Datenschutzbericht
2014/2015

Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

Fünfundzwanzigster
Tätigkeitsbericht nach § 29 Abs. 2
Landesdatenschutzgesetz (LDSG)
für die Zeit vom 1. Januar 2014
bis 31. Dezember 2015

LT-Drs. 17/311

HERAUSGEBER
Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Umschlaggestaltung
Petra Louis

7. Juli 2016

Datenschutzbericht
2014/2015

Inhalt

Die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) sind im Internetangebot des LfDI unter folgender URL abrufbar:
http://www.datenschutz.rlp.de/de/ds.php?submenu=grem

Einführung

Situation und Selbstverständnis des Landesdatenschutzbeauftragten

Der LfDI kontrolliert die Einhaltung der Bestimmungen des Landesdatenschutzgesetzes sowie anderer einschlägiger Bestimmungen und ist Aufsichtsbehörde für die Datenverarbeitung nicht-öffentlicher Stellen. Dieses Amt hat Edgar Wagner acht Jahre lang bis zum 30. September 2015 mit großem Engagement und nachhaltiger Außenwirkung ausgeübt. Ein wichtiger Schwerpunkt seiner Tätigkeit war die Beschäftigung mit den sozialen Medien und den Gefahren für die Persönlichkeit des Einzelnen, die aus technischen und gesellschaftlichen Entwicklungen entstehen können (vgl. 24. Tb., Tz. I-1). In den vorliegenden Berichtszeitraum fallen die Weiterentwicklungen nach den ersten Enthüllungen der teils rechtswidrigen Vorgehensweisen der NSA (vgl. 24. Tb., Tz. I-2), die eng mit der Diskussion um die Ausgestaltung der deutschen Nachrichtendienste insbesondere, aber nicht nur, auf Bundesebene verbunden sind. Zu diesen Geschehnissen und Ereignissen hat der LfDI mit konstruktiven und zukunftsorientierten Lösungsvorschlägen Stellung genommen.

Eine Herzensangelegenheit für Edgar Wagner war das Thema Datenschutz und Bildung (vgl. Tz. II-1, III-8). Hier hat er beachtliche Verdienste erworben, indem er mit dem Internetauftritt Youngdata zur Förderung der Medienkompetenz junger Menschen ein Angebot geschaffen hat, an dem auf seine Initiative hin inzwischen die Datenschutzbeauftragten der anderen deutschen Länder mitwirken und das über die Grenzen der Bundesrepublik Deutschland hinaus Anklang findet. In Rheinland-Pfalz hat Edgar Wagner einschlägige Workshops für Schülerinnen und Schüler entwickelt, die mit Unterstützung der Ministerien für Verbraucherschutz und Bildung mit großem Erfolg und unter erheblicher Nachfrage landesweit durchgeführt werden. Das Wirken von Edgar Wagner hat Spuren im Lande Rheinland-Pfalz und darüber hinaus hinterlassen und den Datenschutz wesentlich vorangetrieben.

Am 1. Oktober 2015 habe ich das Amt des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz übernommen. Ich stehe in der Nachfolge von Prof. Dr. Walter Rudolf, des ersten Landesbeauftragten, der es 16 Jahre im Nebenamt bekleidet hat und von Edgar Wagner als zweitem Landesbeauftragten. Ich trete mein Amt in einer Zeit an, in der Datenschutz und Informationsfreiheit vor neuen Herausforderungen stehen. Dies gilt für die tatsächliche Datenverarbeitung durch Staat und Private und deren gesellschaftliche Auswirkungen, aber auch für die rechtlichen Regelungen von Datenschutz und Informationsfreiheit. Wir leben im Zeitalter der Digitalisierung. Datenverarbeitung ist und wird zuneh-

mend allgegenwärtig, Informationen sind jederzeit und überall verfügbar. Die Entwicklung von Smart Home-Technologien und die Digitalisierung unserer Alltagsumgebung ermöglichen die technische Optimierung nahezu aller Abläufe des täglichen Lebens. Das selbstfahrende Auto und die vollautomatisierte Fabrik sind nur einige der Ideen, die viel näher an der Verwirklichung sind, als dies noch vor kurzer Zeit zu vermuten war. Gesundheitsdaten werden nicht nur gesammelt, sondern auch immer intensiver genutzt, und die Telemedizin wird fortentwickelt.

Gleichzeitig bedeutet Digitalisierung auch Registrierung. Alles, was wir tun und erleben, wird technisch erfasst, gespeichert und regelmäßig auch ausgewertet. Die Daten der Bürgerinnen und Bürger werden immer mehr zum Produktionsfaktor, zum Antriebsmittel der Wirtschaft. Und sie werden zum Gegenstand der Tätigkeiten von Sicherheitsorganen. Dabei ist zu beachten, dass der Umgang mit personenbezogenen Daten regelmäßig den Grundrechtsschutz der Einzelnen betrifft und nicht rein wirtschaftlich verstanden werden kann.

Dieser Bericht betrifft überwiegend einen Zeitraum, der in die Amtszeit meines Vorgängers Edgar Wagner fällt. Jedoch sind die Entwicklungen sehr dynamisch und setzen sich in vielerlei Hinsicht fort. Gerade die jüngsten Entwicklungen, insbesondere das Urteil des Europäischen Gerichtshofs zur Safe Harbor-Entscheidung der Kommission und deren Nichtigkeit, schließen an Vorgänge, Entwicklungen an und können im Zusammenhang betrachtet werden (vgl. Tz. I-1.4, I-1.5). Diese übergreifenden Entwicklungen auf europäischer, aber auch darüber hinausreichend internationaler Ebene, prägen die Rahmenbedingungen des Datenschutzes und werden sie künftig noch stärker prägen. Die Entwicklungen auf der Ebene des Landes sind allerdings für die Bürgerinnen und Bürger ebenso wichtig und oft sehr viel näher an der Lebenswirklichkeit des Einzelnen. Auch wenn dies künftig noch deutlicher von europäischen Vorgaben geprägt werden wird, kommt es für die Bürgerinnen und Bürger dann doch sehr darauf an, wie die sie oder ihn betreffende einzelne Frage des Datenschutzes beantwortet wird. Der Bericht legt daher einen starken Akzent auf die Veranschaulichung und Darstellung des Datenschutzes in den unterschiedlichen Sachbereichen, die für die Einzelnen von Relevanz sind.

Der LfDI ist zuvörderst für die Bürgerinnen und Bürger da. Der Schutz des Grundrechts ist immer auch Schutz der Rechtsstellung des Einzelnen. Diese Rechte sind gegenüber öffentlichen wie nichtöffentlichen Stellen und auf nationaler wie internationaler Ebene des Schutzes bedürftig. Dazu ist eine angemessene Ausstattung der Behörde ebenso erforderlich wie die Effektivität der Befugnisse des LfDI. Gerade hier zeichnen sich auch neuere Entwicklungen durch die Europäisierung ab, die unten näher beschrieben werden (vgl. Tz. I-1.3). Der LfDI ist nicht lediglich ein Interessenvertreter für

die gute Sache des Datenschutzes. Er verteidigt ein Grundrecht. Diese Funktion unterscheidet ihn von anderen Funktionsträgern, die Rechtswahrnehmungen bündeln. Zur angemessenen Wahrung des Grundrechts ist es erforderlich, