ein „Gespräch" führen. Eltern können sich anschließend die aufgenommen Audiosequenzen zuschicken lassen.

Der Trend zur Vernetzung endet nicht an der Haustür. Moderne Pkw sind über das Mobilfunknetz mit dem Internet verbunden und übermitteln Diagnosedaten an den Hersteller. Haben Sie Ihren Autoschlüssel verloren? Kein Problem. Fahrzeuge lassen sich inzwischen auch ferngesteuert öffnen. Messstationen an Ampeln, an Autobahnbrücken und in Parkhäusern erfassen den Verkehr. Die Verkehrssituation oder freie Parkplätze sind in Echtzeit über das Internet abrufbar. Paketdienste verfolgen die transportierten Pakete, so dass sich Kundinnen und Kunden über den Standort informieren können.

Auch außerhalb des privaten Umfelds kommen vernetzte Geräte zum Einsatz. Das Spektrum reicht hier von Steuerungen für Kirchturmglocken bis zu zentralen Steuersystemen von (Atom-)Kraftwerken.

Viele der genannten Dinge verarbeiten höchst sensible und persönliche Daten, die detaillierte Rückschlüsse auf die Vorlieben einer Person erlauben. Die so gesammelten Daten haben eine neue Qualität: Bisher beschränkte sich das Sammeln von Daten vornehmlich auf statische Daten wie Namen oder Geburtstag, die die Nutzerinnen und Nutzer mehr oder weni-

ger bewusst preisgeben. Smart Devices hören permanent mit und reagieren auf ein Schlüsselwort. Die Assistenten werten dazu teilweise auch weitere Daten wie das E-Mail-Postfach aus. Drittanbieter-Apps können einige der Assistenten erweitern – zum Beispiel, indem eine Cocktail-App die benötigten Zutaten auf den virtuellen Einkaufszettel setzt. In der Folge geben Nutzerinnen und Nutzer etwa Vorlieben preis, ohne sich darüber bewusst zu sein – oder sogar ohne die Vorliebe bei sich selbst wahrgenommen zu haben.

Die Anbieterinnen und Anbieter archivieren Sprachaufnahmen und die aus ihnen (automatisch) erzeugten Transskripte häufig über einen langen Zeitraum und erstellen detaillierte Nutzerprofile. Darüber hinaus kann aus den Sprachaufnahmen ein biometrischer Fingerabdruck erstellt werden. Die Identifikation ist potentiell auch dann möglich, wenn Dritte den Assistenten nutzen. Das Ausschalten des Smartphones garantiert dann keine Anonymität mehr.

Die bei der Nutzung von Bewegungstrackern oder Fitnessarmbändern anfallenden Daten lassen nicht nur nachvollziehen, wo sich eine Person zu einer gegebenen Zeit aufhielt. Mit relativ hoher Wahrscheinlichkeit lässt sich über das Aktivitätsmuster sogar feststellen, was sie zu dieser Zeit getan hat. Diese Muster können nicht nur für personalisierte Werbung verwendet werden. Zudem sind (vermeintliche) Diskrepanzen zwischen den aufgezeichneten Aktivitäten und versandten Nachrichten feststellbar. Im Internet der Dinge sind zur Gewährleistung des Datenschutzes daher sowohl die IT-Sicherheit als Basisvoraussetzung als auch die Datenverarbeitung im Hinblick auf das Datenschutzrecht zu betrachten.

IT-Sicherheit im Internet der Dinge

Viele Geräte für das Internet der Dinge weisen teilweise erhebliche Sicherheitsmängel auf. Diese Mängel sind meistens Anfängerfehler und wären vermeidbar, wenn Hersteller die IT-Sicherheit ernster nähmen. Die Kundschaft ist sich der datenschutzrechtlichen Nebenwirkungen eines unsicheren Gerätes jedoch in der Regel nicht bewusst oder kann die Konsequenzen nicht abschätzen. In der Folge ist für sie „IT-Sicherheit“ kein Merkmal, das für die Kaufentscheidung relevant ist und einen Mehrpreis rechtfertigt.

IT-Sicherheit wird deshalb von Herstellern primär als Kostenfaktor wahrgenommen. Um die erforderliche Entwicklungszeit zu verkürzen und billigere Hardware verbauen zu können, wird sowohl an der Qualifikation der Mitarbeiterinnen und Mitarbeiter gespart als auch die IT-Sicherheit bewusst niedriger implementiert als technisch möglich. Zudem stellen sie häufig nach kurzer Zeit keine Updates mehr für die Geräte zur Verfügung. Bekannte Sicherheitslücken werden damit nicht mehr behoben.

Für Hersteller hat die Vernachlässigung der IT-Sicherheit in der Regel keine negativen Konsequenzen. Teilweise ist schon

vom „Internet of unpatchable things“, also dem Internet der Dinge mit nicht behebbaren Fehlern, die Rede. Zudem berücksichtigen auch Anwenderinnen und Anwender die IT-Sicherheit der Geräte bei der Inbetriebnahme regelmäßig nicht ausreichend.

In letzter Zeit wurden mehrere Fälle bekannt, in denen Unbefugte auf vernetzte Systeme im Internet zugreifen konnten. In einigen Fällen war den Betreiberinnen und Betreibern nicht bewusst, dass die Geräte standardmäßig aus dem Internet erreichbar sind. Dies ist insbesondere in Verbindung mit nicht geänderten Standardpasswörtern fatal. Zudem wiesen die Geräte vielfach gravierende Sicherheitslücken auf. Teilweise versäumten Nutzerinnen und Nutzer, Updates einzuspielen. Teilweise bot aber auch der Hersteller keine Updates an, um die Lücke zu schließen.

Das ungeplante Läuten von Kirchturmglocken mag noch amüsant klingen. Nicht mehr lustig sind Alarmanlagen, die sich über das Internet deaktivieren lassen und detaillierte Informationen über die Hausbewohner preisgeben. Todernst wird das unbefugte Umprogrammieren von Baustellenampeln oder die Übernahme der Kontrolle über Kraftwerke. Solche Lücken wurden von der Sicherheitsforschung aber auch von Journalistinnen und Journalisten aufgedeckt und konnten so geschlossen werden, ohne dass es zum Eintritt eines Schadens kam. Angriffe von Kriminellen mit entsprechenden Motiven hätten jedoch zu gravierenden Schäden führen können. Gekaperte Systeme stellen zwar nicht zwangsläufig eine unmittelbare Gefahr dar, sind aber ein Sprungbrett ins interne Netz. In der Regel finden sich hier interessantere Ziele, die aus dem Internet ohne derartige Umwege nicht erreichbar wären.

Datenverarbeitung im Internet der Dinge

Die Prüfung der IT-Sicherheit konzentriert sich darauf, ob die IT- Systeme über die vorgesehenen Schnittstellen hinaus zugänglich sind. Zur Beurteilung des Datenschutzes ist darüber hinaus in den Blick zu nehmen, welche Daten die Geräte im Einzelnen erheben und was mit ihnen geschieht. Hier zeigt sich deutlich, dass Daten „auf Vorrat“ erhoben werden – das heißt ohne einen konkreten und aktuellen Bedarf.

Nutzerinnen und Nutzer bleiben nur dann Herren ihrer Daten, wenn diese ausschließlich in ihrem Einflussbereich bleiben. Eine ausschließliche Nutzung der Daten auf den Geräten ist jedoch oftmals bereits aufgrund des technischen Designs der Hersteller ausgeschlossen. Regelmäßig ist die Einbindung eines Gerätes in die Cloud obligatorisch, lokale Schnittstellen fehlen. Teilweise sind vom Hersteller beworbene Funktionalitäten nur über einen Cloud-Dienst nutzbar, ohne dass eine technische Notwendigkeit ersichtlich ist.

Und diese Entwicklung geht noch weiter: Bislang sind die Geräte auf einen Internetzugang angewiesen, um mit den Herstellern in Kontakt zu treten. Dadurch besteht

ein Mindestmaß an Kontrolle über den Datenaustausch. Zukünftige Generationen „smarter“ Dinge könnten jedoch unmittelbar mit ihrem Hersteller in Kontakt treten. Für das IoT werden bereits Funkstandards entwickelt, die eine Reichweite von mehreren Kilometern und eine kostengünstige Kommunikation erlauben. Den Nutzerinnen und Nutzer wird damit jede Interventionsmöglichkeit genommen. In Deutschland und der Schweiz existieren bereits derartige Prototypen.

Die damit aufgeworfenen Fragen betreffen, zentrale Elemente der DS-GVO:

Die DS-GVO verpflichtet Hersteller dazu, angemessene Maßnahmen zu treffen, um die Einhaltung der Datenschutzgrundsätze sicherzustellen. Zum einen gehört hierzu, bei der Produktentwicklung auch die IT-Sicherheit zu berücksichtigen und notfalls zeitnah Updates bereitzustellen, um Vorfälle wie die oben beschriebenen zu vermeiden. Zum anderen gehört hierzu aber auch, Daten wo immer möglich nur in anonymisierter oder pseudonymisierter Form zu verarbeiten. Die Daten sind zu löschen, sobald sie für den Zweck, zu dem sie erhoben wurden, nicht mehr benötigt werden. Dies wird als „Datenschutz durch Technikgestaltung“ bezeichnet.

Des Weiteren fordert die DS-GVO „datenschutzfreundliche Voreinstellungen“. Im Auslieferungszustand ist die Verarbeitung personenbezogener Daten daher auf das erforderliche Minimum zu beschränken.

Insgesamt betrachtet lässt sich feststellen, dass viele Produkte in beiden Bereichen erhebliche Defizite aufweisen: Weder Datenschutz durch Technikgestaltung noch datenschutzfreundliche Voreinstellungen werden ausreichend berücksichtigt. Hier müssen die Hersteller also dringend umdenken und nachbessern, um die Anforderungen der DS-GVO zu erfüllen.

Der Datenschutz wird im Internet der Dinge meist unzureichend berücksichtigt. Die Hersteller sind daher – auch im Hinblick auf die DS-GVO – gefordert, ihre Angebote auf Konformität mit dem Datenschutzrecht zu überprüfen und entsprechend anzupassen.

13.4 Ransomware – Die Grenzen der IT-Sicherheit?

Im Jahr 2016 hat Ransomware in Form von Verschlüsselungs-Trojanern die IT-Sicherheitslage dramatisch verschärft. Ein prominenter Vertreter dieser Gattung ist der Trojaner Locky. Infektionen durch Locky trafen mehr als 120 Länder. Auch in NRW hatten Privatpersonen, Unternehmen, Behörden und Krankenhäuser zum Teil erhebliche Schäden zu verzeichnen. In einzelnen Fällen war die gesamte IT über mehrere Tage lahmgelegt. Ein Krankenhaus in NRW musste Notfälle an andere Krankenhäuser verweisen und geplante Operationen verschieben. Die klassischen Sicherheitsmechanismen wie Firewalls und Antivirenprogramme haben versagt.

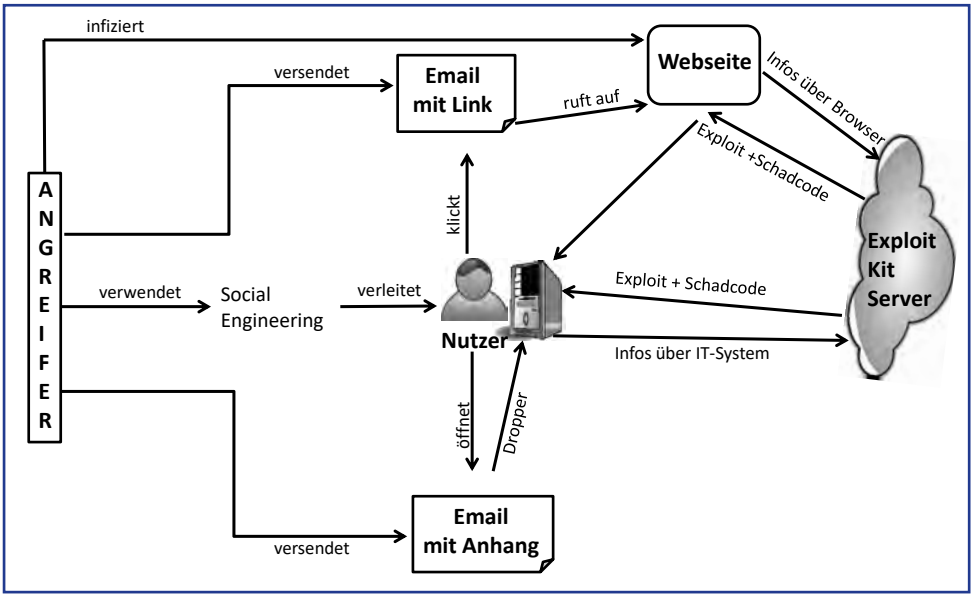
Schon seit längerem ist eine zunehmende Professionalisierung der Cyber-Kriminalität festzustellen. Hinter Angriffen auf IT-Infrastrukturen stehen nicht mehr Einzelpersonen, sondern vermehrt kriminelle Organisationen. Diese sind gut organisiert und verfügen über das fachliche Wissen sowie die entsprechenden Mittel. Die Angriffe verlaufen in kurzen Wellen, sodass die Hersteller von Antivirensoftware nur hinterherlaufen können. Ist ein Schadprogramm von ihnen erkannt, erstellen und verteilen sie Updates an ihre Kunden. Zwischenzeitlich läuft jedoch bereits ein neuer Angriff mit veränderten Merkmalen des Schadprogramms. Die Erkennung durch die „neue“ Antivirensoftware läuft damit schon wieder ins Leere. Zudem gibt es im Internet die Möglichkeit, ein Schadprogramm auf „Marktreife“ zu testen. So stellen Anbieter alle gängigen Antivirenprodukte zur Prüfung potentieller Schadsoftware zur Verfügung. Diese Dienste nehmen auch Kriminelle in Anspruch, um sicher zu gehen, dass ihre Schadsoftware nicht zu erkennen ist.

Ransomware sind Schadprogramme, die Daten „in Geiselhaft nehmen“. Ihre Bezeichnung setzt sich zusammen aus „ransom“ (englisch für Lösegeld) und „ware“, entsprechend etwa Software oder Malware. Ist das Programm in die IT-Infrastruktur eingedrungen, verschlüsselt es die Daten und erwirkt eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems. Für die Entschlüsselung oder Freigabe wird ein „Lösegeld“ verlangt.

Die Verbreitung von Ransomware in Form von Verschlüsselungs-Trojanern erfolgt in der überwiegenden Zahl der Fälle per E-Mail. Eine solche E-Mail enthält einen Anhang mit Schadcode oder einen Link, der auf eine kompromittierte Website im Internet verweist. Beim Öffnen des Anhangs oder des Links aktiviert sich der Trojaner auf dem IT-System und die Daten werden verschlüsselt. Im Anschluss wird der Zielperson ein Fenster eingeblendet, in dem ihr mitgeteilt wird, dass sie eine Entschlüsselungssoftware herunterladen kann. Dies ist allerdings erst nach Überweisung einer bestimmten Anzahl von Bitcoins möglich. Der gesamte durchzuführende Ablauf wird in diesem Fenster detailliert beschrieben.

Die Verschlüsselung mit Locky ist so sicher, dass ohne das Entschlüsselungstool eine Datenwiederherstellung nicht mehr möglich ist. Für andere Varianten von Verschlüsselungstrojanern wurden Möglichkeiten gefunden, die Daten ohne die Zahlung von Lösegeld zu entschlüsseln.

Die folgende Abbildung stellt einen typischen Ablauf eines Angriffs mit Schadsoftware dar:



Der Angreifer oder die Angreiferin versendet E-Mails mit einem Link (oberer Teil der Abbildung) oder einem Anhang (unterer Teil der Abbildung). Das Ziel besteht darin, die Zielperson zu verleiten, den Link anzuklicken bzw. den Anhang zu öffnen. Immer häufiger ist dabei zu beobachten, dass hierfür nicht willkürliche oder als solche leicht erkennbare Spam-Mails versendet werden. Inzwischen sind die E-Mails auf die Zielperson zugeschnitten und damit scheinbar vertrauenswürdig. Dazu beschafft sich die Angreiferin oder der Angreifer beispielsweise mittels Social Engineering im Vorfeld Informationen aus dem persönlichen Umfeld der potentiellen Zielpersonen.

Variante 1: E-Mail mit Link

Die Zielperson erhält eine E-Mail mit einem Inhalt, der ihr glaubwürdig erscheint und sie verleitet den enthaltenen Link anzuklicken. Anschließend ruft der Browser die entsprechende Seite im Internet auf und führt diese aus. Diese Internetseite ist allerdings infiziert. Entweder haben die Angreifenden selbst diese Seite erstellt oder es ist eine von ihnen kompromittierte Seite auf dem Webserver einer unbeteilig-

ten Person. Die Infektion besteht in einem Programm, das die Softwarekonstellation des Browsers ermittelt, mit der die Internetseite aufgerufen wurde. Dazu prüft das Programm beispielweise die Version des Betriebssystems, die Version des Browsers selbst und welche Plugins installiert sind. Diese Informationen sendet das Programm anschließend an einen so genannten Exploit-Kit Server zur Auswertung.

Der Exploit-Kit Server ist der Werkzeugkasten der Angreifenden oder der Angreiferin. Er enthält Informationen über alle gängigen mit Schwachstellen behafteten Softwareprodukte. Gleichzeitig sind auf ihm die entsprechenden Programme (Exploits) hinterlegt, welche die jeweiligen Schwachstellen ausnutzen, um den Schadcode auf dem Zielsystem zu installieren. Der Schadcode ist ebenfalls auf dem Exploit-Kit Server gespeichert. Den Exploit-Kit Server brauchen die Angreifenden nicht einmal selbst zu betreiben, sondern sie können auf einen „Dienstleister" zurückgreifen. Solche Dienstleister betreiben komplette Infrastrukturen, die sich geschützt in einem DarkNet befinden. Üblicherweise wird hierfür auf das Tor-Netzwerk zurückgegriffen. In diesem Netzwerk ist es kaum nachvollziehbar, wer mit wem kommuniziert. Insofern ist es auch für Ermittlungsbehörden schwierig bis unmöglich die Kriminellen zu enttarnen.

Der Exploit-Kit Server prüft nun anhand der von der infizierten Website eingehenden Informationen, ob für die jeweilige Browserkonstellation eine Schwachstelle vorliegt. Ist dies der Fall, wird der zugehörige Exploit mit dem einzuschleusenden Schadcode über die kompromittierte Website auf das IT-System heruntergeladen. Der Exploit nutzt dann die erkannte Schwachstelle, um das Schadprogramm, beispielsweise den Verschlüsselungs-Trojaner Locky, auf dem IT-System zu installieren. Für die Zielperson ist diese Aktion unsichtbar. Das reine Aufrufen einer kompromittierten Website reicht, um die Infektion mit einem Schadprogramm zu starten (Drive-by-Download).

Aber nicht nur Links in E-Mails locken auf kompromittierte Websites. Auch Werbung wird dafür genutzt. Angepasst auf die individuellen Interessen der Zielpersonen, wird diese auf diversen Internetseiten eingeblendet. Klickt man auf eine solche Werbeeinblendung erfolgt eine Weiterleitung auf die kompromittierte Internetseite. Die Kriminellen, die solche Aktionen starten, bezahlen sogar bei den jeweiligen Anbietern für diese Werbeeinblendungen.

Variante 2: E-Mail mit Anhang

In dieser Variante wird die Zielperson verleitet den Anhang einer E-Mail zu öffnen. In dem Anhang verbirgt sich ein so genannter Dropper. Dies ist ein Programm, das Informationen über Softwarekonstellationen des IT-Systems ermittelt, diese an den Exploit-Kit Server überträgt und anschließend den passenden Exploit für die ermittelten Schwachstellen mit dem zugehörigen Schadprogramm nachlädt. Die Anhänge können Zip-Dateien mit JavaScript, HTML-Applikationen, Windows

Script Dateien oder Office Dokumente mit VBA-Makros sein.

Was lernt man daraus?

1. Die größten Einfallstore für die Verbreitung von Schadsoftware sind der E-Mail-Dienst und der WWW-Dienst des Internets.

2. Das Einschleusen erfolgt über die Endgeräte wie Computer oder Smartphone.

3. In den meisten Fällen ist eine Mitwirkung der Zielpersonen erforderlich.

Welche Maßnahmen können getroffen werden?

1. Bei den Zielpersonen, den Nutzerinnen und Nutzern von Informationstechnik, ein Bewusstsein schaffen und sie entsprechend schulen.

2. Regelmäßige Datensicherungen durchführen und diese vom gesicherten System trennen.

3. Das IT-System durch Installation von Updates immer auf aktuellem Stand halten.

4. Potentiell gefährliche E-Mail-Anhänge blocken.

5. Die Ausführung von Makros in Microsoft Office abschalten.

6. Das Nachladen der Exploits mit den Schadprogrammen verhindern.

7. Antivirensoftware und Spamfilter auf dem neuesten Stand halten.

Ist damit das Problem gelöst?

Mit diesen Maßnahmen wird das Risiko einer Infektion durch die jetzige Generation der Verschlüsselungs-Trojaner reduziert. Das grundlegende Problem der sich verschärfenden Sicherheitslage durch immer professionellere Angriffe von Hackern, Cyber-Kriminellen und auch staatlichen Organisationen ist damit jedoch nicht behoben. Neue Angriffsvarianten werden wiederum neue, angepasste Sicherheitsmaßnahmen erfordern. Das Hase-und-Igel-Spiel geht also weiter.

Festzuhalten ist: Die bisher primär verfolgte Strategie der Erkennung von potentiell schädlichen Prozessen durch Firewalls, Intrusion-Prevention-Systeme und Virenschutzprogramme stößt an ihre Grenzen. Unterschiedliche Stimmen gibt es zu der Frage, welche Folgerungen aus dieser Erkenntnis zu ziehen sind.

Einige vertreten die Auffassung, dass wir vor einem Paradigmenwechsel stehen. Dieser bestehe darin, dass wir uns nicht mehr darauf fokussieren sollten, alle Angriffe abzuwehren. Vielmehr müssten wir uns damit abfinden, dass Schäden eintreten und wir müssten lernen, mit diesen Schäden umzugehen.

Andere fordern, die Verbindung zum Internet zu kappen und einen Rückzug in lokale Netze. Die Regierung von Singapur wird Medienberichten zufolge alle Regierungs-

computer im Mai 2017 vom Internet abkoppeln, um die von der öffentlichen Hand verwalteten Daten zu schützen.

Nach unserer Meinung sind beide Positionen als Kapitulation der IT-Sicherheit zu betrachten. In einer Gesellschaft, die mittlerweile so zentral von funktionierenden IT-Infrastrukturen abhängig ist, können Schäden ein nicht kalkulierbares Ausmaß annehmen. Ein großflächiger Ausfall der Strom- oder Wasserversorgung über mehrere Tage, hätte katastrophale Folgen. Andererseits sind in global agierenden Gesellschaften weltumspannende Kommunikationsnetze wie das Internet unverzichtbar. Sowohl das Abfinden mit Schäden, wie auch der totale Rückzug in rein lokale Netze sind aus unserer Sicht nicht die richtigen Antworten.

Überlegungen zur Problemlösung

Moderne japanische Hochhäuser sind nicht auf einem starren Fundament errichtet, sondern flexibel auf einer Gummischicht oder einer Art Stoßdämpfer gelagert. Bei einem Erdbeben schwankt dadurch die Hauskonstruktion, stürzt aber nicht ein. Die Japaner haben nicht an der herkömmlichen Art zu Bauen festgehalten, sondern neue Architekturen entwickelt, um den Herausforderungen durch Erdbeben zu begegnen.

Aus unserer Sicht sind auch im Bereich IT-Sicherheit neue Architekturansätze erforderlich, um die zukünftigen „Erdbebenwellen aus dem Internet“ abzufedern. Wenn die konventionellen Sicherheitsmechanismen keinen hinreichenden Schutz mehr bieten, müssen wir auch IT-Sicherheit neu denken.

Die größten Einfallstore für Schadprogramme sind die Dienste des Internets, wie E-Mail und WWW-Dienste. Gelingt es, diese von der internen Datenverarbeitung fernzuhalten, können die Angriffswellen nicht auf die zu schützenden Daten und Prozesse durchschlagen. Die Virtualisierungstechnologie bietet hierfür die Möglichkeit, indem die potentiell gefährlichen Dienste und Prozesse in einer virtuellen Maschine auf den Endgeräten gekapselt werden. Angriffe schädigen dann nur die virtuelle Maschine, schlagen aber nicht auf die interne Datenverarbeitung durch. Die Virtualisierungstechnologie kennt verschiedene Ausprägungen einer Kapselung. Beispielweise können die mit den kritischen Internetdiensten verbundenen Anwendungen (Browser und E-Mail-Client) auf der Grundlage einer Systemvirtualisierung in einer eigenen virtuellen Maschine ausgeführt werden. Diese virtuelle Maschine enthält ein eigenes Betriebssystem, auf dem diese Anwendungen installiert werden. Die virtuelle Maschine selbst läuft in einem Fenster auf dem nativen Betriebssystem, welches die Hardware steuert. Aus Sicht des nativen Betriebssystems stellt sich die virtuelle Maschine wie eine normale Anwendung dar. Die Prozesse, die in der virtuellen Maschine laufen, haben aber keinen Zugriff auf die Ressourcen des nativen Betriebssystems und damit keinen Zugriff auf die internen Datenverarbeitungsprozesse und deren

Daten. Somit können Angriffe zwar die virtuelle Maschine schädigen, aber nicht die interne Datenverarbeitung. Die virtuelle Maschine ist der „Stoßdämpfer“ zwischen den vom Internet ausgehenden Gefährdungen und den zu schützenden Objekten.

Bei den virtuellen Maschinen handelt es sich um rein softwarebasierte Lösungen. Wegen ihrer hohen Komplexität haben sie einen hohen Ressourcenverbrauch und benötigen leistungsfähige Computer.

Eine Alternative besteht in der Micro-Virtualisierung. Auch bei dieser Form der Virtualisierung wird der potentielle Schadcode gekapselt in einer virtuellen Umgebung ausgeführt. Der Unterschied besteht allerdings darin, dass die Micro-Virtualisierung im Prozessor und damit in der Hardware stattfindet. Damit ist es möglich, einzelne Prozesse in einer micro-virtuellen Maschine ablaufen zu lassen. Dadurch können sogar die einzelnen Aktivitäten einer Applikation isoliert werden, wie beispielweise einzelne Seitenaufrufe in einem Browser.

Darüber hinaus sind sichere Betriebssysteme die Grundvoraussetzung für sichere IT-Infrastrukturen. Die beiden am häufigsten genutzten Betriebssysteme stammen von US-amerikanischen Herstellen. Diese Systeme wurden nicht unter Sicherheitsaspekten entwickelt, sondern primär unter kommerziellen Gesichtspunkten. Dabei gibt es Alternativen. An Universitäten entwickelte Architekturen für Betriebssysteme berücksichtigen nach dem Prinzip „Security by Design“ Sicherheitsaspekte bereits in der Konzeptionsphase. Die Schwierigkeit, solche Systeme zu etablieren, besteht darin, sie zu einer Marktreife zu bringen. Im Informationszeitalter, wo sichere IT-Infrastrukturen zentral für ein Funktionieren unserer Gesellschaft sind, könnte dies auch eine staatliche Aufgabe sein.

Die zunehmende Bedrohungslage für IT-Systeme macht deutlich, dass konventionelle Sicherheitsmechanismen an ihre Grenzen stoßen. Deshalb sind Konzeption und Realisierung neuer Sicherheitsarchitekturen gefragt – auch als staatliche Aufgabe.

14. Videoüberwachung durch Private

14.1 Erweiterung der Videoüberwachungsbefugnisse für Private

Videoüberwachung greift nicht nur im privaten Umfeld als Maßnahme des Hausrechts immer mehr um sich, auch private Betreiber öffentlich zugänglicher Anlagen setzen verstärkt auf diese Technik. In unserer Beratungspraxis spielen Rechtsfragen rund um das Thema Videoüberwachung eine große Rolle. Die geltende Rechtslage bietet dabei ausreichend Raum für eine angemessene Abwägung zwischen den Interessen der Betreiber und dem Recht der Bürgerinnen und Bürger auf Privatheit.

Videoüberwachung durch Private ist in § 6b Bundesdatenschutzgesetz (BDSG) und §§ 32 bzw. 28 Abs. 1 und Abs. 2 BDSG geregelt. Unterschieden wird zwischen der Videoüberwachung im öffentlich zugänglichen (etwa Bahnhöfe, Einkaufszentren) und im nicht öffentlich zugänglichen Bereich, etwa Unternehmensgelände, Lager oder Personalräume.

Bei öffentlich zugänglichen Flächen und Arbeitsplätzen ist die Überwachung im Sinne des § 6b BDSG nur erlaubt, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Daher sind die schutzwürdigen Belange der Betroffenen abzuwägen mit den Interessen der verantwortlichen Stelle an der Videoüberwachung.

Bei nicht-öffentlich zugänglichen Bereichen kann die Videoüberwachung zur Durchführung des Arbeitsverhältnisses oder dem Erreichen eigener Geschäftszwecke ausnahmsweise erforderlich sein. Zu beachten ist dabei, dass ein permanenter Kontrolldruck auf Beschäftigte, etwa weil sie an ihren Arbeitsplätzen beobachtet oder überwacht werden, grundsätzlich nicht zulässig ist. Auch hier sind die schutzwürdigen Interessen der Betroffenen zu wahren.

Nach den Terroranschlägen im Sommer 2016 wurden Änderungen des BDSG vorgeschlagen, die künftig privaten Stellen in öffentlich zugänglichen Anlagen (Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren, Parkplätze, der öffentliche Nahverkehr) den Betrieb von Videokameras zur Verhinderung von Anschlägen erleichtern sollen. Bei der Abwägungsentscheidung soll der Sicherheit und dem Schutz der Bevölkerung ein größeres Gewicht beigemessen werden.

Ein entsprechender Entwurf für ein „Videoüberwachungsverbesserungsgesetz“ befindet sich in den parlamentarischen Beratungen. Diese waren zur Zeit der Be-

richtserstellung noch nicht abgeschlossen.

Gegenwärtig lässt es das BDSG bereits zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt und Videobilder an Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Im Bereich von großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs, werden zahlreiche Kameras auf der Basis des geltenden Rechts in zulässiger Weise betrieben.

Gleichwohl werden die gesetzlichen Bestimmungen des Datenschutzes und die Anwendungspraxis der Aufsichtsbehörden als zu restriktiv kritisiert.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich bereits im November 2016 kritisch zu dem „Videoüberwachungsverbesserungsgesetz“ geäußert. Die Entschließung ist im Anhang abgedruckt und auf unserer Internetseite www.ldi.nrw.de abrufbar.

Unklar ist, ob die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist.

- Der abschreckende Effekt von Videokameras ist nicht belegt. Terroristen wie auch irrational handelnde Einzeltäter nehmen ihren eigenen Tod bei Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen. Nicht auszuschließen ist, dass Kameras sogar motivierend wirken können.

- Hilfe im Notfall ist in den meisten Fällen nicht zu erwarten: Eine Live-Beobachtung findet nicht statt. Videobilder werden oft nicht durch Personal so ausgewertet, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras weitgehend auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt.

- Die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls kann Grundrechtseingriffe nicht pauschal rechtfertigen.

- Schließlich ist es nicht die Aufgabe privater Stellen, die Sicherheit der Bevölkerung zu gewährleisten. Dies ist eine Kernaufgabe des Staates und obliegt daher allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl

für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Mehr Videoüberwachung führt nicht automatisch zu mehr Sicherheit. Gesetzliche Änderungen, die auf die Ausweitung von Videoüberwachung abzielen, werden wir weiterhin kritisch begleiten. Unsere Orientierungshilfe „Sehen und gesehen werden – Videoüberwachung durch Private in NRW“ aus dem Jahr 2014 ist weiterhin eine oft nachgefragte Unterstützung in der täglichen Beratungspraxis. Sie erläutert mit Fallbeispielen ausführlich die Voraussetzungen und Grenzen der Videoüberwachung durch Private. Sie ist auf unserer Internetseite www.ldi.nrw.de abrufbar.

14.2 Vorsicht bei Dashcams im Straßenverkehr

Dashcams werden in Deutschland immer beliebter. Die Aufzeichnungen sollen häufig bei einem Verkehrsunfall als Beweismittel dienen. Ob sie in gerichtlichen Verfahren verwertbar sind wird von den Gerichten unterschiedlich bewertet. Eindeutig ist jedoch: Ihr Einsatz ist datenschutzrechtlich unzulässig.

Dashcam ist ein Kunstwort, zusammengesetzt aus den englischen Wörtern „DASH board“ (Armaturenbrett) und „CAMera“ (Kamera). Dashcams nehmen auf dem Armaturenbrett oder der Windschutzscheibe den gesamten Verkehr auf – und damit unzählige Personen und Fahrzeuge. Dabei handelt es sich um personenbezogene Daten. Für die Aufnahmen bedarf es daher einer rechtlichen Grundlage, die jedoch nicht vorliegt.

Insbesondere sind die Voraussetzungen des § 6b Abs. 1 und 3 Bundesdatenschutzgesetz (BDSG) für eine zulässige Videoüberwachung nicht erfüllt. Durch den Einsatz wird regelmäßig das informationelle Selbstbestimmungsrecht der anderen Verkehrsteilnehmerinnen und -teilnehmer verletzt. Jeder Mensch hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung zu werden.

Dashcams erfassen permanent eine Vielzahl von Personen, die sich im öffentlichen Verkehrsraum aufhalten. Diese haben keinen Anlass zu dieser Maßnahme gegeben und stehen in keinem Zusammenhang zu einem etwaigen Unfallgeschehen. Zudem werden sie unter einen Generalverdacht gestellt. Die Betroffenen erlangen von der Überwachung regelmäßig weder Kenntnis noch können sie sich dieser entziehen. Ein Hinweis auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle erfolgt regelmäßig nicht.

Das Interesse einer Fahrzeugführerin oder eines -führers, vorsorglich Beweise für den individuell eher seltenen Fall des Eintritts eines Verkehrsunfalls zu sichern, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der übrigen Verkehrsteilnehmenden nicht rechtfertigen.

Selbst die Polizei darf öffentlich zugängliche Orte nur unter den sehr engen gesetzlichen Voraussetzungen an Kriminalitätsbrennpunkten mit optisch-technischen Mitteln beobachten. Erst recht verbietet sich dann eine Überwachung des Verkehrsraumes durch Private, da es dafür keine Rechtsgrundlage gibt.

Die Nutzung einer Dashcam verstößt gegen § 6b Abs. 1 und 3 BDSG und stellt damit eine Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG dar, die mit einem Bußgeld in empfindlicher Höhe sanktioniert werden kann.

Eine andere Frage ist: Sind die auf unrechtmäßige Weise erstellten Aufnahmen

überhaupt als Beweis verwertbar? Eine einheitliche Linie der Gerichte ist hier nicht ersichtlich.

Das Amtsgericht München (Az.: 343 C 4445/13) hat am 6. Juni 2013 in einem Unfallprozess die Verwertung einer durch einen Radfahrer aufgenommenen Videoaufzeichnung für zulässig erachtet. Eine andere Abteilung desselben Gerichts hat allerdings in einem Hinweisbeschluss vom 13. August 2014 (Az: 345 C 5551/14) die Auffassung vertreten, dass Bestimmungen des Datenschutzes und des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) einer Verwertung entgegenstehen. Genauso hat das Landgericht Heilbronn mit Urteil vom 3. Februar 2015 (Az.: 3 S 19/14) festgestellt, dass die mittels einer Dashcam angefertigten Aufnahmen im Zivilprozess nicht als Beweismittel für den Hergang eines Unfalls verwertet werden dürfen. Das Oberlandesgericht Stuttgart hat es wiederum im Beschluss vom 4. Mai 2016 (Az.: 4 Ss 543/15) für grundsätzlich zulässig erachtet, in einem Bußgeldverfahren ein Video für die Verfolgung schwerwiegender Verkehrsordnungswidrigkeiten zu verwerten – hier ein Rotlichtverstoß an einer mindestens seit sechs Sekunden rot zeigenden Ampel.

Auch Verwaltungsgerichte haben sich mit Dashcams beschäftigt. In einem öffentlich dargestellten Fall hatte ein Mann in seinem privaten Pkw Dashcams installiert, um vermeintliche oder tatsächliche Verkehrsverstöße zur Anzeige zu bringen. Die niedersächsische Aufsichtsbehörde hatte deshalb die Verwendung dieser Kameras untersagt und die Löschung der Bilder verfügt. Diese Entscheidung hat das Verwaltungsgericht Göttingen am 12. Oktober 2016 bestätigt (Az.: 1 B 171/16). Die Verfolgung von Verkehrsverstößen stelle eine öffentliche Aufgabe dar, deren Erfüllung Polizei und Ordnungsbehörden vorbehalten sei, so das Gericht.

Aufnahmen von Dashcams stellen einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Unabhängig davon, ob sie im Falle eine Unfalls als Beweismittel verwertbar sind, liegt ein datenschutzrechtlicher Verstoß vor, der als Ordnungswidrigkeit mit einem Bußgeld sanktioniert werden kann. Darüber hinaus besteht die Möglichkeit, den Betrieb einer Dashcam im Wege einer Anordnung zu untersagen.

14.3 Face-Check – ein System zur Zugangskontrolle in Spielhallen

Zur Durchführung von Identitätskontrollen beim Zugang zu Spielhallen wurde ein neues, auf biometrischer Gesichtserkennung beruhendes Kontrollsystem datenschutzrechtlich bewertet. Unter bestimmten Voraussetzungen kann es in NRW als eine datenschutzkonforme Identitätskontrolle eingesetzt werden.

Die Rechtslage zur Einhaltung von Identitätskontrollen zum Ausschluss Minderjähriger und zur Durchsetzung von Spielersperren ist in den Ländern unterschiedlich. Soweit eine Verpflichtung der Spielhallenbetreiber zu Einlasskontrollen besteht, wird diese bisher regelmäßig durch Vorlage des Personalausweises und im Fall von Spielersperren durch einen Abgleich mit einer Sperrdatei erfüllt.

In NRW sind Spielhallenbetreiber gemäß § 16 des Gesetzes zur Ausführung des Glücksspielstaatsvertrages unter anderem zur Einhaltung der Jugendschutzanforderungen nach § 4 Abs. 3 Glücksspielstaatsvertrag verpflichtet. Für die Nutzung der gewerblichen Geldspielautomaten in Spielhallen gibt es in NRW kein Sperrsystem, das mit dem für staatliche Spielbanken geltenden Sperrsystem vergleichbar wäre. Betroffene müssen sich damit in jeder einzelnen Spielhalle selbst ein Hausverbot erteilen. Die dazu erhobenen Daten werden in einer Sperrdatei der jeweiligen Spielhalle gespeichert.
Das neue Kontrollsystem Face-Check funktioniert nach den Angaben der Entwickler wie folgt:

- Beim Face-Check werden lediglich Bilddaten von gesperrten Spielern gespeichert, die der Nutzung im Rahmen des Sperrantrages schriftlich zugestimmt haben.

- Im Eingangsbereich einer Spielstätte aufgestellt, erfasst das System alle Personen beim Betreten und fertigt ein Bild an (Enrollment).

- Aus diesen Bilddaten werden die erkennungsrelevanten Referenzdaten extrahiert (Templates = digitale biometrische Merkmalsdaten) und mit den hinterlegten Referenzdaten gesperrter Personen abgeglichen (Matching).

- Wird ein gesperrter Spieler vom System identifiziert, erfolgt eine Meldung an das Personal. Die Bilddaten nicht gesperrter Personen werden nach dem Abgleich sofort wieder gelöscht. Eine Rekonstruktion der Bilddaten aus den Templates ist technisch nicht möglich.

- Für die Dokumentation zum Nachweis des ordnungsgemäßen Einsatzes (etwa zu den angegebenen Öffnungszeiten) sowie der Umsetzung der Spieler- und Jugendschutzvorgaben gegenüber den Aufsichtsbehörden, werden anonymisierte Templates der

Besucher in einer gesicherten Datenbank gespeichert.

Nach unserer Bewertung ist die damit verbundene Datenverarbeitung nach § 28 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zulässig, soweit der Spielhallenbetreiber zur Durchführung von Identitätskontrollen verpflichtet ist. Insoweit besteht ein berechtigtes Interesse an der Erhebung und Verarbeitung der biometrischen Daten. Diese ist auch erforderlich, da keine weniger intensive und dem Betreiber zumutbare Maßnahme zur Zielerreichung ersichtlich ist. Insbesondere stellt die bislang vorgenommene individuelle Ausweiskontrolle bei jedem Spielhallenbesucher durch das Personal der Spielhalle kein milderes Mittel dar, da die zugangsberechtigten Spieler – anders als bei der Ausweiskontrolle – beim Einsatz von Face-Check anonym bleiben und somit weniger Daten erhoben werden. Zudem kommt es immer wieder vor, dass gesperrte Personen fremde oder gefälschte Ausweise nutzen, so dass die Sperre umgangen werden kann. Das neue System hingegen soll eine Trefferquote von 99,5% aufweisen. Die Computersoftware kann außerdem zuverlässig prognostizieren, ob eine Person unter 18 Jahre alt ist, ohne dass es dafür erforderlich ist, Templates von Jugendlichen zu speichern.

Das vorgelegte Face-Check-System kann in NRW eine datenschutzgerechte Lösung zur Kontrolle von Spielhallenbesuchern darstellen. Voraussetzung ist jedoch, dass die erhobenen Bilddaten in Templates umgewandelt und die Bilddaten gelöscht werden, keine Datenweitergabe an Dritte, keine Speicherung und Auswertung von biometrischen Zusatzinformationen sowie kein Hinzuspeichern und Verknüpfen mit sonstigen Daten der Betroffenen erfolgt. Darüber hinaus darf das System nur für diesen Zweck eingesetzt werden und die Templates müssen nach der Überprüfung des Spielhallenbesuchers innerhalb festgesetzter Löschfristen gelöscht werden.

14.4 „Steckbriefe“ in Schaufenstern oder im Internet

Ladendiebstähle sind ärgerlich und teuer. Moderne Videoüberwachungstechnik kann dabei helfen, diese zu vermeiden oder zumindest aufzuklären. Die Strafverfolgung ist jedoch ausschließlich der Polizei und Staatsanwaltschaft vorbehalten. Geschäftsinhaber dürfen daher keine selbst erstellten „Steckbriefe“ im Schaufenster aushängen oder auf andere Weise veröffentlichen.

Die Videoüberwachung in Geschäften nimmt zu. Nach § 6b Bundesdatenschutzgesetz (BDSG) ist sie jedoch nur unter bestimmten Voraussetzungen möglich. Zur Wahrnehmung des Hausrechts etwa nur dann, wenn sie erforderlich ist und überwiegende schutzwürdige Belange der betroffenen Kundinnen, Kunden und Beschäftigten in angemessener Weise berücksichtigt. Eine permanente, flächendeckende Videoüberwachung in Geschäften ist damit in aller Regel unzulässig. Vielmehr bedarf es einer differenzierten Betrachtung.

Bei einer zulässigen Videobeobachtung können Angestellte mittels Echtzeit-Observation Diebstähle durch sofortiges Einschreiten verhindern. In vielen Fällen wird jedoch das Geschehen lediglich aufgezeichnet. Der Ladendiebstahl fällt erst auf, wenn der oder die Täter das Ladenlokal bereits verlassen haben. Die Videokamera hat die Diebe dann zwar erfasst. Sind die Täter der Geschäftsführung oder den Beschäftigten jedoch nicht persönlich bekannt, sind sie nur schwer feststellbar. Die Verlockung ist dann groß, die Öffentlichkeit durch einen „Steckbrief“ im Schaufenster um Mithilfe zu bitten. Das ist jedoch unzulässig.

Denn nicht nur die Videoaufnahme als solche, auch die anschließende Nutzung der Aufnahme für einen anderen als den ursprünglichen Zweck, unterliegt strengen gesetzlichen Voraussetzungen. Zur Abwehr von Gefahren für die Sicherheit sowie zur Verfolgung von Straftaten dürfen die Daten weiter genutzt werden (§ 6b Abs. 3 Satz 2 BDSG). So ist etwa die Weitergabe der Aufnahmen an Polizei oder Staatsanwaltschaft möglich. Bilder von Personen, denen ein rechtswidriges Verhalten vorgeworfen wird oder gegen die ein Hausverbot ausgesprochen worden ist, auszudrucken und diese für die Allgemeinheit sichtbar zu veröffentlichen, ist hingegen nicht erlaubt. Dies gilt sowohl für den Aushang im Geschäft als auch für die Veröffentlichung derartiger „Fahndungsfotos“ im Internet – zum Beispiel bei Facebook. Jede Art von Öffentlichkeitsfahndung stellt einen Eingriff in die Persönlichkeitsrechte der Verdächtigen dar und darf daher ausschließlich von Polizei und Staatsanwaltschaft nach der Strafprozessordnung erfolgen.

Bilder und Videos von privaten Überwachungskameras dürfen an Polizei und Staatsanwaltschaft zur Strafverfolgung weitergegeben werden. Die Veröffentlichung „Privater Steckbriefe“ in Schaufenstern oder im Internet ist hingegen unzulässig.

14.5 Fahrerassistenzsystem in Straßenbahnen

Videokameras in der Fahrerkabine von Straßenbahnen können datenschutzrechtlich unbedenklich und einen Beitrag zur Verkehrssicherheit leisten.

Um das Fahrpersonal zu unterstützen, beabsichtigt ein Nahverkehrsunternehmen ein so genanntes Fahrerassistenzsystem (FAS) in seinen Straßenbahnen zu installieren. Die Kameras könnten auch Passanten und Kfz-Kennzeichen und damit personenbezogene Daten erfassen. Auf Nachfrage haben wir deshalb das FAS geprüft.

Die Datenverarbeitung ist nach § 6b Abs. 1 Nr. 3, Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) zulässig. Die Vermeidung von Gefahren für den Verkehr ist ein berechtigtes Interesse des Unternehmens und durch die besondere Technik wird die Datenverarbeitung auf ein Mindestmaß beschränkt. Damit überwiegen keine schutzwürdigen Interessen der von der Kameraerfassung betroffenen Personen.

Das FAS unterstützt das Fahrpersonal durch drei Kameras in der Fahrerkabine. Diese nehmen das Gleisbett vor dem Fahrzeug auf. Anschließend werden die Daten im Rohformat als digitaler Datenstrom an die Rechnereinheit gesandt und dort verarbeitet. Dabei handelt es sich um ein geschlossenes System ohne Zugriffsmöglichkeiten durch Dritte. Die Verweildauer der Daten im Arbeitsspeicher des Rechners („flüchtiges RAM“) beträgt dabei nur wenige 100 Millisekunden. Im Rechner werden die Bilder auf Pixelcluster-Ebene verglichen. Wer oder was sich im Gleisbett befindet, kann und braucht das System nicht festzustellen. Ausreichend ist die Feststellung, dass ein Hindernis vorhanden ist. In einem solchen Fall warnt das System zunächst das Fahrpersonal. Reagiert es nicht, kann die Technik auch in das Fahrgeschehen eingreifen, zum Beispiel durch Aktivierung der Glocke, des Lichts oder auch der Bremse. Nach Beendigung der Analyse eines Bildsatzes werden die Daten durch das System wieder überschrieben.

Die Beschränkung des Grundrechts auf informationelle Selbstbestimmung steht bei diesem FAS nicht außer Verhältnis zu den Aspekten, die für die Maßnahme sprechen. Unfälle mit Straßenbahnen haben oft verheerende Folgen. Demgegenüber sind die Folgen der Datenverarbeitung durch die technische Ausgestaltung für Betroffene gering. Ein Zugriff auf die Daten ist faktisch unmöglich. Die Daten werden nach ihrer Erhebung nahezu zeitgleich wieder gelöscht.

Datenschutz sollte bereits bei der technischen Entwicklung neuer Kamerasysteme ein wichtiger Aspekt sein. Das Fahrassistenzsystem könnte ein gutes Beispiel für den datenschutzgerechten Einsatz von Videokameras werden.

14.6 Kennzeichenerfassung im Lkw-Leitsystem

Ein neues Lkw-Leitsystem soll den Verkehr auf den Zufahrten und in den Terminals des Duisburger Hafens verbessern. Da das System auch Kfz-Kennzeichen erfasst, stellt sich die Frage der datenschutzrechtlichen Zulässigkeit. Mit unserer Beratung hat die Hafenbetreiberin eine datenschutzgerechte Lösung gefunden.

Auf ausgesuchten Streckenabschnitten sollen die Reisezeiten der Lkw ermittelt und den Lkw-Fahrerinnen und Fahrern günstigere Alternativrouten etwa auf LED-Verkehrsinfo-Schilder vorgeschlagen werden. Die dafür erforderliche Wiedererkennung der Lkw erfolgt durch die Kfz-Kennzeichendaten, die im geschlossenen System der Kamera erfasst und in eine anonymisierte Zeichenkette umgewandelt werden. Anschließend werden diese anonymisiert und über standardisierte Schnittstellen an eine Zentralebene weitergeleitet.

Grundlage des Lkw-Leitsystems sind damit Kfz-Kennzeichendaten. Diese sind personenbezogene Daten (§ 45 Satz 2 Straßenverkehrsgesetz – StVG). Die Verarbeitung muss deshalb auf einer Rechtsgrundlage beruhen. Das gilt auch dann, wenn sie nur für eine kurze Zeit erhoben und verarbeitet werden.

Rechtsgrundlage für diese Erfassung ist § 6b Abs. 1 Nr. 3, Abs. 3 Satz 1 BDSG. Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Zudem dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Ziel des Systems ist es, eine Optimierung hinsichtlich Effizienz und Kosten für alle Beteiligten zu erreichen. Aufgrund einer verbesserten Planungsgrundlage der Be- und Entladestelle sollen Staus im Bereich des Hafens, Wartezeiten vor den Toren der Terminals und der Logistikdienstleister vermieden und die logistischen Prozesse in ihrer Gesamtheit sowie eine bessere Auslastung der Ressourcen unterstützt werden.

Um das Lkw-Verkehrsaufkommen feststellen und ggf. lenken zu können, müssen die Fahrzeuge erfasst werden. Obwohl hierfür ein Personenbezug zwar nicht notwendig ist, wird als Datenbasis jedoch das personenbezogene Kfz-Kennzeichen erfasst. Eine Rückführbarkeit soll dadurch ausgeschlossen werden, indem mittels einer zufälligen Zeichenfolge (Salt), einem Algorithmus und einem verkürzten Signaturstring das Kennzeichen umgewandelt und anonymisiert wird. Zwar kann eine Verknüpfung eines anonymisierten Signaturstrings mit anderen Informationen nicht völlig ausgeschlossen werden. Durch die Änderung des Salt nach einem

Tag und durch eine kurzfristige Löschung im Verarbeitungssystem wird eine solche Verknüpfung jedoch unwahrscheinlich. Die Erhebung und Verarbeitung des personenbezogenen Kennzeichendatums beschränkt sich somit auf den Bruchteil einer Sekunde, bis es im Kamerasystem in ein anonymes Datum umgewandelt wird. Damit steht die Beschränkung des Grundrechts auf informationelle Selbstbestimmung auch nicht außer Verhältnis zu den Aspekten, die für die Maßnahme sprechen.

Werden Kfz-Kennzeichen auch nur für eine sehr kurze Zeit erhoben und verarbeitet , ist hierfür eine Befugnisnorm erforderlich. Eine solche kann § 6b Abs. 1 Nr. 3, Abs. 3 Satz 1 BDSG sein. Werden die Daten in einem geschlossenen Kamerasystem unverzüglich anonymisiert und ist eine Rückverfolgbarkeit nicht möglich, kann die Kennzeichenerfassung datenschutzrechtlich zulässig sein.

15. Wirtschaft

15.1 Datenschutzprüfung in der Wohnungswirtschaft

Gerade in Ballungsgebieten werden viele Mietinteressentinnen und -interessenten wegen der knappen Wohnraumsituation genötigt, umfassende Auskunft über sich zu erteilen. Die Beschwerden über umfangreiche, oft sensible Datenerhebungen vor Abschluss eines Mietvertrages nehmen zu. Grund genug, die Wohnungswirtschaft genauer ins Blickfeld zu nehmen.

Im Jahr 2014 haben wir mit der gemeinsamen Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ Vermieterinnen und Vermietern eine wichtige Praxishilfe an die Hand gegeben (siehe Bericht 2015 unter 5.2). Die Orientierungshilfe ist auf unserer Homepage www.ldi.nrw.de abrufbar. In einer gemeinsamen Prüfinitiative mit dem Bayerischen Landesamt für Datenschutzaufsicht haben wir nunmehr die Verfahrensweise von Immobilienmaklerinnen und -maklern sowie Wohnungsverwaltungsgesellschaften in NRW untersucht.

Ziel der stichprobenhaften Prüfung war es, die Verantwortlichen in der Wohnungswirtschaft für den Datenschutz zu sensibilisieren und darauf hinzuwirken, dass der Grundsatz der Datensparsamkeit berücksichtigt wird. Schwerpunkt der Prüfung war der Inhalt der verwendeten Mieterselbstauskunftsformulare. Berücksichtigt wurden unter anderem auch Aspekte der Datensicherheit bei der Nutzung von Online-Kontaktformularen und elektronischer Kommunikation sowie die Anfertigung von Personalausweiskopien.

Bei der Auswahl haben wir darauf geachtet, dass Immobilienmaklerinnen und -makler sowie Wohnungsverwaltungsgesellschaften aus allen Regionen in NRW einbezogen wurden. Zudem sollten kleine, mittelständische und größere Unternehmen erfasst werden. Diese erhielten einen Fragebogen und wurden aufgefordert, von ihnen verwendete Formulare zur Überprüfung vorzulegen.

Bei allen geprüften Unternehmen bestand Anlass zu Beanstandungen. Viele Unternehmen haben ihre Prozesse daraufhin datenschutzgerechter gestaltet. Einige Unternehmen haben wir dabei umfangreich beraten.

Bei der Prüfung der Formulare zur Mieterselbstauskunft haben wir festgestellt, dass diese häufig bereits vor Besichtigung eines Objektes verlangt werden. Der Fragebogen ist jedoch erst dann auszufüllen, wenn nach erfolgter Besichtigung ernsthaftes Interesse an dem Objekt besteht. Aber auch dann dürfen nicht jegliche Art von Daten erhoben werden. Häufig beanstandet wurden insbesondere folgende Fragen:

■ Kontaktdaten der derzeitigen Vermieterin bzw. des derzeitigen Vermieters

Diese Frage halten wir für unzulässig, da sie zum einen für den Abschluss eines Mietvertrages nicht erforderlich ist und zum anderen dem Grundsatz der Direkterhebung (§ 4 Abs. 2 Satz 1 Bundesdatenschutzgesetz) widerspricht.

■ Bonitätsauskünfte

Die undifferenzierte Forderung nach Vorlage einer „Schufa-Auskunft“ oder „Schufa-Selbstauskunft“ ist unzulässig. Diese Auskünfte enthalten deutlich mehr Datenkategorien als spezielle (häufig kostenpflichtige) zur Weiterleitung an Dritte geeignete Produkte und führen somit zu einer über das erforderliche Maß hinausgehenden Erhebung von Daten. Die Auskunfteien dürfen bei diesen Produkten hauptsächlich folgende Datenkategorien mitteilen:

- Informationen aus amtlichen Schuldner- und Insolvenzverzeichnissen,
- sonstige unbestrittene Daten über negatives Zahlungsverhalten, soweit es sich nicht um Bagatellbeträge handelt.

Erst wenn der Abschluss des Mietvertrags unmittelbar bevorsteht, dürfen eine Bonitätsauskunft bei Auskunfteien oder die Vorlage einer Bonitätsauskunft verlangt werden.

■ Familienstand

Sofern lediglich die Mieterin oder der Mieter Vertragspartei wird, sind Angaben zum Familienstand für die Entscheidung über den Abschluss eines Mietvertrages nicht erforderlich und daher im Ergebnis unzulässig. Nahe Familienangehörige wie Ehegattinnen und -gatten, Lebenspartnerinnen und -partner sowie Kinder dürfen nämlich auch ohne Erlaubnis mit in die Wohnung aufgenommen werden.

■ Frage nach dienstlicher Telefonnummer

Diese Information ist nicht erforderlich, zumal eine telefonische Kontaktaufnahme am Arbeitsplatz eventuell auch arbeitsrechtliche Konsequenzen mit sich bringen könnte. Hier sollte die Angabe – wenn überhaupt – ausschließlich freiwillig erfolgen.

■ Angaben zu Kindern und sonstigen Angehörigen

Da nahe Familienangehörige ohne Erlaubnis mit in die Wohnung aufgenommen werden dürfen, sind die Fragen zu Geburtstag sowie Verwandtschaftsverhältnis der zum Haushalt gehörenden Kinder und sonstigen Angehörigen nicht erforderlich und im Ergebnis unzulässig. Die Namen sowie das Alter der einziehenden Personen darf dagegen erfragt werden.

■ Fragen zum Beruf

Für die Entscheidung über den Abschluss eines Mietvertrages darf nach dem Beruf und der Arbeitsstätte als Kriterium zur Beurteilung der Bonität gefragt werden. Die Frage nach der Dauer einer Beschäftigung bietet jedoch in einer mobilen Gesellschaft

keine Gewissheit für die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses. Diese Frage ist daher nicht geeignet, das Sicherungsbedürfnis einer Vermieterin oder eines Vermieters zu erfüllen.

■ Personalausweiskopie

Auch bezüglich der Erstellung von Personalausweiskopien gab es häufig Grund zu Beanstandungen. Anders als beim Verkauf einer Immobilie ist die Anfertigung von Personalausweiskopien bei Vermietungen in der Regel unzulässig. Gestattet ist allerdings, die Angaben zur Identität durch Vorlage des Personalausweises zu prüfen und einen schriftlichen Vermerk über das Ergebnis der Einsichtnahme zu fertigen. Notiert werden dürfen Name, Vorname und Geburtsdatum, ggf. auch Geburtsort und Anschrift. Denn dabei handelt es sich um für die Personenidentifikation notwendige Daten. Eine weitergehende Notiz, zum Beispiel zur Zugangs- und Seriennummer des Personalausweises, darf nicht erfolgen.

Wenn Online-Kontaktformulare genutzt werden, haben wir häufig darauf hingewiesen, dass es sich um ein allgemeines Kontaktformular handelt und eventuell bereits eine Antwort per E-Mail ausreichend ist. Die zusätzliche Angabe von Telefonnummer und/oder Anschrift als Pflichtfeldangabe ist damit nicht erforderlich.

Einige der geprüften Unternehmen konnten kein Konzept für die Löschung bzw. Sperrung nicht mehr erforderlicher personenbezogener Daten vorweisen. Auffällig war ebenfalls, dass Daten von Bewerberinnen und Bewerbern, die nicht berücksichtigt wurden, teilweise für einen langen Zeitraum (bis zu zehn Jahren) gespeichert wurden.

Die Prüfung hat gezeigt, dass die Verantwortlichen in der Wohnungswirtschaft fortgesetzt für den Datenschutz sensibilisiert werden müssen. Wir werden das Thema weiter verfolgen und diesen Wirtschaftsbereich weiter beraten.

15.2 Fahrerbewertungsportale – Bewertung von Privatpersonen im Internet

Bewertungsportale im Internet sind nicht neu. Bewertet werden etwa schon Restaurants, Hotels sowie Ärztinnen und Ärzte (siehe Bericht 2011 unter 6.7). Neu ist ein Portal, in dem – zugeordnet zum jeweiligen Autokennzeichen – der Fahrstil bewertet werden kann und die Gesamtnote im Internet abrufbar ist. Den Betrieb eines solchen Portals haben wir so eingeschränkt, dass die Bewertungen nicht mehr öffentlich, sondern nur noch von den Bewerteten selbst abrufbar sind. Das Verwaltungsgericht hat diese Einschränkungen bestätigt.

Ein Unternehmen in NRW betreibt im Internet ein Portal, in das jede und jeder über die Eingabe des Autokennzeichens eine Bewertung des Fahrstils abgeben kann. Hierzu gibt es vorformulierte Kataloge mit negativen, positiven und neutralen Kriterien. Die Bewertungen werden sodann auf das amtliche Kennzeichen bezogen ausgewertet und das Gesamturteil im Internet frei zugänglich gemacht. Das Portal verfügt über eine Kennzeichensuchfunktion und über eine Möglichkeit zur Nachverfolgung von Bewertungen. Betroffene können sich an eine Beschwerdestelle bei der Portalbetreiberin wenden, wenn sie sich zu Unrecht bewertet sehen.

Entsprechend der Rechtsprechung des Bundesgerichtshofs zu den berufsbezogenen Bewertungsportalen von Lehrkräften sowie von Ärztinnen und Ärzten beurteilt sich die datenschutzrechtliche Zulässigkeit eines personenbezogenen Bewertungsportals nach § 29 Bundesdatenschutzgesetz.

Das Autokennzeichen ist bereits nach § 45 Satz 2 Straßenverkehrsgesetz ein personenbezogenes Datum. Zudem kann die Nachbarschaft, der Freundeskreis, Arbeitskolleginnen und -kollegen aber auch Autoversicherungen ohne großen Aufwand den Kennzeichen eine Person zuordnen.

Für die datenschutzrechtliche Bewertung sind das Recht auf informationelle Selbstbestimmung der bewerteten Person auf der einen und die Interessen der Portalbetreiberin und der Nutzerinnen und Nutzer des Portals auf der anderen Seite abzuwägen.

Das erklärte Ziel des Portals ist es, der Rücksichtslosigkeit im Straßenverkehr entgegenzuwirken. Zudem soll es nach eigenen Angaben den Nutzerinnen und Nutzern von privaten Mitfahr- und Carsharing-Zentralen die Möglichkeit bieten, die Zuverlässigkeit von Fahrerinnen und Fahrern abzuschätzen. Die Bewerteten sollen zu einer Selbstreflexion über ihr Fahrverhalten angehalten werden und dieses mit dem Ziel erhöhter Rücksichtnahme verbessern.

Diese Ziele mögen grundsätzlich erstrebenswert sein, aber der gewählte Weg verletzt in unzulässiger Weise die Grundrechte der Bewerteten.

In dem Fahrerbewertungsportal sehen wir eine neue Dimension von Bewertungsportalen. Ging es bislang um berufs- oder dienstleistungsbezogene Portale, werden mit diesem Portal privat motivierte Verhaltensweisen – hier das Fahrverhalten – öffentlich an den Pranger gestellt. Die oder der Einzelne wird damit zu einem Objekt einer überraschenden, organisierten Datenerhebung.

Daten zu Privatpersonen dürfen grundsätzlich nur mit Einwilligung der Betroffenen im Internet veröffentlicht werden. Denn im Internet veröffentlichte Informationen, Meinungen oder Bewertungen können – einmal online gestellt – nicht wieder zurückgeholt werden. Sie sind über Jahrzehnte weltweit abrufbar. Während selbst Haftstrafen und Registereinträge zeitlich befristet sind, können Eintragungen im Internet daher die betroffene Person lebenslänglich verfolgen – mit unvorhersehbaren Folgen für das künftige berufliche oder private Leben.

Mit dem Bewertungsportal wird im Übrigen eine unnötige private Nebenjustiz geschaffen. Für die Kontrolle des Straßenverkehrs und die Ahndung von Verkehrsverstößen sind ausschließlich staatliche Stellen wie die Polizei- und Verkehrsordnungsbehörden zuständig. Deren Entscheidungen erfolgen im Rahmen rechtstaatlicher Verfahren und sind gerichtlich überprüfbar. Um das Ziel der Selbstreflexion nicht gänzlich zu verhindern, haben wir das Betreiben des Portals nicht vollständig untersagt, sondern der Betreiberin bestimmte Auflagen erteilt. Hierzu zählt insbesondere, dass den besonderen Gefahren eines Portals im Internet mit der weltweit möglichen Abrufbarkeit Grenzen gesetzt werden. So kann zwar jedermann eine Bewertung in das Portal eingeben, abrufen darf sie aber nur die bewertete Person selbst.

Auf die Klage der Betreiberin gegen unsere Auflagen hat das Verwaltungsgericht Köln unsere Interessenabwägung zugunsten des Datenschutzes bestätigt (Urteil vom 16. Februar 2017, Az. 13 K 6093/15). Das Urteil war zum Redaktionsschluss noch nicht rechtskräftig, da die Berufung zum Oberverwaltungsgericht NRW wegen der grundsätzlichen Bedeutung zugelassen wurde.

Daten über Privatpersonen dürfen grundsätzlich nur mit Einwilligung der Betroffenen im Internet veröffentlicht werden. Dies gilt insbesondere auch für Bewertungsportale. Bestrebungen, das Verhalten von Privatpersonen im Internet zu bewerten, werden wir weiterhin kritisch verfolgen.

15.3 Datenschutz im Kraftfahrzeug – Gemeinsame Erklärung der Datenschutzaufsichten und der Automobilindustrie

Die Digitalisierung von Kraftfahrzeugen nimmt weiter Fahrt auf. Ab dem Jahr 2030 werden Autos allein fahren können – so die Automobilindustrie. Die Bundesregierung hat Anfang 2017 den Entwurf eines Gesetzes zum automatisierten Fahren auf den Weg gebracht. Der Datenschutz darf hier jedoch nicht auf der Strecke bleiben.

Moderne Steuergeräte mit großen Datenspeichern in Autos sind nicht neu. Auf die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht haben wir bereits im Bericht 2015 unter 7.1 aufmerksam gemacht. Das seinerzeit erwähnte autonom fahrende Auto kommt immer näher: Die Automobilindustrie strebt für das Jahr 2030 das fahrerlose Fahren eines Kraftfahrzeugs an. Dann lenkt ein Autopilot. Der Mensch am Steuer wird überflüssig. Der Weg dorthin kann in vier Stufen unterteilt werden, wobei die Unterstützung der Fahrerinnen und Fahrer schrittweise erhöht wird:

1. Stufe – Assistiertes Fahren
Unterstützung durch Assistenzsysteme wie Spurhalteassistent, Stauassistent, Abstandmesser und Totwinkelüberwachung.

2. Stufe – Teilautomatisiertes Fahren
In bestimmten Situationen – etwa auf Autobahnen – muss das Auto nicht mehr gesteuert werden. Die jederzeitige Übernahme durch den Menschen muss jedoch möglich sein.

3. Stufe – Hochautomatisiertes Fahren
Ermöglicht nicht nur automatisches Steuern. Auch den Weg finden die Fahrzeuge alleine. Nur im Notfall muss noch eingegriffen werden.

4. Stufe – Vollautomatisiertes Fahren
In speziellen Anwendungsfällen – zum Beispiel beim Parken und Rangieren im Parkhaus – ist eine Fahrerin oder ein Fahrer überflüssig.

Zurzeit sind die modernen Kraftfahrzeuge dem assistierten (erste Stufe) und teilautomatisierten (zweite Stufe) Bereich zuzuordnen. Der Schritt zum hochautomatisierten Fahren (dritte Stufe) steht noch bevor.

Daneben sind weitere moderne Assistenzsysteme, die die Kopplung des eigenen Smartphones mit dem Fahrzeug (vernetzte Infotainment-Systeme) sowie Zusatzdienstleistungen rund um das Fahrzeug (etwa Pannenhilfe) ermöglichen, bereits heute Standard beim Kauf eines neuen Fahrzeugs.

Im Januar 2017 hat die Bundesregierung einen Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes (BR-Drs. 69/17) auf den Weg gebracht, der die rechtliche Grundlage für die Nutzung von hoch- oder vollautomatisierten Kraftfahrzeugen bil-

den soll. Geregelt wird das Zusammenwirken zwischen dem Kraftfahrzeug mit automatisierter Fahrfunktion und dem Fahrer oder der Fahrerin. Die Fahrzeugführung soll wieder übernommen werden, wenn das elektronische System dies anzeigt. Um im Schadensfall feststellen zu können, ob ein individueller Fahrfehler oder ein Systemfehler die Ursache war, sollen aufgrund einer neuen Regelung im Straßenverkehrsgesetz Fahrzeugdaten aufgezeichnet und abrufbar gehalten werden. Zu den Daten gehören der Status manuelles oder automatisiertes Fahren, das Systemsignal zur Steuerungsübernahme sowie etwaige technische Störungen. Hier ist es wichtig, dass die Regelung zu den aufzuzeichnenden Daten hinreichend bestimmt ist.

Zwar unterstützen die neuen Technologien im vernetzten Automobil das Fahren und können den Verkehr sicherer machen. Auch lässt sich der Fahrzeugverkehr mittels Telematik umweltschonend leiten und in eine Mobilitätskette effizient integrieren. Die Systeme speichern jedoch in einem enormen Umfang Nutzungs- und Bewegungsdaten. Diese Daten erlauben Einblicke in die persönliche Lebensführung und können wirtschaftlich profitabel verwertet werden.

Um den Datenschutz bei der Entwicklung neuer Fahrzeuge zu sichern, stehen die deutschen Datenschutzaufsichtsbehörden mit Vertreterinnen und Vertretern der deutschen Automobilindustrie in einem intensiven Dialog. Trotz der rechtlichen und technischen Komplexität wurden bereits wesentliche Zwischenergebnisse erreicht. Diese sind in der gemeinsamen Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) „Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Fahrzeuge“ vom 26. Januar 2016 zusammengefasst. Die Entschließung ist im Anhang abgedruckt und auf unserer Homepage www.ldi.nrw.de abrufbar.

Kernpunkte der gemeinsamen Erklärung:

- **Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG)**

Ihre ursprüngliche Auffassung, dass alle Daten im Kfz lediglich technische Daten seien, hat die Automobilindustrie im Rahmen des Dialogs aufgegeben und die Personenbeziehbarkeit und damit die Anwendbarkeit des BDSG akzeptiert.

- **Datenschutzgerechte Ausgestaltung der Technik**

Zwar wird das formelle Auskunftsrecht nach § 34 BDSG seitens der Hersteller auf die bei ihnen gespeicherten Daten begrenzt. Die Automobilindustrie erkennt jedoch ihre Grundverantwortung bei der Ausgestaltung der Technik an. Um dieser Verantwortung nachzukommen, wird sie den Grundsatz des Datenschutzes durch Technik (data protection by design) beachten. Dies manifestiert sich etwa in der Herausgabe verständlicher Erläuterungen an

die Nutzerinnen und Nutzer (zum Beispiel durch gut ausgearbeitete Bordinformationen) sowie in der technischen Möglichkeit für die Fahrerin und den Fahrer, bestimmte Funktionen und damit Datenströme aktiv an- und abzuschalten.

■ **Umfang der Verantwortlichkeit**

Andererseits wurde eine Verständigung darüber erzielt, dass die Verantwortung der Hersteller dort endet, wo die Nutzerin oder der Nutzer die Dienste von Drittanbietern in das Fahrzeug integriert. Dabei ist zu berücksichtigen, dass die Hersteller aufgrund europäischer und/oder internationaler Vorgaben teilweise verpflichtet sind, Schnittstellen im Fahrzeug für Drittanbieter offen zu halten.

Der Dialog mit der Automobilindustrie wird nach Veröffentlichung der gemeinsamen Erklärung, die sich auf rechtliche Fragestellungen konzentriert, fortgesetzt. Dabei wird es um eine allgemein verständliche Bordinformation sowie um technisch-organisatorische Eckpunkte und Standardisierungen gehen.

Die gemeinsame Erklärung ist jetzt von der Automobilindustrie technisch umzusetzen. Insbesondere sollten die Hersteller und ihre Vertragswerkstätten gemeinsam dafür Sorge tragen, dass die Fahrzeugnutzerinnen und -nutzer verständliche Informationen darüber erhalten, welche Daten erhoben werden und wer die Daten erhält.

15.4 Fraud Prevention Pool – Neue Datenbank zur Betrugsbekämpfung in der Kreditwirtschaft

Um verstärkt gegen Betrugsfälle, Terrorismusfinanzierung und Geldwäsche vorgehen zu können, haben die Kreditinstitute eine neue Datenbank entwickelt – den so genannten Fraud Prevention Pool (FPP).

Bereits im Jahr 2012 entwickelte der Bankenfachverband mit seinen Mitgliedsinstituten ein Anforderungsprofil für einen FPP. Ziel war eine zentrale Speicherung von personenbezogenen Daten zu Betrugsverdachtsfällen durch einen externen Dienstleister, in den die Mitglieder des Pools Daten einmelden. Diese sollen anschließend als Warninformationen ausgetauscht werden. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben das Konzept des FPP mit dem Ziel beraten, einen allgemeingültigen Kriterienkatalog für solche Warndateien aufzustellen. Darauf aufbauend werden bereits Produkte von Wirtschaftsauskunfteien angeboten.

Hinsichtlich der gesetzlichen Bestimmungen im Kreditwesengesetz (KWG) sind sich die Aufsichtsbehörden einig, dass § 25h Abs. 3 Satz 4 und 5 KWG nicht als Ermächtigungsgrundlage für von Auskunfteien betriebene, zentrale FPP in Betracht kommt. Die Regelung gilt ihrem Wortlaut nach nur für Datenübermittlungen im Einzelfall. Zur Frage, ob diese Norm eine abschließende Datenschutzregelung für den Datenaustausch zwischen Banken darstellt und damit über § 1 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) eine Sperrwirkung gegenüber den allgemeinen Datenübermittlungsnormen des BDSG entfaltet, bestehen allerdings bei den Aufsichtsbehörden unterschiedliche Rechtsauffassungen. Eine diesbezügliche Klarstellung durch den Gesetzgeber wäre daher zu begrüßen.

Unabhängig von den unterschiedlichen Bewertungen hinsichtlich § 25h Abs. 3 KWG fordern die Datenschutzaufsichtsbehörden des Bundes und der Länder für Datenbanken zum Zwecke der Betrugsprävention bundeseinheitliche Mindeststandards. Grundlage des nachfolgenden Katalogs ist, zwischen dem Interesse der Kreditinstitute, ihr Vermögensrisiko zu begrenzen, und dem schützenswerten Gegeninteresse der Betroffenen abzuwägen. Die Datenschutzaufsichtsbehörden fordern daher mehrheitlich:

1. In Bezug auf die Einmeldung in den Pool:
   - Sachverhalt inklusive Identität der Täterin oder des Täters müssen eindeutig festgestellt sein.
   - Auffällige/ungewöhnliche Sachverhalte werden im Vorfeld klar und abschließend definiert (Fallgruppenkatalog/Meldemerkmale), kein Freitext (kein Raum für subjektive Vermutungen).
   - Vorwurf muss signifikant sein (keine Geringfügigkeit, ggf. Betragsgrenze).

- Beweisbarkeit (zum Beispiel durch gefälschte Dokumente).

- Umfassende Dokumentationspflicht zwecks nachträglicher Überprüfbarkeit der Einmeldung.

- Einmeldung nur durch besonders qualifiziertes Personal (Betrugspräventionsabteilung) und klare Compliance-Regelungen.

2. In Bezug auf die Verarbeitung (Speicherung/Nutzung) im Pool:

- Unterrichtung der Betroffenen über ihre konkrete Einmeldung in den Pool (zu Beginn der Geschäftsbeziehung bereits allgemeine Unterrichtung zu FPP durch das einmeldende Institut).

- Alle üblichen Betroffenenrechte gegenüber einer Auskunftei: Unter anderem umfassende Selbstauskunft, Löschung/Sperrung, Berichtigung, Nachberichtspflicht – mit der Garantie unverzüglicher Bearbeitung.

- Problem bei Identitätsbetrug, soweit es Opfer gibt: Opferschutz durch besondere Kennzeichnung – nur nach Einwilligung des Opfers.

- Keine Nutzung des eingemeldeten Sachverhalts für Bonitätsauskünfte und zur Berechnung von Score-Werten.

3. In Bezug auf die Beauskunftung/Übermittlung aus dem Pool:

- Vorliegen eines berechtigten Interesses der anfragenden Stelle (mit berechtigter Bonitätsanfrage indiziert).

- Übermittlung nur der absolut notwendigen Daten (anfragende Stelle soll nur gewarnt und damit zur Vorsicht bewegt werden).

- Übermittlung nur an einen ausgewählt kleinen Kreis bei der anfragenden Stelle.

- Dokumentation des berechtigten Interesses bei der anfragenden Stelle und Stichprobenkontrolle seitens der Auskunftei.

- Bei Warnmeldung aus dem Pool: Kein Automatismus zur Ablehnung, sondern nur berechtigter Anlass zu einer tieferen Prüfung (so genanntes Aussteuern).

Angebote zu Betrugspräventionsdatenbanken werden wir nach Maßgabe dieser drei Kriteriengruppen zu Einmeldung, Speicherung und Beauskunftung prüfen.

15.5 Personen-Identifikation per Videochat im Bankenbereich

Kredit- und Finanzdienstleistungsinstitute sind nach dem Geldwäschegesetz (GwG) verpflichtet, ihren Vertragspartnerinnen und -partnern für die Begründung einer Geschäftsbeziehung zu identifizieren. Wer online ein Konto eröffnen möchte und nicht die elektronische Identitätsfunktion des neuen Personalausweises benutzt, musste hierfür bislang eine Filiale der Deutschen Post AG aufsuchen. Nun gibt es Alternativen ohne Medienbruch, die es ermöglichen, sich vom heimischen Computer aus über Videochat zu identifizieren. Doch wie steht es mit dem Datenschutz?

Für die Online-Identifikation per Videochat müssen die Kundinnen und Kunden das Ausweisdokument vor die Webcam halten und eine an sie übermittelte Transaktionsnummer (TAN) eingeben. Von den Kundinnen und Kunden und ihren Ausweisen werden dann Fotos bzw. Screenshots angefertigt. Diese Identifizierungsverfahren werden von den Kredit- und Finanzdienstleistungsinstituten entweder selbst durchgeführt oder die Institute bedienen sich darauf spezialisierter Anbieter von Identifizierungsverfahren (so genannte ID-Dienstleister). Diese wiederum können die Dienstleistung von Kommunikationsanbietern nutzen.

Wir sind der Auffassung, dass ein solches Verfahren nur unter folgenden – kumulativen – Voraussetzungen zulässig ist:

- Die Kundinnen und Kunden geben eine freiwillige und informierte Einwilligung ab. Dafür ist erforderlich, dass weiterhin alternative Möglichkeiten zur Identifizierung – wie die Identifizierung in einer Filiale der Deutschen Post AG – zur Verfügung stehen.

- Der ID-Dienstleister schwärzt die nach § 4 Abs. 3 Nr. 1 und § 8 Abs. 1 Satz 2 GwG nicht für die Identifizierung erforderlichen Daten sofort bei der Aufnahme. Erforderlich ist die Erhebung von Vor- und Nachname, Geburtsort, Geburtsdatum, Staatsangehörigkeit, Anschrift sowie die Erfassung von Art, Nummer und ausstellender Behörde des zur Überprüfung der Identität vorgelegten Ausweisdokuments.

- Das Gespräch zwischen ID-Dienstleister und Kundinnen bzw. Kunden darf nicht aufgezeichnet werden. Da bereits Fotos und Screenshots angefertigt werden, würde durch die zusätzliche Aufzeichnung eine Doppelerfassung personenbezogener Daten erfolgen.

- Sollte der Identifizierungsprozess abgebrochen werden müssen, muss der ID-Dienstleister die bis dahin angefallenen Daten unverzüglich löschen.

- Die TAN sollte bei den Kundinnen und Kunden über ein anderes Gerät (zum Beispiel Handy) empfangen werden als dasjenige, über welches

die Identifizierung vorgenommen wird. Erforderlich ist die Verwendung einer Ende-zu-Ende-Verschlüsselung, bei der Versender und Empfänger jeweils den Schlüssel zur Entschlüsselung besitzen.

- Der Chat sollte nur über einen Kommunikationsanbieter durchgeführt werden, der nicht „mitliest".

Eine Personenidentifikation per Videochat kann datenschutzrechtlich zulässig sein. Es müssen jedoch Alternativen vorhanden und die genannten Voraussetzungen erfüllt sein.

15.6 Bonitätsauskünfte im Online- und Versandhandel

Der Online- und Versandhandel bietet häufig verschiedene Zahlungsarten an – mit unterschiedlichen Ausfallrisiken. Beim Zahlen per Vorkasse gibt es ein solches Risiko nicht, so dass kein berechtigtes Interesse an einer Bonitätsinformation bei einer Auskunftei besteht. Noch bevor die Zahlungsart geklärt ist, wird gleichwohl häufig eine pauschale Einwilligung der Kundinnen und Kunden in die Abfrage von Bonitätsauskünften erbeten.

Die von uns aufgrund von Beschwerden geprüften Online- und Versandhändler begründeten die vorgeschaltete Bonitätsprüfung damit, dass auf diesem Wege ausschließlich Zahlungsmethoden angeboten würden, die aufgrund des Ergebnisses der jeweiligen Bonitätsüberprüfung zur Risikominimierung in Betracht kommen. Nur so ließe sich vermeiden, dass viele Kaufvorgänge abgebrochen werden, weil die bevorzugte Zahlungsart aufgrund schlechter Bonitätsbewertung nicht angeboten wird.

Im Oktober 2015 kamen die Datenschutzaufsichtsbehörden des Bundes und der Länder nahezu einhellig zu der Auffassung, dass eine vorherige Bonitätsabfrage allein zur Steuerung der anzubietenden Zahlungsarten unzulässig ist.

Für eine Bonitätsabfrage vor Auswahl der gewünschten Zahlungsart durch die Kundschaft liegt kein berechtigtes Interesse im Sinne der §§ 28 Abs. 1 Satz 1 Nr. 2, 29 Abs. 2 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) vor. Dieses besteht nur bei der Auswahl einer riskanten Zahlungsart, zum Beispiel „Kauf auf Rechnung“ oder „Ratenzahlungsvereinbarung“.

Das Ziel, Kaufabbrüche zu verhindern, indem jeweils ausschließlich im Einzelfall geeignete Zahlungsmodalitäten angeboten werden, stellt kein berechtigtes Interesse dar. Eine Bonitätsprüfung ist vor der Auswahl einer Zahlungsart nicht erforderlich, da sich für die Händlerin bzw. für den Händler (noch) kein finanzielles Ausfallrisiko abzeichnet. Dies gilt besonders, wenn der Bestellvorgang nach der Zahlungsartensteuerung abgebrochen wird oder eine Zahlungsmethode ohne kreditorisches Risiko (etwa Vorkasse) ausgewählt wird.

Neben der fehlenden Erforderlichkeit einer vorweggenommenen Bonitätsabfrage sehen wir schützenswerte Gegeninteressen der betroffenen Kundschaft. Nach Kenntnisstand der Aufsichtsbehörden beziehen Auskunfteien teilweise die Anzahl der Bonitätsabfragen in ihre Scorewertberechnung ein. Häufige Bonitätsanfragen könnten daher den Bonitätswert verschlechtern.

Die Zulässigkeit einer vorgelagerten Bonitätsabfrage kann auch nicht durch eine pauschale Einwilligung zu Beginn des Zahlungssteuerungsprozesses erreicht werden. Soweit diese in den Allgemeinen Geschäftsbedingungen enthalten ist,

dürfte sie zivilrechtlichen Anforderungen nicht genügen. Zweifel bestehen wegen mangelnder Bestimmtheit und Transparenz der Regeln sowie wegen des Überraschungscharakters. Da eine Bonitätsprüfung nicht erforderlich ist, sofern eine Zahlungsart gewählt wird, die kein finanzielles Ausfallrisiko für die Händlerin oder den Händler mit sich bringt, sehen wir darin auch eine unangemessene Benachteiligung der Kundinnen und Kunden. Zudem zeigt die Erfahrung: Erklärungen zu verlinkten Inhalten („Bonitätsprüfung“) werden von der Kundschaft häufig bestätigt, ohne dass sie sich des Inhalts der abgegebenen Erklärung bewusst sind.

Der bessere Weg wäre, zu Beginn des Bestellprozesses auf verständliche Weise darüber aufzuklären, welche Zahlungswege ein Ausfallrisiko bedeuten und deshalb Bonitätsabfragen erforderlich machen. Eine entsprechende Information kann mit der Erfüllung der Informationspflichten nach § 312j Bürgerliches Gesetzbuch zu den akzeptierten Zahlungsmitteln verbunden werden. Transparenter ist eine deutliche Kennzeichnung derjenigen Zahlungsarten im Bestellmenü, die mit einem finanziellen Ausfallrisiko behaftet sind und bei deren Auswahl eine Bonitätsprüfung erfolgt (zum Beispiel in Tabellenform).

Eine Bonitätsabfrage nach Auswahl einer Zahlungsart mit kreditorischem Risiko ist gemäß §§ 28 und 29 BDSG zulässig. Es bestehen allerdings dennoch die Informationspflichten gemäß § 4 Abs. 3 BDSG und ggf. nach § 13 Telemediengesetz.

Wir haben erreicht, dass durch unsere Intervention in NRW in vielen Fällen auf eine vorgelagerte Bonitätsabfrage vor Auswahl der gewünschten Zahlungsart verzichtet wird. Kundinnen und Kunden raten wir bei der Bestellung genau zu prüfen, ob Bonitätsauskünfte nur nach vorheriger Auswahl einer solchen Zahlungsart erfolgen, die ein finanzielles Ausfallrisiko für den Handel bedeuten können.

15.7 Auskunfteien: Einmeldehinweis von Inkassounternehmen – Rechtsprechung des Bundesgerichtshofs und Praxishinweise

Mit Forderungseinzug beauftragte Stellen – wie Inkassounternehmen und Anwaltskanzleien – können unter bestimmten gesetzlichen Voraussetzungen negative Zahlungserfahrungen mit Schuldnerinnen und Schuldnern an Wirtschaftsauskunfteien übermitteln. Über die Möglichkeit der Einmeldung in eine Auskunftei müssen sie jedoch zuvor die Betroffenen unterrichten. Zu den inhaltlichen Anforderungen an einen solchen Unterrichtungstext hat sich im Jahr 2015 der Bundesgerichtshof (BGH) geäußert. Sinn und Zweck des Einmeldehinweises ist es, den Verbraucherinnen und Verbrauchern aufzuzeigen, dass mit einfachem Bestreiten der Forderung die Datenübermittlung verhindert werden kann. Ein solches Bestreiten ist immer dann angezeigt, wenn die Forderung aus Sicht der Betroffenen unrechtmäßig ist.

Einmeldungen von Negativmerkmalen (zum Beispiel die Nichtzahlung einer Rechnung) bei Wirtschaftsauskunfteien führen zu starken Einschränkungen im Wirtschaftsleben der Betroffenen. Sie sind daher nur unter den engen in § 28a Bundesdatenschutzgesetz (BDSG) genannten Voraussetzungen zulässig. Einmeldevoraussetzungen für offene, nicht titulierte Forderungen sind nach § 28a Abs. 1 Satz 1 Nr. 4 Buchstabe c BDSG unter anderem, dass das Inkassounternehmen die Betroffenen im Vorfeld rechtzeitig über die Möglichkeit einer Übermittlung an die Auskunftei unterrichtet und diese die Forderung nicht bestritten und damit konkludent akzeptiert haben.

Der BGH betont in seinem Urteil vom 19. März 2015 (Az.: I ZR 157/13), dass die Hinweispflicht über die bevorstehende Datenübermittlung im Sinne von § 28a Abs. 1 Satz 1 Nr. 4 Buchstabe c BDSG gerade nicht als zusätzliches Druckmittel zur Durchsetzung einer Forderung verwandt werden darf. Daher müsse die Formulierung des Hinweises in einer Weise erfolgen, die einen solchen Druck ausschließe. Diese Anforderung erfülle nur eine Unterrichtung, mit der deutlich werde, dass ein Bestreiten der Forderung durch die Schuldnerin oder den Schuldner ausreiche, um eine Übermittlung der Schuldnerdaten an eine Wirtschaftsauskunftei zu verhindern.

Zwar sind im Internet grundsätzlich alle Gesetze zugänglich (Homepage des Bundesministeriums der Justiz und für Verbraucherschutz: www.gesetze-im-internet.de). Allerdings hat nicht jede Verbraucherin oder jeder Verbraucher Zugang zum Internet. Der alleinige Hinweis auf eine bevorstehende Einmeldung „unter den Voraussetzungen des § 28a BDSG“ ist deshalb nicht ausreichend. Nicht jede oder jeder hat die Möglichkeit oder ist in

der Lage, sich schnell und einfach zu informieren und ohne großen Aufwand Zugang zur Norm zu erhalten.

Ferner erscheint auch fraglich, ob § 28a BDSG so leicht verständlich ist, dass es keiner Erläuterung bedarf. Schließlich sind in § 28a Abs. 1 BDSG unter den Ziffern 1 – 5 alternative Erlaubnistatbestände normiert. Innerhalb der Ziffer 4 hingegen müssen die Buchstaben a - d kumulativ vorliegen.

Auch darf bezweifelt werden, dass sich der Wortsinn der Norm ohne weiteres erschließt. Eine Übermittlung ist (neben anderen Voraussetzungen) zum Beispiel nur dann zulässig, „wenn der Betroffene die Forderung nicht bestritten hat“. Zwar ist damit erkennbar, dass die Verbraucherin oder der Verbraucher auch selbst die Forderung bestreiten kann. Dennoch dürften sich Unsicherheiten ergeben, ob ein einfaches oder ein qualifiziertes Bestreiten gefordert wird, zumal in der Literatur teilweise und entgegen der Meinung des BGH vertreten wird, dass das Bestreiten substantiierter Natur sein müsse. Wenn schon in Rechtsprechung und Literatur keine einhellige Meinung darüber besteht, welche Tiefe das Bestreiten haben muss, so kann nicht erwartet werden, dass die Empfängerinnen und Empfänger des Einmeldehinweises ein einfaches Bestreiten als ausreichend werten.

Wir haben die Unterrichtungstexte von Inkassounternehmen in NRW stichprobenweise überprüft. Ein Großteil der Unternehmen hat die Unterrichtungstexte nach dem Urteil des BGH angepasst.

Folgende Informationen sollten in jedem Fall deutlich zum Ausdruck kommen:

Aus einem Unterrichtungstext nach § 28a Abs. 1 Satz 1 Nr. 4 Buchstabe c BDSG muss hervorgehen, unter welchen Voraussetzungen an welche konkrete Stelle eine Übermittlung von personenbezogenen Daten erfolgt. Darüber hinaus sollte ebenfalls deutlich werden, dass es sich bei dieser Stelle um eine Wirtschaftsauskunftei handelt. Es ist insbesondere in verständlicher Weise darauf hinzuweisen, dass ein Bestreiten der Forderung durch die Schuldnerin oder den Schuldner selbst ausreicht, um eine Übermittlung von bonitätsverschlechternden Negativmerkmalen an Wirtschaftsauskunfteien zu verhindern.

Im Unterrichtungstext nach § 28a Abs. 1 Satz 1 Nr. 4 Buchstabe c BDSG muss deutlich erkennbar sein, dass ein (rechtzeitiges) Bestreiten der Forderung durch die betroffene Person ausreicht, um eine Einmeldung in eine Wirtschaftsauskunftei zu verhindern.

15.8 Kontrolle von Kundenparkplätzen durch Serviceunternehmen

Parkplätze vor Geschäftszentren sind meistens kostenlos – jedoch nur für die eigene Kundschaft und nur für eine bestimmte Dauer. Die Geschäfte setzen vermehrt auf eine Kontrolle durch private Unternehmen und fordern bei Verstößen nachträglich ein Nutzungsentgelt. Die dafür erforderliche Datenerhebung kann datenschutzrechtlich zulässig sein.

Wenn kostenlose Kundenparkplätze nicht nur für die Dauer des Einkaufes, sondern für längere Zeit oder auch unabhängig vom Einkauf genutzt werden, wird der Parkraum schnell knapp. Um dem entgegenzuwirken, beauftragen die Geschäftsinhaberinnen und -inhaber private Unternehmen mit der Überwachung ihres Parkraums.

Bei der Einfahrt auf dem Parkplatz wird mit Hinweisschildern auf die Nutzungsbedingungen, die Benutzung von Parkscheiben und die Höchstparkdauer hingewiesen. Kundinnen und Kunden werden aufgefordert, unverzüglich die Parkscheibe auf die Ankunftszeit einzustellen und gut sichtbar hinter der Frontscheibe des Autos zu hinterlegen. Die von den Geschäften beauftragten privaten Überwachungsunternehmen kontrollieren, ob die Parkscheibe genutzt und die Höchstparkdauer eingehalten wird. Zur Beweisführung werden die folgenden Daten erhoben: Kennzeichen, Typ und Farbe des Fahrzeugs, Parkplatz, Uhrzeit sowie Fotos vom Fahrzeug; vor allem von der Windschutzscheibe und dem Armaturenbrett zum Nachweis, ob eine Parkscheibe angebracht wurde.

Wurde gegen die Nutzungsbedingungen verstoßen, wird eine Zahlungsaufforderung, vergleichbar mit einem Kassenbon, am Fahrzeug angebracht. Diese enthält eine Info-Hotline, über die weitere Informationen sowie ein Link auf die Beweisfotos erhältlich sind. Die Fotos sind nicht frei zugänglich und werden von der Überwachungsfirma auch nicht in soziale Netzwerke eingestellt.

Wird nicht innerhalb eines mehrwöchigen Zeitraums gezahlt, erfolgt eine Halterabfrage beim Kraftfahrt-Bundesamt (KBA). Anschließend werden ggf. Zahlungserinnerungen und Mahnungen versandt sowie die Forderung an ein Inkassounternehmen zur Beitreibung der Forderung abgegeben.

Das Überwachungsunternehmen handelt im Auftrag des Geschäfts- und Parkplatzinhabers ausschließlich zivilrechtlich. Es wird nicht amtlich tätig. Gemäß § 858 Abs. 1 Bürgerliches Gesetzbuch handelt widerrechtlich, wer dem Besitzer ohne dessen Willen den Besitz entzieht oder ihn im Besitz stört, sofern nicht das Gesetz die Entziehung oder die Störung gestattet. Wird das Fahrzeug entgegen den Parkplatz-Nutzungsbedingungen – also widerrechtlich – abgestellt, ist dies eine

verbotene Eigenmacht in diesem Sinne. Mittels der Maßnahmen zur Beweissicherung und der Zahlungsaufforderung setzt der Geschäftsinhaber sein Besitz- oder Eigentumsrecht (Hausrecht) durch. Sofern Fahrzeuge auf diesen beschilderten Kundenparkplätzen abgestellt werden, akzeptiert die Fahrerin oder der Fahrer die Parkplatzordnung und geht damit einen Nutzungsvertrag ein.

Die dafür erforderliche Datenerhebung ist nach § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 Bundesdatenschutzgesetz zulässig. Durch die Hinweise bei der Einfahrt und beim Parken sowie durch das abgestufte Vorgehen sind die Interessen der Betroffenen ausreichend gewahrt.

Auch die Halterauskunft beim Kraftfahrt-Bundesamt oder bei der Zulassungsbehörde kann zulässig sein. Für eine Halteranfrage im Wege der einfachen Registerauskunft nach § 39 Abs. 1 Straßenverkehrsgesetz ist lediglich die Darlegung erforderlich, dass „die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt“ werden.

Gegründet auf den Nutzungsvertrag für den Parkraum hat der Parkrauminhaber einen Anspruch auf ein erhöhtes Nutzungsentgelt. Zur Durchsetzung dieses zivilrechtlichen Anspruchs benötigt er die Halterdaten. Damit ist er zur Abfrage berechtigt.

Vor der Einfahrt auf den Parkplatz sollten die Fahrerinnen und Fahrer auf die Hinweisschilder zur Nutzung des Parkplatzes achten. Die privaten Überwachungsfirmen haben dafür zu sorgen, dass Beweisfotos nur die für die Anspruchsdurchsetzung notwendigen Informationen abbilden. Weitere personenbezogene Inhalte – etwa auf dem Armaturenbrett liegende Fotos, Ausweise, Schriftstücke – sind zu schwärzen. Datenerhebungen im Zusammenhang widerrechtlich geparkter Fahrzeuge können unter Beachtung dieser Voraussetzungen zulässig sein.

15.9 Private Nachhilfeinstitute – Einschätzung der Bonität der Eltern anhand eines Bewertungsbogens

Verwundert waren Eltern als sie erfuhren, dass ein privates Nachhilfeinstitut sich bei Hausbesuchen nicht nur für die Kinder, sondern auch für die häusliche Einrichtung interessiert. Anhand eines Bewerbungsbogens sollte so die Bonität ermittelt werden. Dieses Verhalten ist nicht nur datenschutzrechtlich bedenklich.

Fachberaterinnen und Fachberater des Nachhilfeinstituts waren aufgerufen, nach dem Kundenbesuch eine Checkliste auszufüllen. Diese Liste enthielt zunächst eine Einschätzung zur „persönlichen Arbeitshaltung des Schülers“ sowie eine Beurteilung der Eltern, ob diese „sehr nett und offen, neutral oder schwierige Leute sind und man mit ihnen gut zu Recht kommt“. Dann folgten Angaben zu den folgenden Merkmalen:

- in welcher „Art von Immobilie“ die Familie lebt,
- welchen Zustand die „Einrichtung (Möbel etc.)“ hat und
- wie viele und welcher „Pkw“ genutzt wird.

Die Fachberaterin oder der Fachberater gaben anhand der genannten Merkmale eine subjektive Bewertung ab, von der das Unternehmen dann die Bonität ableitete. Die interessierten Eltern wussten weder von der Existenz dieses Bewertungsbogens noch wurden sie über diese Einschätzung befragt oder informiert.

Mit diesem Bewertungsbogen forschte das Unternehmen den Privatbereich der Eltern aus. Auch hätten die erfassten Daten missbräuchlich – zum Beispiel für Wohnungseinbrüche – verwandt werden können, wenn sie in die Hände unbefugter Dritter gelangt wären.

Auf unsere Nachfrage teilte das Nachhilfeinstitut mit, dass die Angaben für die Einschätzung der Bonität der Vertragspartnerinnen und Vertragspartner benötigt würden, da das Institut ausnahmslos Vorleistungen erbringe.

Diese Geschäftspraxis verstieß gegen den Datenschutz. Eine wirksam erteilte Einwilligung der Betroffenen lag nicht vor. Eine gesetzliche Erlaubnis für die Verarbeitung war auch nicht gegeben. So waren die in dem Bewertungsbogen erhobenen Daten weder für die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit den Betroffenen erforderlich. Auch überwogen die schutzwürdigen Interessen der Eltern, da ohne deren Wissen und Mitwirkung eine subjektive Wahrnehmung und Bewertung ihres Privatbereichs erfolgte und dieses verschriftlicht wurde.

Wir haben das Nachhilfeinstitut darauf hingewiesen, dass der interne Bewertungsbogen unzulässig ist und aufgefordert, die bereits ausgefüllten Bögen zu vernichten.

Statt einer Bonitätsauskunft hinter dem Rücken der Betroffenen kann vor Beginn der Nachhilfe eine einmalige Anmeldegebühr im Voraus verlangt werden, die eventuell nach einer bestimmten geleisteten Stundenzahl verrechnet wird.

Wir fordern – gerade auch die kleinen und mittelständischen – Unternehmen auf, ihre Datenerhebung stets auf das Notwendige zu beschränken. Eine Ausforschung des privaten Lebensbereichs zur Feststellung von Bonität ist unzulässig.

15.10 Unverschlüsselte E-Mail-Kommunikation zwischen Versicherungskunden und Versicherungsunternehmen

Versicherungsunternehmen berichten, dass eine große Anzahl der Versicherten an einer Kommunikation per E-Mail interessiert sei. Viele wären aber nicht bereit, dabei Angebote der Versicherungen wie Ende-zu-Ende-Verschlüsselung oder alternativ die Kommunikation über ein sicheres Internet-Portal zu nutzen. Stattdessen verlangen die Kundinnen und Kunden von ihren Versicherungen, eine zügige und unkomplizierte Korrespondenz ohne Verschlüsselung.

Diese Anforderung bringt die Versicherungen in einen Interessenkonflikt: Einerseits müssen sie kundenfreundlich agieren. Andererseits verlangt § 9 Bundesdatenschutzgesetz von ihnen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Daten unter anderem vor unbefugtem Zugriff zu schützen und dabei den Stand der Technik einzuhalten. Weichen sie hiervon ab, trifft sie das Risiko aufsichtsrechtlicher Maßnahmen. Auch der ausdrückliche Verzicht der Versicherten auf sichere Kommunikationswege ist keine Lösung, denn in eine solche Absenkung des Schutzniveaus kann nicht wirksam eingewilligt werden.

Auf eine Verschlüsselung verzichten zu wollen, ist aus Kundensicht auch nicht ratsam. Eine unverschlüsselte E-Mail ist lesbar wie eine Postkarte. Gerade in der Kommunikation mit Versicherungen geht es aber oft um besonders schützenswerte Daten wie Informationen über die Gesundheit oder den Finanzstatus. Das Interesse Dritter an diesen Daten und das damit verbundene Risiko sollten nicht unterschätzt werden.

Wir raten daher dazu, technische Möglichkeiten, die die Datenübertragung sicher machen, unbedingt zu nutzen. Diese sind heutzutage auch benutzerfreundlich und nicht mehr allzu kompliziert.

Versicherungen sollten den Kundenwünschen nach unverschlüsselter Kommunikation per E-Mail mit Hilfestellungen zu sicheren Kommunikationswegen wie Ende-zu-Ende-Verschlüsselung entgegenkommen. Kundinnen und Kunden sollten diese Angebote als eine unerlässliche Vorsichtsmaßnahme zum Selbstdatenschutz in ihrem eigenen Interesse anwenden.

15.11 Beschränkung des Bargeldverkehrs

Immer wieder fordern nationale und internationale Stimmen aus Politik und Finanzwirtschaft, die Möglichkeit der Barzahlung einzuschränken. Die Bestrebungen reichen von der Abschaffung von 500-Euro-Scheinen über die Einführung einer Obergrenze für Bargeldgeschäfte bis zur kompletten Abschaffung des Bargelds. Bürgerinnen und Bürger die Wahlfreiheit zu nehmen, auch anonym zahlen zu können, stellt einen erheblichen Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung dar.

Der Landtag NRW hat sich mit zwei Fraktionsanträgen zu Bargeldobergrenzen befasst (LT-Drs. 16/12815). Zu der öffentlichen Anhörung am 3. Mai 2016 hat der Haushalts- und Finanzausschuss des Landtags die Landesbeauftragte für Datenschutz und Informationsfreiheit eingeladen. Wir haben diese Gelegenheit gerne genutzt und uns gegen jegliche Einschränkung des Bargeldverkehrs ausgesprochen (APr 16/1275). Unsere schriftliche Stellungnahme ist auf unserer Internetseite www.ldi.nrw.de abrufbar.

Aus dem Grundrecht der informationellen Selbstbestimmung ergibt sich das Recht des Einzelnen, selbst über die Verwendung seiner persönlichen Daten zu bestimmen. Der Zwang zur Verwendung bargeldloser Zahlungsmittel – generell oder ab einer bestimmten Höhe des Transfers – schränkt diese Freiheit ein. Bei jeder bargeldlosen Bezahlung werden zwangsläufig Zahlungsbewegungen elektronisch registriert und gespeichert. Hinter jedem Zahlungsvorgang steht dabei immer die einzelne Person. Je mehr Zahlungsbewegungen erfolgen, desto einfacher ist es, ein Profil zu erstellen – mit Vorlieben und Interessen. Aus dem Wissen über die Zeit und den Ort einer Zahlung können zudem detaillierte Bewegungsprofile entstehen. Diese Daten sind für Unternehmen von hohem Nutzen. Auch staatliche Stellen haben ein hohes Interesse daran, auf die Daten der Bürgerinnen und Bürger zuzugreifen.

Eine Einschränkung der Barzahlung führt zu einer Datenverarbeitung, die den Grundsätzen der Datenvermeidung und Datensparsamkeit nicht entspricht, und stellt einen Grundrechtseingriff dar.

Ein solcher Eingriff kann gerechtfertigt sein, wenn er zur Erreichung der damit verfolgten Ziele erforderlich und verhältnismäßig ist. Erklärte Ziele der Einschränkung der Barzahlungen sollen vor allem die Bekämpfung von Schwarzarbeit, Geldwäsche und Steuerhinterziehung sowie von Terrorismusfinanzierung sein. Unserer Wahrnehmung nach konnte bisher nicht nachgewiesen werden, dass die mit einer Bargeldbeschränkung verbundene unvermeidbare Erfassung und verdachtslose Registrierung von Zahlungsvorgängen für diese Zwecke wirklich geeignet, erforderlich und angemessen sind. Jedenfalls liegt

die Vermutung nahe, dass diejenigen, die sich im Bereich der genannten Straftaten bewegen, die in Rede stehenden Grenzen wohl kaum einhalten oder auf andere Wege der Finanzierung ausweichen würden.

Mit Bargeld zu zahlen hinterlässt keine Datenspuren, die möglicherweise Rückschlüsse auf ein Kaufverhalten und Interessen möglich machen. Die Zahlung mit Bargeld sichert den Zahlenden Privatsphäre und Anonymität zu. Sie ist weder antiquiert noch verdächtig, sondern die aktive Inanspruchnahme von Freiheitsrechten. Auch wenn die komplette Abschaffung des Bargeldes schwerer wiegen würde als eine Begrenzung, zeigt ein Blick in andere Länder, dass häufig zunächst ein Barzahlungslimit festgesetzt und dieses in der Folgezeit immer weiter herabgesetzt wurde. Der Schritt zur völligen Abschaffung ist dann nicht mehr weit. Deswegen sind bereits Bargeldobergrenzen abzulehnen.

Jede Art der Einschränkung der Wahlfreiheit der Bürgerinnen und Bürger auch anonym zahlen zu können, begegnet starken verfassungsrechtlichen und datenschutzrechtlichen Bedenken und ist kritisch zu sehen.

15.12 Ermittlung von Wohnungsleerstand durch Kommune beim Versorgungsunternehmen

Informationen der Energieversorger zu leerstehenden Wohneinheiten sowie den Namen und Adressen der betreffenden Eigentümerinnen und Eigentümer sind interessant – auch als Planungsgrundlage für Kommunen. Eine Weitergabe ist jedoch ohne Einwilligung unzulässig.

Energieversorger können den Leerstand einer Wohneinheit erkennen, wenn ein so genannter Leerstandstarif vereinbart wurde oder wenn in einem bestimmten Zeitraum kein Strom verbraucht wurde. Eine Kommune wollte diese Informationen nutzen, um Konzepte für die Verbesserung der Wohnraumsituation zu erarbeiten und um Eigentümerinnen und Eigentümer leerstehender Wohneinheiten gezielt anzusprechen. Die Übermittlung der Daten an eine Kommune für diesen Zweck ist ohne Einwilligung der Vertragspartnerinnen und -partner des Energieversorgers jedoch nicht zulässig.

Eine Datenübermittlung auf der Grundlage von § 28 Abs. 2 Nr. 2 Buchstabe a Bundesdatenschutzgesetz kommt nicht in Betracht. Danach müsste die Übermittlung erforderlich zur Wahrung berechtigter Interessen Dritter sein. Außerdem dürfte kein Grund zu der Annahme bestehen, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.
Zwar ist ein berechtigtes Interesse der Kommune anzunehmen, leerstehende Wohneinheiten zu identifizieren und die betreffenden Eigentümerinnen und Eigentümer zu kontaktieren. Letztere haben jedoch ein schutzwürdiges Interesse, dass ihre Daten und Informationen über die Nutzung bzw. Nichtnutzung ihres Eigentums nicht an Dritte weitergegeben werden – und dies wiegt höher als das Interesse der Kommune. Das gilt insbesondere, weil keinerlei Verbindung zu dem Zweck besteht, zu dem die Daten ursprünglich erhoben wurden, nämlich die Vertragsabwicklung mit dem Versorgungsunternehmen.

Wir haben den Energieversorger deshalb darauf hingewiesen, dass eine Weitergabe der Kundendaten ohne ausdrückliche Einwilligung der Betroffenen unzulässig ist.

16. Informationsfreiheit

16.1 NRW-Vorsitz in den bundesweiten Gremien zur Informationsfreiheit

Im Jahr 2016 hatte NRW den Vorsitz in der „Konferenz der Informationsfreiheitsbeauftragten in Deutschland“ (IFK). Vorbereitet wurden die Sitzungen, die turnusmäßig zweimal im Jahr stattfinden, durch den „Arbeitskreis Informationsfreiheit“ (AKIF), ebenfalls unter Vorsitz der LDI NRW.

Die IFK ist ein Zusammenschluss der Informationsfreiheitsbeauftragten des Bundes und der Länder mit dem Ziel, das Recht auf Informationszugang zu fördern und gemeinsam für seine Fortentwicklung einzutreten. Der Vorsitz wechselt jährlich.

Auf der ersten Sitzung konnte ein neues Mitglied begrüßt werden: Mit dem Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg vom 17. Dezember 2015 und der darin normierten Übertragung der Aufgabe des Informationsfreiheitsbeauftragten wurde der Landesbeauftragte für den Datenschutz Baden-Württemberg Mitglied der IFK. Noch immer gibt es bedauerlicherweise vier Länder – Bayern, Hessen, Niedersachsen und Sachsen –, in denen es nach wie vor kein Gesetz gibt, das den Zugang zu Informationen bei öffentlichen Stellen regelt – sei es auf der Basis eines Antrages, sei es antragslos im Rahmen eines Transparenzgesetzes. In der Folge gibt es in diesen Ländern auch nicht die Funktion einer oder eines Informationsfreiheitsbeauftragten. Die IFK hat wiederholt angemahnt, diese gesetzgeberischen Lücken in den Ländern zu schließen.

Im Vorsitzjahr 2016 ging es inhaltlich schwerpunktmäßig darum, gemeinsam auf Weiterentwicklungen in Sachen Transparenz, proaktive Veröffentlichung und Open Data hinzuwirken sowie begonnene Fortentwicklungen zu unterstützen und voranzutreiben.

Am 28. April 2016 verabschiedete die IFK in Form eines Umlaufbeschlusses die Entschließung „Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!“.

Am 15. Juni 2016 folgte auf der ersten Sitzung in NRW die Entschließung „GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!“.

Auf der zweiten Sitzung am 2. Dezember 2016 wurde die Entschließung: „Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!“ verabschiedet.

Die Entschließungen sind im Anhang abgedruckt und auf unserer Internetseite www.ldi.nrw.de abrufbar.

Außerdem gab sich die IFK mit Beschluss vom 2. Dezember 2016 eine Geschäftsordnung (GO IFK). Der Beschluss vom 2. Dezember 2016 ist im Anhang abgedruckt und auf unserer Internetseite www.ldi.nrw.de abrufbar. Ein wichtiges Ziel war es dabei, den ursprünglichen „Modus der Öffentlichkeit“ in das neue Regelwerk zu integrieren und die öffentliche Ausrichtung der IFK und des AKIF fortzuentwickeln. Die Informationsfreiheitsbeauftragten in Deutschland wollen und werden auch weiterhin in Sachen Transparenz und Open Data mit gutem Beispiel vorangehen: Alle Sitzungen der Konferenz und des Arbeitskreises sind grundsätzlich öffentlich, und die Tagesordnungen und Protokolle beider Gremien, die Positionen der IFK sowie die GO IFK werden regelmäßig im Internet auf den Webseiten der Mitglieder veröffentlicht.

Am 1. Januar 2017 ging der Vorsitz auf Rheinland-Pfalz über. Der IFK und dem AKIF werden die Themen auch weiterhin nicht ausgehen, denn nach wie vor gibt es im Bereich von Informationsfreiheit, Transparenz und Open Data sehr viel Handlungs-, Fortentwicklungs- und Regelungsbedarf.

16.2 Transparenzgesetz NRW?

Was ist aus dem Vorhaben der Landesregierung geworden, das Informationsfreiheitsgesetz NRW (IFG NRW) zu einem Transparenzgesetz NRW weiterzuentwickeln?

Mit dieser Frage befasste sich bereits der Bericht 2015 unter 12.1. Die Antwort ist zum gegenwärtigen Zeitpunkt ebenso einfach wie ernüchternd: Nichts. Es gibt nach wie vor kein Transparenzgesetz in NRW, das diesem Namen im informationsfreiheitsrechtlichen Sinne gerecht würde.

Es gab zwar Entwicklungen auf diesem Gebiet, aber die neu geschaffenen oder aktuell angekündigten Einzelregelungen verstärken die bereits seit langem festzustellende Tendenz zur Rechtszersplitterung. Der „große Wurf“ ist in Sachen Transparenz nach wie vor nicht in Sicht. Zudem tragen die Bezeichnungen der Gesetze zum Teil eher zur Irritation als zur Klarstellung für die Bürgerinnen und Bürger bei.

Im Einzelnen:

- Das am 1. Januar 2002 in Kraft getretene IFG NRW hat sich bewährt, regelt allerdings ausschließlich den allgemeinen Anspruch auf Zugang zu amtlichen Informationen, der mittels eines entsprechenden Antrags geltend zu machen ist. Ausnahme ist die Pflicht zur Veröffentlichung von Geschäftsverteilungsplänen, Organigrammen und Aktenplänen (§ 12 IFG NRW).

- Zweck des Umweltinformationsgesetzes NRW (UIG NRW) vom 29. März 2007 ist es, den rechtlichen Rahmen für den freien Zugang zu Umweltinformationen bei informationspflichtigen Stellen sowie für die Verbreitung dieser Umweltinformationen zu schaffen. Gegenstand der Regelung ist also der Umgang mit Umweltinformationen. Nach wie vor besteht das UIG NRW neben dem IFG NRW, was die Rechtsanwendung weder für die verantwortlichen Stellen noch für die Anspruchsberechtigten erleichtert.

- Gleiches gilt für weitere Einzelregelungen, die in verschiedenen Gesetzen Teilaspekte von Informationsfreiheit und/oder Transparenzbelangen betreffen. Wer hat hier noch einen Überblick?

- Die Bezeichnung „Transparenzgesetz “ ist in NRW bereits seit dem 17. Dezember 2009 besetzt. Die Kurzbezeichnung täuscht jedoch leicht darüber hinweg, dass es sich hierbei um das „Gesetz zur Schaffung von mehr Transparenz in öffentlichen Unternehmen im Lande Nordrhein-Westfalen (Transparenzgesetz)“ handelt. Das Gesetz regelt die Offenlegung von Vergütungen in verschiedensten Bereichen. Auch dies betrifft einen wichtigen, aber ebenfalls nur punktuellen Transparenzaspekt. Geändert wurden mit dem Artikelgesetz mehrere andere

Rechtsvorschriften, so dass sich Regelungen zur Offenlegung von Vergütungen heute in verschiedenen Gesetzen finden oder manchmal vielleicht auch nicht so leicht finden lassen.

- Nach einem Beschluss der Regierungschefs von Bund und Ländern vom 14. Oktober 2016 sollen so genannte „Open-Data-Gesetze“ erlassen und dabei bundesweit vergleichbare Standards für den Zugang zu öffentlichen Datenpools verankert werden. Auch wenn die Zielrichtung des Beschlusses ausdrücklich zu begrüßen ist: Wiederum geht es ausschließlich um einen Teilaspekt der Veröffentlichung amtlicher Informationen. Geregelt werden soll die Veröffentlichung von so genannten „Rohdaten“, die von enormem wirtschaftlichen Wert sein können.

Die stetig wiederholte Forderung nach Transparenz öffentlichen Handelns ist jedoch in viel umfassenderem Sinne zu verstehen. Gemeint ist hiermit nicht nur (aber auch) die Veröffentlichung amtlicher Rohdaten, sondern darüber hinaus auch die Veröffentlichung von zusammenhängenden, aus sich heraus nachvollziehbaren Unterlagen, wie zum Beispiel Verträgen, Gutachten, Studien, Berichten, Konzepten, Richtlinien, Erlassen.

In NRW ist endlich das IFG NRW zu dem bereits seit langem in Aussicht gestellten Transparenzgesetz fortzuentwickeln. Hier ist sowohl ein individueller, antragsgebundener Informationszugangsanspruch vorzusehen als auch die Verpflichtung öffentlicher Stellen, bestimmte Informationen und Dokumente von sich aus und antragsunabhängig im Internet zu veröffentlichen. In ein solches Transparenzgesetz sollten insbesondere auch die oben angesprochenen Open-Data-Regelungen zur Veröffentlichung von Rohdaten wie auch die Vorschriften des UIG NRW integriert werden.

Da es vergleichbare Probleme bundesweit gibt, hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland unter dem Vorsitz der LDI NRW die Entschließung „Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!“ am 2. Dezember 2016 (Abdruck im Anhang) verabschiedet. Damit wiederholt und verstärkt die Konferenz ihre langjährige Forderung, endlich in Bund und allen Ländern umfassende Transparenzgesetze zu erlassen.

16.3 Antworten auf FragDenStaat

Lange Zeit gab es offene Fragen zum Umgang mit elektronischen Anträgen auf Informationszugang nach dem Informationsfreiheitsgesetz NRW (IFG NRW), die über die Internetplattform www.fragdenstaat.de gestellt wurden. Befriedigende Antworten konnten wir nunmehr gemeinsam mit FragDenStaat sowie dem Innenministerium NRW finden.

Bereits der Bericht 2015 zielte unter 12.3 darauf, die bestehenden Unsicherheiten öffentlicher Stellen aufzugreifen und auszuräumen. Wie die Stellungnahme der Landesregierung vom 22. Dezember 2015 (LT-Drs.16/3580) und die anschließende Erörterung im Innenausschuss am 18. Februar 2016 (APr 16/1161) zeigte, gab es jedoch noch Klärungsbedarf.

Im April 2016 fand auf unsere Initiative im Hause der LDI NRW eine gemeinsame Besprechung mit dem Innenministerium NRW sowie den Betreibern der Internetplattform statt. Die Funktions- und Arbeitsweise von FragDenStaat wurde dabei ausführlich erläutert.

FragDenStaat erklärte zunächst noch einmal eingehend das Ziel des Projekts sowie den Ablauf und die Verantwortlichkeiten einer Antragstellung über diese Plattform. Es wurde ausdrücklich klargestellt, dass die bzw. der Antragstellende jederzeit die Hoheit über das Verfahren habe und mithin auch selbst darüber entscheide, ob der Antrag öffentlich gestellt werde oder nicht. Weiter wurde klargestellt, dass die Plattform eine eigene E-Mail-Adresse generiere, über die die Kommunikation zwischen FragDenStaat und Behörde abgewickelt werde. Über die eigene E-Mail-Adresse müsse der Antrag noch einmal bestätigt werden, so dass sichergestellt werden könne, dass nicht eine fremde E-Mail-Adresse verwendet werde. Vorformulierte Texte könnten der informationssuchenden Person zwar helfen, die richtige Zugangsnorm für den Antrag zu verwenden, die Texte seien jedoch von dieser auch veränderbar.

Besonders ausführlich wurde die Frage des Schutzes der Daten der Beschäftigten erörtert, die die entsprechenden Dokumente bearbeitet oder unterschrieben haben. So wies das Innenministerium NRW darauf hin, dass in der Vergangenheit behördliche Schreiben mit den Namen der Bearbeiterinnen und Bearbeiter im Internet veröffentlicht worden seien; es sei sehr schwierig oder gar unmöglich für die betroffenen Beschäftigten gewesen, sich gegen eine solche Veröffentlichung zu wehren. FragDenStaat stellte hierzu klar, dass bei einer öffentlichen Antragstellung die Antwort-E-Mail der verantwortlichen Stelle zwar veröffentlicht werde, die personenbezogenen Daten der Beschäftigten inzwischen jedoch zuvor durch einen Algorithmus geschwärzt würden. Angehängte pdf-Dokumente, die ebenfalls personenbezogene Daten enthalten und nicht

automatisch geschwärzt werden könnten, würden nicht automatisiert veröffentlicht. Die Plattform stelle ein Tool zur Schwärzung bereit; die Schwärzung selbst müsse indes von den Antragstellenden erfolgen. Es bestehe ferner für auskunftspflichtige Stellen oder die betroffenen Beschäftigten die Möglichkeit, sich unmittelbar an FragDenStaat zu wenden, wenn die Schwärzung der Beschäftigtendaten im Dokument durch die oder den Antragstellenden unterblieben sei. Das Verfahren sei in dieser Weise inzwischen geändert worden; die personenbezogenen Daten würden auf Wunsch sodann zeitnah gelöscht.

Im Nachgang zu dieser Besprechung wurde die Thematik anlässlich des Antrags einer Fraktion „Informationsfreiheit schützen – Transparenz und einfachen Zugang zu staatlichen Informationen sicherstellen“ (LT-Drs. 16/11219) in der Sitzung des Innenausschusses des Landtags NRW am 30. Juni 2016 noch einmal erörtert (vgl. APr 16/1364, S. 12 ff.). Im Ausschuss stellte die Landesregierung ausdrücklich klar, dass Anträge, die über die Internetplattform FragDenStaat gestellt werden, grundsätzlich beantwortet werden. Grundlegende Bedenken seien in der gemeinsamen Besprechung mit FragDenStaat und der LDI NRW ausgeräumt worden.

Verantwortliche Stellen, an die über FragDenStaat eine Anfrage nach dem IFG NRW gerichtet wird, haben bei ihrer Prüfung Folgendes zu berücksichtigen:

- Gemäß § 4 Abs. 1 IFG NRW hat jede natürliche Person grundsätzlich einen Anspruch auf Zugang zu den bei einer öffentlichen Stelle vorhandenen Informationen.

- § 5 Abs. 1 Satz 2 IFG NRW sieht ausdrücklich vor, dass Anträge auch in elektronischer Form gestellt werden können.

- Die Ablehnung eines Informationszugangsantrags allein aus dem Grund, dass er über FragDenStaat gestellt worden ist, ist deshalb unzulässig.

Aus datenschutzrechtlichen Gründen darf die auskunftspflichtige Stelle personenbezogene Daten, insbesondere die Adresse der Antragstellerinnen und Antragsteller, nur und erst dann erheben, wenn dies zu ihrer Aufgabenerfüllung nicht nur nützlich oder dienlich, sondern sogar erforderlich ist. Dies kommt insbesondere in folgenden Fallgruppen in Betracht:

1. Erlass eines Gebührenbescheids

2. Erlass eines Ablehnungsbescheids, wenn die Antragstellerinnen und -steller Rechtsmittel einlegen wollen

3. materiell-rechtliche Gründe, vor allem Geltendmachung eines rechtlichen Interesses oder Vorliegen der erforderlichen Einwilligung zur Weitergabe von personenbezogenen Daten

4. Zusendung von Informationsmaterial per Post (beispielsweise CD-ROM)

Konkrete Beispielfälle hierzu finden sich bereits im Bericht 2015 unter 12.3.

Anfragen auf Informationszugang, die über die Internetplattform FragDenStaat gestellt werden, sind grundsätzlich zu beantworten. Nur wenn und soweit es zur Aufgabenerfüllung der informationspflichtigen Stelle erforderlich ist, dürfen personenbezogene Daten der informationssuchenden Person erhoben werden.

16.4 Veröffentlichung von Gutachten der Wissenschaftlichen Dienste des Bundestags und der Landesparlamente

Seit Februar 2016 veröffentlicht der Deutsche Bundestag die Gutachten seiner Wissenschaftlichen Dienste. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Landesparlamente auf, dem Beispiel zu folgen.

Nach der aktuellen Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 25. Juni 2015, Az. 7 C 1/14) muss die Bundestagsverwaltung auf Antrag Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste gewähren. Die Gutachten sind nach Ansicht des Bundesverwaltungsgerichts nicht unmittelbar der geschützten Tätigkeit der Abgeordneten zuzuordnen und daher auf Anfrage herauszugeben. Mittlerweile veröffentlicht die Bundestagsverwaltung die Ausarbeitungen der Wissenschaftlichen Dienste generell vier Wochen nach Auslieferung an die auftraggebenden Abgeordneten im Internet. Eines Antrags bedarf es damit nicht mehr.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat daher mit der Entschließung „Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!“ vom 28. April 2016 die Landesparlamente aufgefordert, dem Beispiel der Bundestagverwaltung in Sachen Transparenz und Open Data zu folgen. Die Entschließung ist auf unserer Homepage www.ldi.nrw.de abrufbar und im Anhang abgedruckt.

Wir haben dem Landtag NRW die Entschließung zugeleitet und mit der Landtagspräsidentin erörtert. Der Landtag in NRW verfährt bereits ähnlich wie die Bundestagsverwaltung: In der Geschäftsordnung des Landtags ist geregelt, dass die Ausarbeitungen des Parlamentarischen Beratungs- und Gutachterdienstes grundsätzlich auch anderen Interessenten zur Verfügung gestellt werden (Grundsatz der Allgemeinzugänglichkeit), sofern nicht in besonderen Fällen eine vertrauliche Behandlung beansprucht wird oder sich aus den Umständen ergibt. Nach Ablauf der jeweiligen Legislaturperiode gilt auch in dem Fall, dass eine vertrauliche Behandlung beansprucht wird, der Grundsatz der Allgemeinzugänglichkeit. Auch ohne dass ein entsprechender Antrag vorliegt, werden die Gutachten in dem der Geschäftsordnung entsprechenden Umfang in einer Datenbank proaktiv veröffentlicht.

Die Veröffentlichungen des Bundestages sowie die langjährig geübte Praxis des Landtags NRW sind gute Schritte in Richtung transparenten Verwaltungshandelns.

16.5 GovData – das Datenportal für Deutschland

GovData ist ein Metadatenportal, über das Bund, Länder und Kommunen offene Daten wie etwa Statistiken, Geodaten oder Organigramme allgemein zugänglich machen. Sinnvoll ist dieses Portal allerdings nur, wenn sich möglichst viele öffentliche Stellen aktiv daran beteiligen.

GovData basiert auf einer Verwaltungsvereinbarung, der bislang noch nicht alle Länder beigetreten sind. Das Ziel dieser Vereinbarung ist es, standardisiert und gebündelt Daten der öffentlichen Hand über eine gemeinsame Infrastruktur leicht auffindbar bereitzustellen. Nutznießende der Vereinbarung sind sowohl Bürgerinnen und Bürger als auch Wirtschaft und Wissenschaft sowie die Verwaltung selbst. Die mit GovData bewirkte Transparenz der Verwaltung fördert die Teilhabe, das heißt die Einbeziehung der Gesellschaft in staatliche Entscheidungsprozesse, die Zusammenarbeit von staatlichen Stellen untereinander sowie des Staates mit gesellschaftlichen Gruppen.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder sehen in GovData dementsprechend einen wichtigen Beitrag zu mehr Transparenz und zum Ausbau von Open Data. Sie fordern daher in der gemeinsamen Entschließung „GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!“ vom 15. Juni 2016 (Abdruck im Anhang) eine umfassendere und aktive Teilnahme an dem Portal.

Verbesserungsbedürftig ist neben der aktiven Beteiligung der Verwaltung der Bekanntheitsgrad des Portals: Der Antwort der Bundesregierung auf eine Kleine Anfrage zum Entwicklungsstand des Portals zufolge haben in den ersten acht Monaten des Jahres 2015 im Durchschnitt gerade einmal 8.180 unterschiedliche Besucherinnen und Besucher pro Monat auf die Seite www.govdata.de zugegriffen (siehe BT-Drs. 18/6027).

GovData ist ein guter Schritt in die richtige Richtung und bedarf der Weiterentwicklung und des Ausbaus – sowohl durch bereits amtierende als auch noch zu gewinnende Akteurinnen und Akteure. Übrigens: NRW zählt zu den Teilnehmenden der ersten Stunde.

16.6 Offenlegung von Kooperationsverträgen zwischen Hochschulen und Unternehmen

Das Oberverwaltungsgericht NRW hat entschieden, dass eine Universität ihre Kooperationsvereinbarung mit einem Pharmaunternehmen nicht offenlegen muss. Die gerichtliche Auseinandersetzung ist damit beendet – die Diskussion über mehr Transparenz bei der Finanzierung von Forschungsvorhaben geht jedoch weiter.

Bereits im Bericht 2011 unter 16.1 wurde über diesen Fall berichtet. Das OVG NRW hat nunmehr in letzter Instanz entschieden, dass der sachliche Anwendungsbereich des Informationsfreiheitsgesetzes NRW (IFG NRW) nicht eröffnet sei (Urteil vom 18. August 2015, Az. 15 A 97/13). Die streitgegenständliche Kooperationsvereinbarung unterfalle dem Bereich von Forschung und Lehre, der nach § 2 Abs. 3 IFG NRW vom Anwendungsbereich des IFG NRW ausgenommen sei. Um zu verhindern, dass es durch einen Informationszugang zu einer Gefährdung der Grundrechtspositionen von Wissenschaft und Forschung komme, sei der Begriff „Forschung und Lehre“ im Sinne der Norm ebenso weitreichend zu verstehen wie derjenige der Wissenschaftsfreiheit des Grundgesetzes. Neben der wissenschaftlichen Erkenntnisgewinnung durch Forschung umfasse der Begriff auch wissenschaftsrelevante Angelegenheiten wie etwa Drittmittelverträge und ähnliche organisatorische Vorkehrungen für Forschungsvorhaben.

Aktualität hat das Thema in der Öffentlichkeit noch einmal durch eine Sachverständigenanhörung im Innenausschuss und Ausschuss für Innovation, Wissenschaft und Forschung des Landtags NRW erhalten. In ihrem zeitlich unmittelbar auf das Urteil des OVG NRW folgenden Antrag „Informationsfreiheit darf nicht an der Universitätstür Halt machen!“ hatte eine Landtagsfraktion mehr Transparenz in diesem Bereich gefordert (LT-Drs. 16/9589). Angeregt wurden unter anderem eine Präzisierung des § 71a Hochschulgesetz NRW (HG NRW) sowie eine gesetzliche Regelung zur Veröffentlichung von Forschungskooperationsverträgen. In der Anhörung haben wir die Forderung nach einer konkreteren Veröffentlichungspflicht ausdrücklich begrüßt und erneut darauf hingewiesen, dass die vor zwei Jahren neu ins HG NRW aufgenommene Transparenzregel des § 71a konkrete Parameter wie etwa Namen der Drittmittelgeberinnen und -geber, Förderumfang und Projektlaufzeit vermissen lasse (siehe dazu auch Bericht 2015 unter 12.1 sowie unsere Stellungnahme 16/3727, abrufbar unter www.ldi.nrw.de).

Der Antrag wurde abgelehnt. Der Gesetzgeber sieht keinen Bedarf für eine Novellierung des seit Oktober 2014 geltenden § 71 a HG NRW.

Bei der Frage nach einem bestmöglichen Ausgleich im Spannungsfeld zwischen

Wissenschafts- und Informationsfreiheit lohnt sich ein Blick in andere Bundesländer. Nach § 75 Abs. 6 des Bremischen Hochschulgesetzes etwa haben dortige Hochschulen eine öffentlich zugängliche Datenbank für Drittmittelprojekte unter Benennung des Projektinhalts, der Identität der Drittmittelgeber, der Fördersumme sowie der Projektlaufzeit zu führen. Auch das rheinland-pfälzische Transparenzgesetz enthält in seinem § 16 Abs. 3 eine vergleichbare Regelung. Für einen anderen Weg hat sich Niedersachsen entschieden: Dort haben sich alle Universitäten und Fachhochschulen im Wege einer freiwilligen Selbstverpflichtung gemeinsam mit dem Wissenschaftsministerium auf „Leitlinien zur Transparenz in der Forschung“ geeinigt. Diese beinhalten eine (Selbst-) Verpflichtung zur Veröffentlichung wesentlicher Daten drittmittelfinanzierter Projekte.

NRW benötigt mehr Transparenz auch im Bereich von Kooperationsverträgen – dabei sollten alle rechtlichen Möglichkeiten, dieses Ziel zu erreichen, in Betracht gezogen werden.

16.7 Eröffnung des Verwaltungsrechtswegs – Aufdeckung einer Gesetzeslücke

Das Informationsfreiheitsgesetz NRW (IFG NRW) hat sich in der Anwendungspraxis bewährt. Einzelne Fälle zeigen jedoch einen Ergänzungs- bzw. Novellierungsbedarf auf. So erhielt ein Antragsteller zwar letztlich nicht die gewünschten Informationen, er trug jedoch maßgeblich dazu bei, eine Gesetzeslücke in NRW aufzudecken.

Der Antragsteller beanspruchte Informationen eines kommunalen Wirtschaftsunternehmens, einer juristischen Person des Privatrechts. Im Einzelnen begehrte er Informationszugang zu den Entscheidungsgrundlagen, die zu einer Trinkwasserpreiserhöhung geführt hatten. Die Gesellschaft teilte dem Antragsteller mit, dass keine Bereitschaft bestehe, Kalkulationsgrundlagen gegenüber Kundinnen und Kunden offenzulegen. Dabei verwies sie darauf, dass sie als juristische Person des Privatrechts nur dann auskunftsverpflichtet wäre, wenn sie im Wege einer förmlichen Beleihung öffentlich-rechtliche Aufgaben wahrnehme. Diese Voraussetzung sei nicht erfüllt.

Wir haben Antragsteller und die Gesellschaft dahingehend beraten, dass gemäß § 2 Abs. 4 IFG NRW auch eine juristische Person des Privatrechts als Behörde im Sinne des IFG NRW gilt, wenn sie öffentlich-rechtliche Aufgaben wahrnimmt. Das ist der Fall, wenn sie eine Aufgabe innehat, die durch Gesetz übertragen ist. Die Aufgabe der öffentlichen Wasserversorgung ist durch das Wassergesetz NRW den Gemeinden zugewiesen und kann von diesen auf Dritte – wie hier: auch auf private Unternehmen – übertragen werden; nach der Übertragung handelt es sich weiterhin um eine öffentlich-rechtliche Aufgabe. Der Antragsteller begehrte also den Zugang zu Informationen, die eine öffentlich-rechtliche Aufgabe betreffen, so dass das IFG NRW Anwendung findet.

Die Gesellschaft war im Ergebnis anderer Ansicht und verweigerte den Informationszugang. Der Antragsteller sah sich deshalb gezwungen, eine gerichtliche Entscheidung des Verwaltungsgerichts herbeizuführen. Hierbei stieß er auf eine weitere unvorhersehbare und für ihn tatsächlich unüberwindbare Hürde: Das Verwaltungsgericht sah die Klage als unzulässig an, weil der Verwaltungsrechtsweg nicht eröffnet sei. Zumindest ein Verfahrensbeteiligter müsse eine Behörde oder eine mit hoheitlichen Befugnissen versehene Stelle sein. Das Gericht wich damit von der Rechtsprechung des OVG NRW ab, das eine dem öffentlichen Recht zuzuordnende Anspruchsgrundlage für die Eröffnung des Verwaltungsrechtswegs als ausreichend ansieht (Urteil vom 8. Juni 2005, Az. 8 E 283/05).

Der Antragsteller nahm die Klage deshalb zurück und wandte sich an den Petitionsausschuss des Landtags NRW. Auch die-

ser konnte ihm zwar in der Sache nicht zum gewünschten Informationszugang verhelfen, empfahl in Abstimmung mit uns jedoch der Landesregierung, bei der nächsten Novellierung des IFG NRW die Aufnahme einer Rechtswegzuweisung zu den Verwaltungsgerichten ausdrücklich vorzusehen. Vorbild für die noch zu schaffende Regelung in NRW könnten die Informationsfreiheits- bzw. Transparenzgesetze der Länder Schleswig-Holstein, Rheinland-Pfalz und Thüringen sein.

Nunmehr ist der Gesetzgeber gefordert, die Empfehlung umzusetzen und hinsichtlich der Rechtswegeröffnung für die Zukunft die notwendige Klarheit zu schaffen.

16.8 Anspruch auf Informationen aus nichtöffentlichen Sitzungen kommunaler Gremien

Nicht selten berufen sich Gemeinden und Gemeindeverbände bei der Ablehnung von Informationszugangsanträgen auf die Vertraulichkeit der Beratung und begründen dies mit der Nichtöffentlichkeit der Gremiensitzung. Die Entscheidung über solche Anträge ist im Einzelfall schwierig.

Nach § 7 Abs. 1 Informationsfreiheitsgesetz NRW (IFG NRW) ist der Antrag auf Informationszugang unter anderem für Protokolle vertraulicher Beratungen abzulehnen. Die Nichtöffentlichkeit einer Ratssitzung ist zwar ein Indiz für die Vertraulichkeit der Sitzung, reicht jedoch allein nicht aus, um den Informationszugang zu allen Informationen, die in einer solchen Sitzung behandelt worden sind, zu verweigern. Allein aufgrund der Tatsache, dass eine Sitzung nichtöffentlich stattgefunden hat, kann also nicht ohne weiteres der Rückschluss gezogen werden, dass es sich bei der entsprechenden Niederschrift um ein Protokoll einer vertraulichen Beratung handelt. Die Vertraulichkeit einer Beratung ergibt sich auch nicht bereits daraus, dass die Beteiligten sie für vertraulich erklären.

Im Einzelfall ist die Beurteilung, ob eine Beratung vertraulich ist oder nicht, jedoch alles andere als einfach. Erste Anhaltspunkte gibt das OVG NRW. Es geht davon aus, dass für die Annahme einer vertraulichen Beratung erforderlich ist, „dass die Beratung aus bestimmten Gründen eine gewisse Vertraulichkeit genießt. Diese Gründe haben sich an dem Schutzzweck der Norm zu orientieren, der darin liegt, dass eine offene Meinungsbildung und ein freier Meinungsaustausch geschützt werden soll, um eine effektive, funktionsfähige und neutrale Entscheidungsfindung zu gewährleisten“ (Urteil vom 9. November 2006, Az. 8 A 1679/04).

Auch wenn Kommunen häufig pauschal und ohne weitere Begründung Informationszugangsanträge mit dem Hinweis auf die Nichtöffentlichkeit der Beratung ablehnen, zeigt die Praxis, dass es auch anders geht:

In einem Fall hatte die Kommune die Herausgabe eines Berichtes des kommunalen Rechnungsprüfungsausschusses zunächst unter anderem wegen der Vertraulichkeit der Beratung im Sinne von § 7 Abs. 1 IFG abgelehnt. Obwohl anfänglich sogar noch weitere Ablehnungsgründe nach § 6 IFG – nämlich Beeinträchtigungen der Tätigkeit der Staatsanwaltschaft und des Erfolges der behördlichen Maßnahme – geltend gemacht wurden, entschied sich die Kommune letztlich dazu, den begehrten Bericht doch herauszugeben. Sie ging sogar noch einen Schritt weiter und veröffentlichte den Bericht auf ihrer Homepage. Es ist nicht auszuschließen, dass die öffentliche Berichterstattung und der damit verbundene öffentliche Druck zu dieser Entscheidung beigetragen haben.

Die Ablehnung eines Informationszugangsantrages wegen Vertraulichkeit der Beratung bedarf einer differenzierten Begründung und kann nicht allein auf die Nichtöffentlichkeit der Sitzung gestützt werden. Es hat sich gezeigt, dass die Entscheidung über einen IFG-Antrag trotz vermeintlicher Ablehnungsgründe bei wohlwollender Prüfung zu positiven Ergebnissen führen kann, die das Verwaltungshandeln nicht beeinträchtigen. Viele Auseinandersetzungen um Informationszugangsanträge könnten vermieden werden, wenn öffentliche Stellen vermehrt Informationen von sich aus unabhängig von einer Antragstellung veröffentlichen würden. Das in Aussicht gestellte Transparenzgesetz könnte dazu einen wichtigen Beitrag leisten.

Anhang

Kühlungsborner Erklärung der unabhängigen Datenschutzbehörden der Länder vom 10. November 2016[1]

Der Vollzug der Europäischen Datenschutz-Grundverordnung (DS-GVO) erfordert eine effektive Organisationsstruktur. Zentrale Bedeutung kommt dabei dem Europäischen Datenschutzausschuss (EDSA) zu, der für alle Aufsichtsbehörden verbindliche Beschlüsse treffen kann und in dem jeder Mitgliedstaat eine Stimme hat.

Die Datenschutzbehörden der Länder fordern den Bundesgesetzgeber auf, bei der gesetzlichen Regelung des Vertreters der deutschen Aufsichtsbehörden im EDSA der Unabhängigkeit aller Aufsichtsbehörden und der Zuständigkeitsverteilung zwischen Bund und Ländern Rechnung zu tragen.

Der Vollzug der Datenschutzregelungen obliegt im föderativen System der Bundesrepublik Deutschland den Datenschutzbehörden der Länder. Die Zuständigkeit des/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) beschränkt sich auf wenige spezifische Bereiche. Diesem Umstand muss bei der Vertretung der deutschen Aufsichtsbehörden im EDSA nach Artikel 68 DS-GVO Rechnung getragen werden. Die unabhängigen Datenschutzbehörden der Länder setzen sich daher für die folgenden Regelungen ein:

- Die Vertretung der deutschen Aufsichtsbehörden im EDSA kann sowohl durch den/die BfDI als auch eine Landesaufsichtsbehörde erfolgen. Die Stellvertretung obliegt dann dem jeweils anderen.

- Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestimmt die beiden Vertreter im EDSA.

- Die Vertretung im EDSA hat der nationalen Zuständigkeitsverteilung für den Vollzug Rechnung zu tragen. Die für den Vollzug zuständigen Aufsichtsbehörden müssen die Möglichkeit erhalten, über den Vertreter im EDSA Angelegenheiten einzubringen und ihre jeweiligen Positionen im Verfahren autonom zu bestimmen.

Unter Zugrundelegung dieser Leitlinien ist nach Auffassung der Länder eine effektive Vertretung der unabhängigen Datenschutzbehörden im EDSA möglich.

1 bei Enthaltung Bayerns

Pressemitteilung der unabhängigen Datenschutzbehörden der Länder vom 1. Februar 2017

Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz!

Am heutigen Mittwoch (01.02.2017) hat das Bundeskabinett den Entwurf zu einem neuen Bundesdatenschutzgesetz (BDSG) beschlossen, der jetzt in den Bundestag eingebracht werden soll. Anlass der Gesetzesnovelle ist das neue EU-Datenschutzrecht, bestehend aus der Datenschutz-Grundverordnung (DS-GVO) und der Datenschutz-Richtlinie im Bereich Justiz und Inneres. Die Mitgliedstaaten haben bis Mai 2018 ihr nationales Datenschutzrecht an die Verordnung anzupassen und die Richtlinie in nationales Recht umzusetzen.

Nach Auffassung der unabhängigen Datenschutzbehörden der Länder wird der im Bundeskabinett beschlossene Gesetzentwurf den europarechtlichen Vorgaben nicht gerecht und stellt bereits bestehende datenschutzrechtliche Standards in Frage. So schränkt der Entwurf die Informations-, Auskunfts- und Löschrechte der betroffenen Personen erheblich ein. Diese Einschnitte in die Betroffenenrechte stellen lediglich eine Arbeitserleichterung für die Daten verarbeitenden Stellen dar und stehen dem Schutzcharakter der Vorschriften zur Auskunft, Information und Löschung von Daten diametral entgegen. Die DS-GVO gestattet dem nationalen Gesetzgeber nur in sehr engem Rahmen weitere Einschränkungen der Betroffenenrechte vorzusehen. Entsprechend der Intention der DS-GVO haben die Verantwortlichen vielmehr primär durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, ihren Informations-, Auskunfts- und Löschpflichten zu genügen. Der nationale Gesetzgeber sollte auf eine weiter gehende Beschneidung der Betroffenenrechte verzichten.

Der Entwurf beschränkt zudem die Aufsichtsbefugnisse der Datenschutzbehörden gegenüber Berufsgeheimnisträgern dahingehend, dass sie ihnen und ihren Auftragsverarbeitern gegenüber nur ausgeübt werden dürfen, soweit hierdurch keine Berufsgeheimnisse verletzt werden. Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern werden häufig besonders schützenswerte Daten, wie z.B. Gesundheitsdaten, verarbeitet. Eine gesonderte Regelung für Beschränkungen der Aufsicht bei Berufsgeheimnisträgern ist weder notwendig noch verhältnismäßig, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Der Gesetzgeber sollte hier keine derart undifferenzierte Regelung treffen.

Darüber hinaus sieht der Gesetzentwurf zur Verarbeitung von Gesundheitsdaten sehr weitgehende Regelungen ohne Interessenabwägung vor. Er schafft damit zu allgemeine gesetzliche Verarbeitungsbefugnisse sowohl für nicht-öffentliche als auch öffentliche Stellen. Es werden zudem keine verbindlichen technisch-organisatorischen Schutzmaßnahmen geregelt. Dies kann zu Lücken im gebotenen Grundrechtsschutz führen.

Daten dürfen nur zu einem oder mehreren vorab festgelegten Zwecken verarbeitet werden. Die auch hier bestehende Möglichkeit für den nationalen Gesetzgeber, in engem Rahmen konkrete Normen zur Zweckänderung zu schaffen, ist als Ausnahmetatbestand restriktiv auszulegen. Die detaillierten nationalen Regelungen des Gesetzentwurfs überdehnen ihn aber über alle Maßen, höhlen damit die Zweckbindung weiter aus und konterkarieren überdies das Ziel der Vereinheitlichung des europäischen Rechts. Diese Aushöhlung des Grundsatzes der Zweckbindung darf nicht Gesetzeskraft erlangen.

Wiederholt haben die Datenschutzbeauftragten des Bundes und der Länder ein umfassendes Gesetz zum Beschäftigtendatenschutz gefordert. Der Gesetzentwurf sieht demgegenüber lediglich einige klarstellende Regelungen für den Beschäftigtendatenschutz vor. Stattdessen bedarf es aber detaillierter bereichsspezifischer Regelungen auf Grundlage der DSGVO.

Auch im Entwurf zum neuen BDSG findet sich die ausgeweitete Regelung zur Videoüberwachung durch Private, wie sie bereits mit dem „Videoüberwachungsverbesserungsgesetz“ eingefügt werden soll. Diesbezüglich wird auf die Entschließung der DSK vom 09.11.2016 verwiesen.

Schließlich kritisieren die Datenschutzbehörden der Länder, dass die Bundesbeauftragte für den Datenschutz als alleinige Vertreterin für alle deutschen Datenschutzbehörden im Europäischen Datenschutzausschuss (EDSA) vorgesehen ist. Stattdessen fordern die Landesdatenschutzbehörden eine Vertretungsregelung, die nicht nur der Unabhängigkeit aller Aufsichtsbehörden, sondern auch den tatsächlichen Vollzugszuständigkeiten Rechnung trägt, die vorwiegend bei den Ländern liegen. Dem EDSA kommt zukünftig eine zentrale Bedeutung zu, kann dieser doch Beschlüsse treffen, die für alle Aufsichtsbehörden verbindlich sind.

Der vom Kabinett verabschiedete Entwurf ist nach alledem trotz einiger Verbesserungen im Vergleich zu Vorentwürfen an einigen Stellen europarechtlich zweifelhaft und enthält eine Reihe von datenschutzrechtlichen Rückschritten.

Entschließungen der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

89. Konferenz vom 18./19. März 2015

■ Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

■ Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist da-

her frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden („Predictive Policing").

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes

und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

■ Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

   Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z.B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

■ Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer – und ggf. auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindest-

lohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

■ IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit

verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o.g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.
Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

■ Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist.[1]

1 Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

■ Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken

werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

■ Datenschutz nach „Charlie Hebdo“: Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen.

Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

90. Konferenz vom 30. September /1. Oktober 2015

■ Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglichtes den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom24. April 2013,

1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden“ hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“).

Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert.

Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt.

Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“).
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen.
Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

■ Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren. Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d.h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden. Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prü-

fen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

91. Konferenz vom 6./7. April 2016

■ Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.
Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu bestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.
Dementsprechend müssen insbesondere die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt das insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto insbesondere solche Verwaltungsdienstleistungen in Anspruch zu nehmen, die keinen Personenbezug erfordern.
- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.

- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.
- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.
- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.
- Auch für die Länder übergreifende Nutzung von Servicekonten ist eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.
- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.
- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betrof-

fenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

■ Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.
Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).

- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.

- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.

- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.

- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

■ Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell[1], dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

1 - Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster
- Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg
- Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München
- Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

■ Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen. Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben. Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i.V.m. Erwägungsgrund [EG] 155),
- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i.V.m. EG 53, letzte beide Sätze),
- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i.V.m. EG 150, vorletzter Satz), jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentli-

che Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),
- Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen(Art. 37 Abs. 4).

92. Konferenz 9./10. November 2016

■ „Videoüberwachungsverbesserungsgesetz“ zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz“ Änderungen des Bundesdatenschutzgesetzes (BDSG)einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[1] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben. Ter-

1 bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit

roristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen. Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

■ Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[1] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift“ (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

1 bei Enthaltung Hamburgs

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.
- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.
- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.
- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.

2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.

3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

Entschließungen zwischen den Konferenzen:

■ 05. Februar 2015 – Keine Cookies ohne Einwilligung der Internetnutzer

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Artikel 5 Absatz 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sogenannten Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Artikel 5 Absatz 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

■ 9. Juni 2015 – Gegen den Gesetzentwurf zur Vorratsdatenspeicherung von Telekommunikationsdaten bestehen erhebliche verfassungsrechtliche Bedenken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in der Entschließung vom 9. Juni 2015 auf ihre erheblichen verfassungsrechtlichen Bedenken gegen den Gesetzentwurf der Bundesregierung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für die Sicherheitsbehörden hin.

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.
Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z.B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtbegriffe (z.B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer

Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.
Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

■ 14. August 2015 – Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung

Konferenz der Datenschutzbeauftragten veröffentlicht Kernforderungen für geplante EU-Datenschutz-Grundverordnung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat ein Kernpunktepapier zur Europäischen Datenschutzgrundverordnung (DSGVO) vorgelegt. Darin formulieren die Datenschutzbeauftragten des Bundes und der Länder 14 konkrete Vorschläge an den Europäischen Rat, die Kommission und das Parlament, die im Gesetzgebungsverfahren zur Stärkung des Schutzes der Privatheit aller Bürgerinnen und Bürger der EU Beachtung finden sollen.

Die Vorschläge der Konferenz umfassen insbesondere die Forderung nach einer Stärkung der Zweckbindung. Es müsse sichergestellt sein, dass für bestimmte Zwecke erhobene Daten nicht für andere nicht genannte Zwecke verwendet, insbesondere an Dritte weitergegeben, werden dürfen. Die Konferenz spricht sich dafür aus, dass die Einwilligung als Grundlage für die Verarbeitung von Daten ausdrücklich erteilt werden müsse und z.B. der Abschluss eines Vertrages nicht von der Einwilligung des Kunden in weitere, damit nicht zusammenhängende Datenverarbeitungen abhängig gemacht werden dürfe. Betroffene sollen ihre Rechte auf Auskunft, Berichtung, Sperrung oder Löschung grundsätzlich unentgeltlich geltend machen können. Die Datenschutz-Grundverordnung sollte verpflichtende Vorgaben zur Bestellung von betrieblichen und behördlichen Datenschutzbeauftragten als Ansprechpartner vor Ort für Unternehmens- und Behördenleitungen sowie für Bürgerinnen und Bürger enthalten. Datenübermittlung an Behörden und Gerichte in Drittstaaten sollen grundsätzlich nur zulässig sein, wenn dies in

internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Zur Stärkung des Beschäftigtendatenschutzes sollten in der Grundverordnung Mindeststandards enthalten sein, über die hinaus die Mitgliedstaaten in ihren nationalen Regelungen weitergehende Regelungen treffen können. Und schließlich soll insbesondere für die Nutzerinnen und Nutzer sozialer Netzwerke im Internet ein ausdrückliches Recht zur Verwendung von Pseudonymen festgeschrieben werden.

Die derzeit stattfindenden Trilogverhandlungen werden voraussichtlich im Laufe dieses Jahres abgeschlossen. Nach Verabschiedung der Datenschutz-Grundverordnung sollen die Regelungen nach einem Übergangszeitraum von zwei Jahren für die Mitgliedstaaten verbindlich in Kraft treten.

Hinweis: Das Kernpunktepapier ist auf unserer Internetseite www.ldi.nrw.de abrufbar.

■ 29. Oktober 2015 – Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 09. Oktober 2015 seinen Standpunkt zur Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) angenommen hat, beraten Kommission, Parlament und Rat im sogenannten Trilog über ihre verschiedenen Positionen zur JI-Richtlinie mit dem Ziel der gemeinsamen Verabschiedung von JI-Richtlinie und Datenschutz-Grundverordnung (DSGVO) im Paket zum Jahresende 2015.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Konferenz) hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012[1] mehrfach öffentlich zur Datenschutzreform positioniert. Am 26. August 2015 hat sie zu den Trilogverhandlungen zur DSGVO Stellung genommen[2]. Sie hat ferner zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben[3]. Von Anfang an hat sie das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“ und dabei auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus im

1 Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

2 Trilogpapier der Konferenz zur DSGVO, abrufbar unter: www.datenschutz.hessen.de/entschliessungen.htm

3 Stellungnahmen zur DSGVO und zur JI-Richtlinie vom 11.6.2012; Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012, jeweils abrufbar unter www.datenschutz.hessen.de/entschliessungen.htm und www.datenschutz.hessen.de/taetigkeitsberichte.htm

Anwendungsbereich der JI-Richtlinie hingewiesen. Mit dieser Richtlinie wird eine Lücke geschlossen, denn einen Rechtsakt, der die Datenverarbeitung in den Bereichen Polizei und Justiz in der EU umfassend regelt, kennt das EU-Recht bislang nicht. Dies hat die Konferenz in der Vergangenheit immer wieder kritisiert[4] .

Die Konferenz setzt sich für eine Richtlinie ein, die auf möglichst hohem Niveau eine Mindestharmonisierung innerhalb der Europäischen Union herbeiführt. Sie begrüßt insofern die Entwürfe von Rat und Europäischem Parlament, als beide eine Mindestharmonisierung festschreiben. Mit einer Richtlinie verbindet die Konferenz die Erwartung an den deutschen Gesetzgeber und die deutsche Rechtsprechung, weiterhin Impulsgeber für die Schaffung eines effektiven Datenschutzrechts zu bleiben.

Vor diesem Hintergrund bewertet die Konferenz die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union. Kernanliegen des Datenschutzes im Bereich der polizeilichen Datenverarbeitung ist es, Grenzen der Erfassung und Speicherung in polizeilichen Dateien zu setzen: Bürgerinnen und Bürgern müssen darauf vertrauen können, nicht in polizeilichen Dateien erfasst zu werden, wenn sie keinen Anlass für eine polizeiliche Speicherung gegeben haben. Rechtmäßig von der Polizei erhobene Daten dürfen nur unter besonderen Voraussetzungen auch für andere polizeiliche Zwecke verwendet werden. Wer beispielsweise Opfer oder Zeuge einer Straftat war, muss darüber hinaus darauf vertrauen können, dass seine Daten nur beschränkt und unter strengen Voraussetzungen von Polizeibehörden verarbeitet werden dürfen. Dieses sind nur einige grundsätzliche Forderungen, die in der JI- Richtlinie zu regeln sind. Dazu stellt die Konferenz mit Bedauern fest, dass die Regelungen dieser Grundanliegen insbesondere in der vom Rat vorgelegten Fassung häufig allgemein bleiben, sich im Wesentlichen in dem Verweis auf das nationale Recht erschöpfen oder gar gänzlich fehlen.

Einen ganz wesentlichen Impuls für das deutsche Datenschutzrecht im Bereich von Polizei und Justiz erwartet die Konferenz von den Regelungen zur Durchsetzung des Datenschutzrechts durch die Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Datenschutz muss effektiv durchsetzbar sein. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Bei den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punk-

4 Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

te, denen sich nach Ansicht der Konferenz die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der JI-Richtlinie.

II. Die Vorschläge im Einzelnen

1. Keine Ausweitung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO!

Der Anwendungsbereich der JI-Richtlinie kann nicht isoliert betrachtet werden, sondern er bestimmt spiegelbildlich den Anwendungsbereich der DSGVO. Denn die DSGVO findet nach deren Art. 2 Abs. 2 lit. e keine Anwendung, soweit die JI-Richtlinie Anwendung findet. Vor diesem Hintergrund sind in der Vergangenheit verschiedene Entwürfe diskutiert worden, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-Richtlinie führen könnten. Auch die vorgelegte Version des Rates wirft insofern in Art. 1 Abs. 1 JI-Richtlinie Fragen auf, als der Anwendungsbereich der JI-Richtlinie um die Formulierung „zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit“ erweitert worden ist.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche der DSGVO und der JI-Richtlinie wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der Kommission enthält die JI-Richtlinie Regelungen zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung“. Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst sei, soweit sie nicht der Prävention einer Straftat diene. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizei unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JIRichtlinie – zusammenzufassen, solle der Anwendungsbereich der Richtlinie entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die Richtlinie zu fassen. Die Ordnungsverwaltung solle der JI-Richtlinie unterfallen, soweit sie Ordnungswidrigkeiten verfolgt. Damit stellt der Rat seine ursprüngliche Argumentation auf den Kopf. Denn diese Ausweitung der JI-Richtlinie führt gerade dazu, dass Ordnungsverwaltungen sodann sowohl der DSGVO als auch der JI-Richtlinie unterfielen, je nachdem welche Aufgabe sie erfüllten.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-Richtlinie für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Dies ist nach der vom Rat vorgelegten Fassung nicht der Fall. Die Datenverarbeitung anderer Behörden als der Polizeibehörden sollte weiterhin von der DSGVO geregelt werden.

Die Konferenz sieht die in der Ratsfassung hinzugefügte Erweiterung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO kritisch. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte, wie im Entwurf der Kommission und des Europäischen Parlaments vorgesehen, von der DSGVO geregelt werden.

2. Die Durchbrechung der Zweckbindung darf nur in engen Grenzen erfolgen!

Die Konferenz hat in ihrer Stellungnahme vom 11. Juni 2012 die Klarstellung gefordert, dass die Regelungen über die Zweckbindung nicht so verstanden werden dürfen, „dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzung für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf". Die Bedeutung der Zweckbindung wurde auch durch die Europäische Grundrechtecharta betont, in der sich in Art. 8 Abs. 2 die Zweckbindung als tragendes Prinzip des Datenschutzes findet. In der Richtlinie sollte daher die Zweckbindung (Art. 4 Abs. 1 lit. b JI-Richtlinie) insgesamt strikter gefasst werden[5] .

Der Rat hat in seiner Fassung den ursprünglichen Vorschlag der Kommission in Art. 4 Abs. 2 dahingehend ergänzt, dass eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig ist, wenn es dafür nach anwendbarem (nationalen) Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhältnismäßig ist. Der Entwurf der Kommission enthielt insofern nur allgemeine Regelungen, nach der eine Weiterverarbeitung nicht „unvereinbar" mit dem ursprünglichen Zweck der Erhebung und nicht exzessiv sein dürfe (Art. 4 Abs. 1 lit. b und c).

Die Konferenz bedauert insofern, dass der Entwurf des Rates keine ambitionierteren, strengeren Vorgaben macht. Die vorgeschlagenen Regelungen lassen nach der Auffassung der Konferenz einen zu weiten Rahmen, den auszufüllen ganz weitgehend dem nationalen Gesetzgeber überlassen wird. In Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) sollte der Begriff der Unvereinbarkeit von Datenverarbeitungen konkretisiert werden. Danach liegt eine Unvereinbarkeit vor, „wenn mit

5 Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff“)[6] .

Die Konferenz spricht sich für strenge Vorgaben an die Durchbrechung der Zweckbindung aus und regt insofern an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung zu machen. Der Begriff der Unvereinbarkeit in Art. 4 sollte bei Abs. 1 lit. b JI-Richtlinie in der Fassung des Rates wie folgt präzisiert werden: Eine Weiterverarbeitung der personenbezogenen Daten ist als unvereinbar mit dem ursprünglichen Erhebungszweck anzusehen, wenn die Daten nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.

3. Unverdächtige und andere besondere Personengruppen brauchen mehr Schutz!

Der Schutz unverdächtiger Bürgerinnen und Bürger sowie besondere Voraussetzungen für besondere Personengruppen stellen ein Kernanliegen des Datenschutzes im Bereich der Polizei und Justiz dar. Die Konferenz bedauert insofern die ersatzlose Streichung des Art. 5 in der Fassung des Rates und weist ausdrücklich auf die Fassung des Europäischen Parlaments zu Art. 5 hin, der sich an einer Stellungnahme der Art. 29-Gruppe orientiert. Ziel der von der Art. 29-Gruppe vorgeschlagenen Regelung des Art. 5 ist es sicherzustellen, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen mit kürzeren Fristen gespeichert werden und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Die Konferenz lehnt die Streichung des Art. 5 der JI-Richtlinie in der Ratsversion ab und unterstützt Art. 5 in der Fassung des Europäischen Parlaments.

4. Datenspeicherungen sind regelmäßig auf ihre Erforderlichkeit und Verhältnismäßigkeit zu überprüfen!

Ungeachtet des Rechts auf Löschung sollten die datenverarbeitenden Stellen verpflichtet sein, die Erforderlichkeit und Verhältnismäßigkeit von Speicherungen in regelmäßigen Abständen zu überprüfen. Eine solche Verpflichtung enthält die Ratsversion im Gegensatz zu Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments nicht. Der Rat beschränkt sich in seinem Entwurf darauf, die Mitgliedstaaten zur Festlegung von Speicher- und Aussonderungsprüffristen in Verfahrensverzeichnissen („records“, Art.

6 Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

23 JI-Richtlinie) zu verpflichten, wenn dies möglich ist. Dies reicht nicht aus. Vielmehr fordert die Konferenz als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher und Aussonderungsprüffristen, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

Die Konferenz fordert als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen nach dem Vorbild von Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

5. Moderner Datenschutz braucht umfassende Benachrichtigungspflichten!

Benachrichtigungen gehören zu den datenschutzrechtlichen „Kernrechten" der Betroffenen. Effektiver Rechtsschutz ist nicht möglich, wenn der von einer (heimlichen) Datenerhebung Betroffene keine Kenntnis von der Erhebung und Speicherung erlangt. Die Kontrolle dieser Datenverarbeitungen ist zwar auch Aufgabe der Datenschutzaufsichtsbehörden, doch sollte auch jede Bürgerin und jeder Bürger in die Lage versetzt werden, die sie oder ihn betreffende polizeiliche Maßnahme überprüfen zu können und überprüfen zu lassen.

Die Konferenz setzt sich daher für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

Zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtsschutzes durch Aufsichtsbehörden und Gerichte setzt sich die Konferenz für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

6. Keine Sonderregelung der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren!

Die Konferenz spricht sich für eine möglichst weitgehende einheitliche Regelung der Rechte der Betroffenen im Anwendungsbereich der JI-Richtlinie aus. Demgegenüber enthält Art. 17 hinsichtlich personenbezogener Daten in Gerichtsbeschlüssen oder staatsanwaltschaftlichen Verfahrensakten die Regelung, dass die Ausübung der Betroffenenrechte „im Einklang mit dem einzelstaatlichen Recht" erfolgt. Schon in ihrer Stellungnahme vom 11. Juni 2012 hatte die Konferenz eine Klarstellung zum Regelungsgehalt

des Art. 17 JI-Richtlinie gefordert. Leider tragen auch die vorgelegten Fassungen von Europäischem Parlament und Rat nicht dazu bei, die notwendige Klarstellung herbeizuführen. Die Konferenz betont daher noch einmal diese Notwendigkeit, da ansonsten Zweifel an der Anwendbarkeit der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren entstehen können. Zu diesem Zweck ist die Sonderregelung des Art. 17 zu streichen und sind die Betroffenenrechte in strafrechtlichen Ermittlungen einheitlich in der JI-Richtlinie zu regeln.

Die Konferenz spricht sich für eine Streichung des Art. 17 JI-Richtlinie aus, und wiederholt ihre Forderung, dass die in Kapitel III gewährten Betroffenenrechte auch im Bereich des staatsanwaltschaftlichen Ermittlungsverfahrens Anwendung finden.

7. Klarstellung – Datenverarbeitung nach dem Stand der Technik!

Die Konferenz unterstreicht die Bedeutung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Die Verpflichtung, diese Grundsätze zu beachten, wird in Art. 19 JI-Richtlinie jedoch in verschiedener Hinsicht erheblich beschränkt, unter anderem durch Bezugnahme auf „verfügbare Technologie“. Dies wird dem notwendigen Grundrechtsschutz nicht gerecht, denn „verfügbar“ sind auch veraltete Technologien, die nicht (mehr) die ausreichende Sicherheit bieten.

Demgegenüber stellt der „Stand der Technik“ („state of the art“) sicher, dass jeweils die modernsten vorhandenen Technologien einzusetzen sind. Der Stand der Technik ist eine im Europäischen Datenschutz handhabbare Definition. Sie findet seit längerem eine bewährte Anwendung in der Praxis und sollte auch in der JI-Richtlinie verwendet werden.

Der an verschiedenen Stellen gebrauchte ungenaue und dem Schutzbedarf personenbezogener Daten nicht gerecht werdende Begriff „verfügbare“ Technik bzw. Technologie sollte konsequenter Weise auch in der JI-Richtlinie durch „Stand der Technik“ ersetzt werden. Die Konferenz spricht sich insofern für Art. 19 in der Fassung des Europäischen Parlaments aus.

8. Datenschutz-Folgeabschätzung auch im Bereich der JI-Richtlinie!

Bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden sind Datenschutz-Folgeabschätzungen äußerst wichtig, da gerade bei dieser Verarbeitung erhöhte Risiken für den Einzelnen bestehen. Das Europäische Parlament hat eine entsprechende Regelung zur Datenschutz-Folgenabschätzung vorgeschlagen, die jedoch vom Rat abgelehnt wird.

Die vom Europäischen Parlament in Art. 25a vorgeschlagene Bestimmung sieht eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitungsvorgänge aufgrund ihrer Natur, ihres Anwendungsbereichs oder ihrer Bestimmungszwecke eine konkrete Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellen können. Für die in Art. 25a (2) lit. b erwähnten „biometrischen Daten“ gibt es in Art. 3 Abs. 11 des Vorschlags des Europäischen Parlaments eine entsprechende Definition.

In Art. 33 des Entwurfs der Datenschutz-Grundverordnung (Ratsfassung) ist, anders als beim Richtlinien-Vorschlag, nach wie vor eine Datenschutz-Folgenabschätzung vorgesehen. Doch gerade im verarbeitungsintensiven Bereich der Strafverfolgung sind gründliche Sicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten von größter Wichtigkeit, weshalb sich die Konferenz für die Aufnahme einer entsprechenden Regelung in den Richtlinienvorschlag ausspricht.

Die Konferenz setzt sich für eine Regelung der Datenschutz-Folgenabschätzung ein, die sich an Art. 25a des Richtlinien-Vorschlags des Europäischen Parlaments orientiert. In diesem Zusammenhang befürwortet die Konferenz die Wiederaufnahme der Definition der „biometrischen Daten“, wie sie vom Europäischen Parlament in Art. 3 Abs. 11 vorgesehen war.

9. Guter Datenschutz braucht behördliche Datenschutzbeauftragte!

Die Konferenz bedauert, dass der Rat es in seiner Version ablehnt, die Mitgliedstaaten zur Schaffung eines behördlichen Datenschutzbeauftragten zu verpflichten, sondern dies stattdessen in deren Ermessen stellt. Die Datenschutzbeauftragten des Bundes und der Länder haben überwiegend sehr gute Erfahrung bei der Zusammenarbeit mit den Datenschutzbeauftragten der beaufsichtigten Behörden gemacht und halten die interne Kontrolle vor Ort – neben der externen Kontrolle durch die Aufsichtsbehörden – für ein unverzichtbares Element eines flächendeckenden effektiven Datenschutzregimes.

Die Konferenz betont die Bedeutung einer verpflichtenden Bestellung eines behördlichen Datenschutzbeauftragten und spricht sich deshalb für Art. 30 des Vorschlages des Europäischen Parlaments aus.

10. Übermittlungen an Behörden und Gerichte in Drittstaaten bedürfen eines transparenten Verfahrens, der Abwägung im Einzelfall und müssen überprüfbar dokumentiert sein!

Neu an den Regelungen über die Übermittlung personenbezogener Daten in Drittstaaten ist, dass auch im JI-Bereich das Instrument des Angemessenheitsbeschlusses eingeführt werden soll. Die Konferenz ist der Auffassung, dass die geltenden Angemessenheitsbeschlüsse nicht auf den JI-Bereich übertragbar sind. Neben den Übermittlungen in Drittstaaten mit adäquatem Datenschutzniveau wird die Mehrzahl der Übermittlungen weiterhin auf der Grundlage bilateraler Abkommen und nationalen Rechts (im Einzelfall) erfolgen.

Die Konferenz fordert, in Übereinstimmung mit der Rechtsprechung des EuGH Abwägungsklauseln für alle Übermittlungen vorzusehen. Diese sollten die übermittelnde Behörde verpflichten, eine Abwägung zwischen dem Interesse an der Übermittlung und den schutzwürdigen Interessen des Betroffenen vorzunehmen. Die JI-Richtlinie sollte zugleich Dokumentationspflichten festschreiben, um die Kontrolle von Übermittlungen überprüfbar zu machen. Die Konferenz bedauert insofern die Streichung der Dokumentationspflicht in Art. 35 Abs. 2 in der Fassung des Rates. Zudem sollten die Drittstaaten über Verarbeitungsbeschränkungen (Löschfristen etc.) informiert werden.

Die Konferenz spricht sich ebenfalls für eine Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung entsprechende Regelung aus. Danach sind Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt noch vollstreckbar, wenn dies nicht in interna-

tionalen Übereinkommen zur Amts- und Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten Stellen. Die Konferenz erkennt an, dass mit der Schaffung einer solchen Regelung insbesondere die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden wird. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Die Konferenz fordert bei jeder Übermittlung in Drittstaaten eine Abwägung im Einzelfall. Des Weiteren muss die JI-Richtlinie sicherstellen, dass Übermittlungen dokumentiert und damit kontrollierbar sind. Deshalb sollte die Dokumentationspflicht gem. Art. 35 in der Fassung der Kommission beibehalten werden. Über nationale Verarbeitungsbeschränkungen ist bei jeder Übermittlung zu informieren. Des Weiteren fordert die Konferenz eine Regelung zur Übermittlung personenbezogener Daten an Behörden und Gerichte eines Drittstaates in Anlehnung an Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung.

11. Befugnisse der Datenschutzbehörden müssen gestärkt werden!

Datenschutz muss effektiv durchsetzbar sein. Die Konferenz erwartet von der Datenschutzreform daher eine Stärkung der Befugnisse der Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Art. 8 Abs. 3 der EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV verlangen vielmehr eine wirksame Durchsetzung der Grundrechte der Bürgerinnen und Bürger. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Datenschutz muss effektiv durchsetzbar sein. Dazu fordert die Konferenz die Stärkung der Befugnisse der Datenschutzbehörden durch die JI-Richtlinie. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

■ 20. April 2016 – Klagerecht für Datenschutzbehörden – EU-Kommissionsentscheidungen müssen gerichtlich überprüfbar sein

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert in ihrer Entschließung vom 20. April 2016 den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden gegen Entscheidungen der EU-Kommission vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU-US Privacy Shield“ bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Dateschutzgruppe hat zum „EU-US Privacy Shield“ zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU-US Privacy Shield“ in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner o. g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermög-

lichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6.10.2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist“.

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

■ Videoüberwachung in Schwimmbädern

Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises vom 19.02.2014, Stand 10. August 2015

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen.

Ansonsten findet das Bundesdatenschutzgesetz (BDSG) Anwendung, weshalb die in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (OH Videoüberwachung) beschriebenen Grundsätze für diese Schwimmbäder anwendbar sind.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Für diese öffentlich zugänglichen Räume beurteilt sich die datenschutzrechtliche Zulässigkeit nach § 6b BDSG.

Da sich die Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten, genießen sie besonderen Schutz (vgl. OH Videoüberwachung) und die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf besonderer Sorgfalt. Nach § 6b BDSG muss die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur

Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unabhängig von der Frage eines berechtigten Interesses oder der befugten Hausrechtsausübung ist eine Videoüberwachung jedenfalls nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z.B. zum Saunabereich) zu entrichten ist. Dies kann durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Es ist nicht verhältnismäßig, einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung für eine große Zahl von Personen hinzunehmen, nur, damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen[1].

1 OLG Koblenz, Beschluss vom 07.05.2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17.05.2006, Az.: 12 O 639/04: Der Betreiber eines Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch – wenn auch nicht ununterbrochen – auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre des Betroffenen berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens.

Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z.B. Beschädigung von Haartrocknern).

Darüber hinaus sind die in der OH Videoüberwachung unter Ziffer 2.2 benannten Maßnahmen (z.B. Verfahrensverzeichnis, Vorabkontrolle, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

■ Videoüberwachung in öffentlichen Verkehrsmitteln

Datenschutzgerechter Einsatz von optisch-elektronischen Einrichtungen in Verkehrsmitteln des öffentlichen Personennahverkehrs und des länderübergreifenden schienengebundenen Regionalverkehrs, Stand 16. September 2015

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre 2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt. Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z.B. Fahrerarbeitsplätze), findet neben dieser Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1 Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z.B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobach-

tet und dadurch im Notfall ein schnelles Eingreifen möglich wird.

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw. dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z.B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box- Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z.B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwachung durch einen Notfallschalter für den

Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o.Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frage ankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur

zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken – wie beispielsweise dem länderübergreifenden Bahnbetrieb – eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2 Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optischelektronischen Einrichtungen erfasst werden (z.B. der zum Zutritt für Fahrgäste hin

offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzonen, d.h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z.B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahmefällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigen darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten tech-

nischen Personals erfolgen kann. Dies kann beispielsweise durch den Einbau diesbezüglicher Werkstattschalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z.B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetriebnahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1 Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens „Videoüberwachung“ mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2 Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder / Piktogramme / Displays außen die Videoüberwachung kenntlich machen (vgl. § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.
Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3 Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funktionsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4 Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1 Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträger gespeichert und die Übrigen unverzüglich gelöscht.

4.2 Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3 Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie der Zeitpunkt der

Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vgl. Anlage zu § 9 BDSG).

4.4 Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z.B. pauschal eine „möglichst umfassende“ Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5 Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter betrieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

Beschluss vom 15./16. September 2015

■ Nutzung von Kameradrohnen durch Private

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmen-

bedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches (StGB)), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

■ Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen, Stand März 2016

Diese Orientierungshilfe enthält Hinweise zur datenschutzgerechten Formulierung und Gestaltung von schriftlichen Einwilligungserklärungen nach § 4a Bundesdatenschutzgesetz (BDSG) und elektronischen Texten nach § 13 Abs. 2 und Abs. 3 des Telemediengesetzes (TMG). Einwilligungen in Übermittlungen in Drittstaaten werden von dieser Orientierungshilfe nicht erfasst. Ergänzend sind gegebenenfalls die gesetzlichen Regelungen zu Allgemeinen Geschäftsbedingungen zu beachten.

In der täglichen Praxis der Datenschutzaufsichtsbehörden fällt immer wieder auf, dass in Antragsvordrucken von Firmen, Versicherungen, Banken, und anderen neben den vom Leistungsanbieter fest vorgegebenen Vertragsbedingungen die eventuell dazu ergänzend vorgesehenen datenschutzrechtlichen Einwilligungserklärungen nicht den Erfordernissen des § 4a BDSG entsprechen oder aber als „Einwilligungen" bezeichnete Texte vielmehr in Wirklichkeit als unabdingbare Vertragserklärungen bzw. allgemein geltende Geschäftsbedingungen einzustufen sind. Muss eine (AGB-rechtlich zulässige) Erklärung abgegeben bzw. Vertragsbedingung akzeptiert werden, um einen Vertrag abzuschließen, hat die betroffene Person also gar keine freie Wahlmöglichkeit, so handelt es sich nicht um eine datenschutzrechtliche Einwilligung nach § 4a BDSG, sondern um ein Vertragsangebot, das angenommen oder abgelehnt werden kann. Die mögliche Erlaubnis für den Datenumgang ergibt sich dann nicht aus § 4a BDSG, sondern aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

1. Überschriften

Bereits die Überschriften bringen häufig nicht klar genug zum Ausdruck, ob hier vom Antragsteller oder Kunden neben seiner hauptsächlichen Erklärung, beispielsweise dem Versicherungsantrag oder seiner Teilnahmeerklärung, noch zusätzlich eine datenschutzrechtliche Einwilligung abverlangt wird. Dies soll anhand einiger Negativbeispiele für Überschriften aufgezeigt werden:

- Datenschutzerklärung
- Datenschutz
- Datenschutzklausel
- Hinweis zum Datenschutz
- Erklärung zum Datenschutz
- Erklärung zur Datenverarbeitung

Im Gegensatz dazu weisen folgende dem § 4a BDSG entsprechende Positivbeispiele für Überschriften den Unterzeichnenden darauf hin, dass er mit Unterzeichnung eine datenschutzrechtliche Einwilligung abgibt:

- Einwilligungserklärung Datenschutz
- Datenschutzrechtliche Einwilligungserklärung
- Datenschutzrechtliche Einwilligungsklausel
- Einwilligungserklärung nach dem Bundesdatenschutzgesetz

2. Eindeutigkeit

Auch die Erklärung selbst ist zuweilen nicht eindeutig genug vorformuliert. So reicht es nicht aus, wenn sie mit den Worten beginnt: „**Mir ist bekannt, dass ...**“. Hier ist dem Kunden nicht bewusst, dass er eine zusätzliche Erklärung abgibt.

Die notwendige Klarheit besteht nur, wenn die Formulierung den Erklärungscharakter eindeutig zum Ausdruck bringt, wie es in folgenden Positivbeispielen aufgezeigt wird:

- Ich willige ein, dass ...
- Ich bin einverstanden, dass ...
- Mit der Unterschrift geben Sie Ihre Einwilligung, dass ...
- Durch Ihre Unterschrift wird die vorstehende Einwilligungserklärung mit den auf der Rückseite abgedruckten näheren Erläuterungen zur Datenverarbeitung und Datennutzung für ...(Zweck) Bestandteil des Antrages.

Weiter muss es sich um eine bewusste Erklärung der betreffenden Person selbst handeln (opt-in). Schon von der verantwortlichen Stelle im Sinne einer Zustimmung vorangekreuzte Einwilligungstexte oder nur mit einer Streich-/Abwahl-Möglichkeit versehene „vorgegebene Zustimmungen“ (opt-out) genügen dem grundsätzlich nicht.

3. Freiwilligkeit

Eine wirksame datenschutzrechtliche Einwilligung im Sinne von § 4a BDSG liegt nur dann vor, wenn diese freiwillig abgegeben werden und auch jederzeit widerrufen werden kann. Eine unter Druck oder Zwang abgegebene datenschutzrechtliche Einwilligung ist unwirksam.

4. Hervorhebung

In zahlreichen vorformulierten Einwilligungserklärungen fehlt es an der gemäß § 4a Abs. 1 Satz 4 BDSG und – bei Einwilligung in Werbung – gemäß § 28 Abs. 3a Satz 2 BDSG erforderlichen besonderen Hervorhebung gegenüber anderen Textpassagen, zum Beispiel durch

- Fettdruck, Schriftart oder Schriftgröße,
- farbliche Gestaltung der Schrift oder des Hintergrundes oder
- eine Umrahmung der Erklärung.

5. Platzierung

Die datenschutzrechtliche Einwilligungserklärung gehört als besondere beziehungsweise zusätzliche Willensäußerung der betroffenen Person in hervorgehobener Form (siehe unter Ziffer 4) grundsätzlich insgesamt auf das eigentliche Antragsformular und dort in aller Regel unmittelbar vor die Unterschrift, die dann sowohl die Hauptsacheerklärung (beispielsweise den Versicherungsantrag) als auch die datenschutzrechtliche Einwilligungserklärung abdeckt.

Denkbar ist aber auch bei längeren Einwilligungstexten eine besonders hervorzuhebende aussagekräftige Kurzfassung mit den wesentlichen Inhalten der datenschutzrechtlichen Einwilligungserklärung bei der Unterschrift mit einem Hinweis auf den beispielsweise auf der Rückseite oder auf einer Anlage enthaltenen erläuternden Text (siehe letztes Positivbeispiel unter Ziffer 2.).

Besonders datenschutzfreundlich – und in einzelnen Fallkonstellationen zwingend erforderlich (beispielsweise bei der beabsichtigten Übermittlung von Gesundheitsdaten) – ist es, wenn im Formular für die datenschutzrechtliche Einwilligung eine gesonderte Unterschrift vorgesehen ist.

Jedenfalls ist zur Sicherstellung der Eindeutigkeit und Freiwilligkeit (siehe Ziffern 2 und 3) erforderlich, dass die Einwilligungserklärung für ihre Gültigkeit ausdrücklich angenommen werden muss (beispielsweise durch ein Ankreuzen).

6. Trennung

In manchen Formularen werden die Datenschutzhinweise und -informationen nach § 4 Abs. 3 BDSG zu unabdingbaren Vertragsinhalten beziehungsweise allgemein geltenden Geschäftsbedingungen mit einer auf freiwilliger Basis abgefragten datenschutzrechtlichen Einwilligungserklärung nach § 4a BDSG vermischt. Unter der Überschrift „Datenschutzhinweise“ beginnt der Text mit Hinweisen und geht dann im weiteren Verlauf unvermittelt in eine Einwilligungserklärung über.

Dem Betroffenen wird hier nicht deutlich genug vor Augen geführt, dass er eine datenschutzrechtliche Einwilligungserklärung abgeben soll. Die reinen Informationen über Datenverarbeitung auf der Grundlage von Gesetz beziehungsweise Vertrag auf der einen Seite und die freiwillige datenschutzrechtliche Einwilligungserklärung auf der anderen Seite müssen textlich getrennt dargestellt werden. Eine mangelnde Trennung kann dazu führen, dass die Einwilligung als solche nicht erkannt wird und deshalb unwirksam sein kann.

7. Klare Zuordnung

Die ansonsten korrekt gestaltete datenschutzrechtliche Einwilligungserklärung soll nicht mit Datenverwendungen aufgebläht werden, die gar nicht einwilligungsbedürftig sind, da sie bereits auf Grund eines Gesetzes oder einer sonstigen Rechtsvorschrift zulässig sind.

Es ist vielmehr eine klare Zuordnung zur Einwilligung einerseits und zu den Datenschutzinformationen nach § 4 Abs. 3 BDSG andererseits vorzunehmen. Ist es rechtlich strittig, ob eine Datenverwendung einer Einwilligung bedarf, bestehen keine Bedenken, sie unter Beachtung der oben genannten Formvorschriften „vorsichtshalber" in die Einwilligungserklärung mit einzubeziehen.

8. Einwilligung bei besonderen Arten personenbezogener Daten

Soweit sich die Einwilligung auf besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) beziehen soll, ist bei der formularmäßigen Gestaltung der Erklärung § 4a Abs. 3 BDSG zu beachten, das heißt die Einwilligung muss ausdrücklich auch für diese besonderen Arten personenbezogener Daten erklärt werden.

9. Inhalt von Einwilligungen

Der Text der Einwilligungserklärung muss die betroffene Person klar und allgemein verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle informieren, und muss, soweit nach den Umständen des Einzelfalls erforderlich, auf eventuelle Folgen der Verweigerung der Einwilligung hinweisen (§ 4a Abs. 1 Satz 2 BDSG).

Auf die grundsätzlich gegebene Widerrufsmöglichkeit der Einwilligung ist hinzuweisen; im Bereich der Telemedien ist ein solcher Hinweis durch § 13 Abs. 3 TMG sogar ausdrücklich vorgeschrieben (siehe bei Nr. 10).

Wenn im Rahmen der Verarbeitung auch Datenübermittlungen an Dritte in Betracht kommen, sind die Datenübermittlungen mit deren Zweckbestimmung und die Empfänger der Daten transparent zu erläutern. Eine undifferenzierte, nicht mehr überschaubare Darstellung einer großen Anzahl genannter Datenempfänger kann den Transparenzanforderungen widersprechen und nach der zivilrechtlichen Rechtsprechung zu einer Unwirksamkeit der Einwilligung führen.

10. Einwilligung bei Telemedienangeboten

Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt (beispielsweise auf einer Webseite), so sind gemäß § 13 Abs. 2 und Abs. 3 TMG einige Besonderheiten zu beachten:
Danach muss der Diensteanbieter sicherstellen, dass

- der Nutzer die Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen und
- mit Wirkung für die Zukunft widerrufen kann.

Der Nutzer muss zudem vor Erklärung der Einwilligung auf sein jederzeitiges Widerrufsrecht hingewiesen werden, wobei diese Information für den Nutzer jederzeit abrufbar sein muss. Diese Unterrichtung kann beispielsweise in der Datenschutzerklärung erfolgen.

11. Werbeeinwilligungen

Hierzu wird auf die ergänzenden Regelungen in § 28 Abs. 3a und 3b BDSG hingewiesen. Siehe insoweit auch die Ziffern 2 und 4 der Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke.

Beschluss vom 13./14. September 2016

■ Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),
- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

30. Konferenz vom 30. Juni 2015

Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP)!

Die Bundesregierung hat sich dafür ausgesprochen, noch im Jahr 2015 das geplante Freihandelsabkommen (Transatlantic Trade and Investment Partnership, TTIP) zwischen der EU und den Vereinigten Staaten von Amerika zu verabschieden. Mit dem geplanten Abkommen würde die derzeit weltgrößte Freihandelszone entstehen.

Seit der Aufnahme der Verhandlungen zwischen der EU und den USA im Jahr 2013 wurden deren Intransparenz und der spärliche Informationsfluss kritisiert. Als Reaktion auf diese Kritik hat die EU-Handelskommissarin Cecilia Malmström im November 2014 mehr Transparenz versprochen. In diesem Rahmen hat sich die Europäische Kommission dazu verpflichtet, die Öffentlichkeit darüber zu informieren, mit wem sich ihre führenden Politiker und höheren Beamten treffen und einen erweiterten Zugang zu Dokumenten im Zusammenhang mit den Verhandlungen über eine transatlantische Handels- und Investitionspartnerschaft mit den Vereinigten Staaten zu ermöglichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) sieht diese Initiative als einen wichtigen ersten Schritt hin zu mehr Offenheit und mahnt deren Fortführung und Ausweitung dringlich an. Sie hebt die Notwendigkeit größtmöglicher Transparenz in den Verhandlungen für eine lebendige öffentliche Debatte hervor, in der die Bürgerinnen und Bürger vollständig über die Auswirkungen auf ihr tägliches Leben informiert werden. Die Informationsfreiheitsbeauftragten fordern im Sinne von Open Government Data, der Öffentlichkeit neben zusammenfassenden und erläuternden Informationen vermehrt Originaldokumente zur Verfügung zu stellen, um es den Bürgerinnen und Bürgern zu ermöglichen, sich eine eigene Meinung von den Inhalten und dem Ablauf der Verhandlungen zu bilden. Hierzu gehören auch Informationen über die Positionen und Forderungen der USA sowie von Lobbyisten. Eine umfassende Offenlegung von In-

formationen zu TTIP auf EU- sowie auf Bundes-Ebene soll so früh und so weit wie möglich erfolgen. Erst wenn Originaldokumente aus den Bereichen Umwelt-, Arbeitnehmer- und Verbraucherschutz bekannt sind, kann beurteilt werden, ob es zu einer Absenkung europäischer Standards kommt.

Die IFK fordert die Bundesregierung und die Europäische Kommission dazu auf, in den Verhandlungen mit den USA darauf zu bestehen, dass für Streitigkeiten zwischen den Handelspartnern öffentlich tagende hoheitliche Gerichte geschaffen werden. Nur dadurch kann die notwendige Transparenz gewährleistet werden.

■ Auch Kammern sind zur Transparenz verpflichtet!

Immer wieder verweigern sich berufsständische Kammern den Transparenzanforderungen der jeweiligen Informationszugangsgesetze.

Berufsständische Kammern nehmen hoheitliche Aufgaben auf Bundes- und Länderebene wahr. Für die jeweiligen Berufsgruppen besteht eine gesetzliche Pflicht zur Mitgliedschaft, die Kammern sind für Berufszulassungen zuständig und haben oft weitgehende Sanktionsmöglichkeiten.

Informationen, die im Rahmen ihrer Tätigkeit anfallen, unterfallen den Informationszugangsgesetzen von Bund und Ländern. Dies gilt auch für Jahresabschlüsse und Angaben zu Einnahmen, Ausgaben und Rückstellungen der Kammern. Für die Verpflichtung der Kammern ist es unerheblich, ob Antragstellende Kammermitglieder sind und welche Motive zur Antragstellung führten. Öffentlich-rechtliche Körperschaften befinden sich in weiten Bereichen nicht in Konkurrenz zu Marktteilnehmern – Wettbewerbsnachteile können sich zumeist nicht ergeben. Folglich stehen schutzwürdige Betriebs- und Geschäftsgeheimnisse einem Informationszugang in der Regel nicht entgegen.

Ansprüche auf Informationszugang sind unverzüglich, spätestens jedoch innerhalb der in den Informationszugangsgesetzen des Bundes bzw. der Länder genannten Fristen zu erfüllen. Eine Entscheidung darf nicht auf Gremiensitzungen verschoben, sondern sollte im Rahmen der regulären Geschäftsführung getroffen werden. Im Übrigen sind transparenzpflichtige Informationen der berufsständischen Kammern in den bereits vorhandenen Informationsregistern zu veröffentlichen.

Die Informationsfreiheitsbeauftragten in Deutschland fordern daher die berufsständischen Kammern auf, ihren Transparenzverpflichtungen nachzukommen.

31. Konferenz vom 15. Juni 2016

■ GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!

„GovData – das Datenportal für Deutschland“ ist eine Anwendung des IT-Planungsrats, die auf der Grundlage einer Verwaltungsvereinbarung vom Bund und mehreren Ländern betrieben wird. Das Portal bietet einen einheitlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen. Ziel ist es, diese Daten möglichst flächendeckend zur Verfügung zu stellen und sie an einer zentralen Stelle auffindbar und so einfacher nutzbar zu machen. GovData dient damit nicht nur der Information der Bürgerinnen und Bürger, sondern fördert zugleich auch die Transparenz und Akzeptanz des Verwaltungshandelns. Es stellt der Wirtschaft darüber hinaus Verwaltungsdaten zur Entwicklung neuer Geschäftsmodelle zur Verfügung.

Bislang beteiligen sich jedoch an dem Bund-Länder-Online-Portal noch nicht alle Länder. Viele Daten, an deren Veröffentlichung ein großes öffentliches Interesse besteht, sind noch nicht abrufbar. Das immense wirtschaftliche Potential von Open Data bleibt ungenutzt.

Sowohl für die Wirtschaft als auch für die Zivilgesellschaft ergeben sich erhebliche Vorteile durch einen freien Zugang zu den öffentlichen Daten der Verwaltung. Der Umfang und die Qualität der in GovData zur Verfügung gestellten Daten müssen verbessert und der Nutzwert des Portals weiter erhöht werden.

Daher appelliert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland an die verbleibenden Länder, der Verwaltungsvereinbarung beizutreten, und fordert alle Vereinbarungspartner zur verstärkten Bereitstellung von Daten auf.

32. Konferenz vom 2. Dezember 2016

■ „Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!“[1]

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern auf, jetzt flächendeckend Transparenzgesetze zu schaffen. Solche Gesetze verbinden den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung öffentlicher Stellen, bestimmte Informationen aktiv auf Informationsplattformen im Internet zu veröffentlichen.

Anlass für die Forderung ist ein Beschluss der Regierungschefs von Bund und Ländern vom 14. Oktober 2016. Nach dieser Vereinbarung werden Bund und Länder Open-Data-Gesetze erlassen und das Ziel verfolgen, bundesweit vergleichbare Standards für den Zugang zu öffentlichen Datenpools zu erreichen.

Die Informationsfreiheitsbeauftragten befürworten zwar die Zielrichtung des Beschlusses; dieser greift jedoch zu kurz. Neben der Bereitstellung von Rohdaten in standardisierten und offenen Formaten für eine Weiterverwendung gebietet die Transparenz öffentlichen Handelns, zusammenhängende, aus sich heraus nachvollziehbare Unterlagen zur Verfügung zu stellen. Hierfür kommen beispielsweise Verträge, Gutachten, Studien, umweltrelevante Konzepte, Pläne, Programme oder Zulassungsentscheidungen, Berichte, Protokolle, Beschlüsse, Organisationserlasse, Statistiken, öffentliche Planungen, Haushalts-, Stellen-, Organisations-, Geschäftsverteilungs- und Aktenpläne, Drucksachen, Verwaltungsvorschriften oder wesentliche Bestandteile von Subventions- und Zuwendungsvergaben und Baugenehmigungen sowie die wesentlichen Unternehmensdaten öffentlicher Beteiligungen einschließlich der Vergütung der Leitungsebenen infrage.

Daher fordert die Konferenz, dass Bund und Länder ihre Behörden verpflichten, derartige Dokumente grundsätzlich im Internet zu veröffentlichen. Der bekannt gewordene Entwurf des Eckpunktepapiers des Bundes vom 18.10.2016[2] genügt diesen Anforderungen nicht. Anstatt separate Gesetze zu schaffen oder die Regelungen den eher informationstechnisch orientierten E-Government-Gesetzen zu überlassen, sollte der Beschluss der Regierungschefs von Bund und Ländern so umgesetzt werden, dass Open-Data-Regelungen in Transparenzgesetze aufgenommen werden. Länder, die noch nicht über solche Gesetze verfügen, sollten nach Auffassung der Informationsfreiheits-

1 Bei Enthaltung des Bundes

2 Siehe netzpolitik.org

beauftragten vorhandene Informationsfreiheitsgesetze entsprechend fortentwickeln. Auch fordert die Konferenz jene Länder auf, die keinen allgemeinen Anspruch auf Informationszugang gewähren, endlich ein modernes Informationsrecht einzuführen.

Entschließungen zwischen den Konferenzen:

■ 4. Dezember 2015 – Informationsfreiheit 2.0 – endlich gleiches Recht in Bund und Ländern![1]

Vor zehn Jahren hat der Deutsche Bundestag das Informationsfreiheitsgesetz verabschiedet und damit für solche Länder, die bislang noch kein derartiges Gesetz kannten, ein Beispiel gegeben. Inzwischen besteht in elf Ländern ein Recht auf Zugang zu Verwaltungsinformationen, ohne dass die Antragsteller ihr Einsichtsinteresse begründen müssen.

Trotz einer flächendeckenden Entwicklung hin zu mehr Verwaltungstransparenz besteht weiterhin Handlungsbedarf. So zeigen weder Bayern noch Hessen Bestrebungen, Informationsfreiheitsgesetze zu schaffen. Die niedersächsische Landesregierung hat zwar beschlossen, einen Entwurf vorzulegen, berät aber noch über die Einzelheiten. In Sachsen soll bis spätestens 2019 ein Informationsfreiheitsgesetz geschaffen werden. Indes enttäuscht der lange erwartete Gesetzentwurf der baden-württembergischen Landesregierung durch viele überflüssige Einschränkungen. Das brandenburgische Beispiel zeigt, dass auch die Novellierung vorhandener Gesetze dazu dienen kann, das Rad durch die Schaffung neuer Ausnahmen zurückzudrehen. Die Umsetzung der Evaluation des Informationsfreiheitsgesetzes des Bundes steht noch aus. Ob dort – ebenso wie bereits in den Transparenzgesetzen von Hamburg und Bremen – Verwaltungen verpflichtet werden, bestimmte Informationen von sich aus im Internet zu veröffentlichen, ist ungewiss. In Rheinland-Pfalz tritt zum 01. Januar 2016 als erstem Flächenland ein solches Transparenzgesetz in Kraft. Es umfasst auch das im Übrigen bundesweit eingeführte Recht auf Zugang zu Umweltinformationen. Auch in Thüringen und Nordrhein-Westfalen ist laut Koalitionsvertrag beabsichtigt, das derzeitige Informationsfreiheitsgesetz zu einem Transparenzgesetz fortzuentwickeln.

Nach Auffassung der Informationsfreiheitsbeauftragten sollten moderne Regelungen über den Informationszugang in Form effektiver Transparenzgesetze

1. der herkömmlichen Informationserteilung auf Antrag eine Pflicht der Verwaltung zur proaktiven Veröffentlichung von Informationen in Open-Data-Portalen zur Seite stellen,

1 bei Stimmenenthaltung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

2. Ausnahmen vom freien Zugang zu Informationen nur in einem unbedingt erforderlichen Maß enthalten,

3. neben klassischen Verwaltungen auch Unternehmen der öffentlichen Hand einbeziehen und

4. der vorhandenen Rechtszersplitterung auf dem Gebiet der Informationsfreiheit entgegenwirken und das Umweltinformationsrecht mit dem Informationsfreiheitsrecht zusammenführen.

Sowohl bei der Novellierung vorhandener als auch bei der Schaffung neuer Regelungen muss die Erhöhung der Transparenz oberstes Ziel sein. Nach Auffassung der Informationsfreiheitsbeauftragten gibt es keinen vernünftigen Grund dafür, dass einige Länder noch immer kein Recht auf voraussetzungslosen Zugang zu Informationen haben.

Die Informationsfreiheit hat dort, wo sie eingeführt wurde, zu mehr staatlicher Transparenz, einer besseren Informiertheit der Bürger und einer offeneren Verwaltungskultur geführt. Transparenzgesetze und Open-Data-Plattformen im Internet haben diese Wirkung in erfreulicher Weise befördert. Die Befürchtung von Kritikern, dass Verwaltungen von einer Antragsflut überrannt würden, hat sich nicht bewahrheitet.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Gesetzgeber in Bund und Ländern auf, die positiven Erfahrungen mit der Informationsfreiheit in Deutschland anzuerkennen und die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen.

■ 28. April 2016 – Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!

Nach der aktuellen Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 25. Juni 2015, Az.: 7 C 1/14) muss die Bundestagsverwaltung auf Antrag Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste gewähren.

Wie der Deutsche Bundestag inzwischen bekannt gab, bedarf es derartiger individueller Anträge seit dem 18. Februar 2016 nicht mehr, denn die Bundestagsverwaltung veröffentlicht generell die Ausarbeitungen der Wissenschaftlichen Dienste nunmehr vier Wochen nach Auslieferung an die auftraggebenden Abgeordneten, damit diese zunächst die Möglichkeit haben, die Gutachten exklusiv nutzen zu können, proaktiv im Internet. Dabei

werden die Namen der Auftraggeber nicht bekannt gegeben.

Die Entscheidung zur proaktiven Veröffentlichung ist im Sinne von Open Data und Transparenz nachdrücklich zu unterstützen, da es ein großes öffentliches Interesse an den Ausarbeitungen der Wissenschaftlichen Dienste gibt. So lagen infolge der neuen Rechtsprechung des Bundesverwaltungsgerichts der Bundestagsverwaltung in kürzester Zeit weit über 2000 Informationszugangsanträge vor. Die individuelle Bearbeitung dieser Anträge hätte in aller Regel viel Zeit gebunden und unnötig hohe Personal- und Sachkosten verursacht. Durch die Entscheidung werden die Kosten sowohl für die Verwaltung als auch für die Bürgerinnen und Bürger deutlich gesenkt. Die Ausarbeitungen stehen der interessierten Öffentlichkeit zukünftig schnell und einfach zur Verfügung.

Vor diesem Hintergrund fordert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland die Verwaltungen der Landesparlamente auf, dem Beispiel der Bundestagsverwaltung in Sachen Transparenz und Open Data zu folgen. Dabei sind etwaige Ausschlussgründe (insbesondere durch Schwärzung der Namen der Auftraggeber) sowie landesrechtliche Vorgaben zu berücksichtigen. Auch die Verwaltungen der Landesparlamente sollten Ausarbeitungen der jeweiligen Wissenschaftlichen Dienste bzw. der Gesetzgebungs- und Beratungsdienste unabhängig von individuellen Zugangsanträgen im Internet veröffentlichen, soweit dies nicht bereits geschieht.

■ Beschluss der IFK vom 2. Dezember 2016: Geschäftsordnung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (GO IFK)

A. Zweck, Aufgaben und Arbeitsweise der Informationsfreiheitsbeauftragten in Deutschland

I. Zweck der IFK

Die IFK ist ein Zusammenschluss der Informationsfreiheitsbeauftragten des Bundes und der Länder mit dem Ziel, das Recht auf Informationszugang zu fördern und gemeinsam für seine Fortentwicklung einzutreten.

II. Zusammensetzung der IFK

Die IFK besteht aus dem oder der Informationsfreiheitsbeauftragten des Bundes und den Informationsfreiheitsbeauftragten der Länder, die bereits ein Informationsfreiheitsgesetz oder ein vergleichbares Gesetz haben. Mit der Übertragung der Funktion wird die oder der Informationsfreiheitsbeauftragte Mitglied der IFK. Bis dahin ist eine Teilnahme

jener öffentlichen Stelle, die voraussichtlich mit der Wahrung der Informationsfreiheit beauftragt werden wird, ohne Stimmrecht möglich.

B. Aufgaben der IFK

Die IFK verständigt sich auf gemeinsame Positionen in Fragen der Informationsfreiheit. Dies geschieht insbesondere durch Entschließungen, Positionspapiere und Stellungnahmen.

I. Vorsitz der IFK

Ein Mitglied der IFK führt den Vorsitz. Der Vorsitz wechselt in alphabetischer Reihenfolge. Der Bund steht am Beginn der Reihenfolge. Die IFK kann jederzeit Abweichungen von der Reihenfolge beschließen, insbesondere dann, wenn ein weiteres Land Mitglied wird. Die Amtszeit des Vorsitzes beginnt am 1. Januar eines Jahres und dauert ein Jahr.
Der Vorsitz richtet die Sitzungen der IFK aus. Er leitet die Sitzungen und vertritt die IFK nach außen.

II. Sitzungen der IFK

Die IFK tagt in der Regel zweimal im Jahr. Der Vorsitz stimmt den Termin der Sitzung frühzeitig ab und lädt die Mitglieder der IFK spätestens einen Monat vor der Sitzung ein. Die Tagesordnung der IFK wird in der Regel durch den Arbeitskreis Informationsfreiheit (vgl. unter C.) vorbereitet. Den Mitgliedern der IFK steht es frei, unabhängig davon zusätzliche Tagesordnungspunkte bis drei Wochen vor dem Konferenztermin anzumelden. Bereits die Anmeldung eines Tagungsordnungspunktes sollte eine Problemdarstellung und ein Beratungsziel enthalten. Nicht fristgerecht angemeldete Tagesordnungspunkte werden nur dann behandelt, wenn Dringlichkeit gegeben ist. Die Entscheidung darüber trifft der Vorsitz.

Spätestens zwei Wochen vor der Sitzung ist den Mitgliedern die vorläufige, abgestimmte Tagesordnung für die IFK zuzuleiten.

III. Öffentlichkeit der Sitzungen

Die IFK tagt grundsätzlich in öffentlicher Sitzung.

Die Tagesordnungen und Protokolle (vgl. unter B. II. bzw. C. II. 3.) der Sitzungen sowie diese Geschäftsordnung werden auf den Webseiten der Mitglieder veröffentlicht.

Die Teilnahme der Öffentlichkeit an Sitzungen ist von der verfügbaren Raumkapazität abhängig. Eine rechtzeitige Anmeldung beim jeweiligen Vorsitz ist daher erforderlich.

Bei der Veröffentlichung der Tagesordnung ist auf die Öffentlichkeit der Sitzung sowie auf die Notwendigkeit der Anmeldung hinzuweisen. Zum Schutz überwiegender öffentlicher oder privater Interessen kann der Vorsitz auf Antrag eines oder mehrerer Mitglieder die Öffentlichkeit von ihren Sitzungen oder Teilen der Sitzungen ausschließen. Der Antrag sowie die Entscheidung müssen begründet werden. Die Begründung der Entscheidung ist in das Protokoll aufzunehmen. Der Vorsitz gibt den Mitgliedern der IFK rechtzeitig vor der Sitzung die Gelegenheit, die Themen zu benennen, die ihrer Ansicht nach ausnahmsweise den Ausschluss der Öffentlichkeit erfordern. Der Vorsitz stellt die Tagesordnung falls erforderlich so zusammen, dass die öffentlichen und die nicht öffentlichen Themen jeweils in unterschiedlichen Zeitblöcken behandelt werden. Hiervon unbenommen bleibt die Möglichkeit, die Öffentlichkeit auf Antrag eines Mitglieds während der Behandlung eines Tagesordnungspunktes auszuschließen.

IV. Abstimmungen der IFK

Zur Erreichung einer gemeinsamen Position ist bei Abstimmungen Einstimmigkeit erforderlich. Einstimmigkeit liegt vor, wenn es keine Gegenstimmen gibt.

Bei Abstimmungen hat jedes Mitglied eine Stimme. Stimmberechtigt sind grundsätzlich nur anwesende Mitglieder. In besonderen Ausnahmefällen kann sich ein nicht-anwesendes Mitglied bei der Ausübung des Stimmrechts durch ein anderes Mitglied vertreten lassen.

V. Protokoll

Für jede Sitzung der IFK ist ein Protokoll zu fertigen. Der Entwurf des Protokolls ist allen Mitgliedern zuzuleiten. Einwendungen gegen das Protokoll sind innerhalb von vier Wochen geltend zu machen.

Das Protokoll der IFK wird auf den jeweiligen Homepages der Mitglieder veröffentlicht. Soweit erforderlich werden schutzbedürftige Ausführungen des Protokolls zu den unter Ausschluss der Öffentlichkeit behandelten Themen von der Veröffentlichung ausgenommen.

VI. Umlaufverfahren

Zwischen den Sitzungen der IFK können gemeinsame Positionen nach B. IV. ausnahmsweise im Umlaufverfahren herbeigeführt werden.

Das Verfahren wird durch den Vorsitz der IFK eingeleitet. Für die Kommentierung der Entwürfe im Umlaufverfahren sind angemessene Fristen zu setzen. Eine Nichtäußerung (Schweigen) auf einen Entwurf gilt als Enthaltung. Der Vorsitz stellt den zustande gekommenen Text fest und teilt diesen den Mitgliedern der IFK mit.

VII. Veröffentlichungen der IFK

Gemeinsame Positionen der IFK werden auf den Webseiten der Mitglieder veröffentlicht.

C. Arbeitsgremium der IFK

I. Zusammensetzung des Arbeitsgremiums

Der Arbeitskreis Informationsfreiheit (AKIF) unterstützt die IFK. Alle Informationsfreiheitsbeauftragten sollen einen Vertreter in den AKIF entsenden. Der AKIF ist auf Dauer angelegt. Der AKIF wird jeweils vom Vorsitz der IFK geleitet.

II. Aufgaben und Arbeitsweise des AKIF

1. Sitzungen des AKIF

Der AKIF arbeitet der IFK zu. Er bereitet deren Entscheidungen insbesondere durch die Erarbeitung von Entwürfen für Positionen vor. Die IFK kann den AKIF mit Positionsbestimmungen beauftragen.

Der AKIF bereitet grundsätzlich die Tagesordnung der IFK vor.
Der AKIF tagt in der Regel mindestens vier Wochen vor der IFK.
Für die Entscheidung des AKIF über die Zuleitung von Entwürfen für Positionen an die IFK reicht die einfache Mehrheit der abgegebenen Stimmen der vertretenen Mitglieder des AKIF aus.

2. Öffentlichkeit der Sitzungen

Die Festlegungen unter B. III. gelten für den AKIF entsprechend.

3. Protokoll

Der Vorsitz des AKIF erstellt für seine Sitzung ein Protokoll. Der Entwurf des Protokolls ist allen Mitgliedern zuzuleiten. Einwendungen können von den teilnehmenden Mitglie-

dern innerhalb von zwei Wochen geltend gemacht werden. Das Protokoll wird auf der nachfolgenden IFK zur Veröffentlichung freigegeben.

D. Änderungen und Geltungsdauer der Geschäftsordnung

I. Änderungen

Die Geschäftsordnung kann nur mit einer 2/3-Mehrheit der Stimmen aller Mitglieder der IFK geändert werden. B. IV. kann nur einstimmig geändert werden.

II. Inkrafttreten, Außerkrafttreten

Die Geschäftsordnung tritt am Tag nach ihrer Verabschiedung durch die IFK in Kraft.

Hinweise auf Informationsmaterial

Neben dem aktuellen Datenschutz- und Informationsfreiheitsbericht können Sie bei uns weiteres Informationsmaterial kostenlos anfordern. Eine vollständige Übersicht und ein Online-Bestellformular finden Sie auf unserer Hompepage unter www.ldi.nrw.de

Sie erreichen uns auch:

- per Post
Landesbeauftragte für Datenschutz
und Informationsfreiheit NRW
Kavalleriestr. 2-4
40213 Düsseldorf

- per E-Mail
poststelle@ldi.nrw.de

- per Telefon
0211 38424-0

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

www.ldi.nrw.de

Bericht 2017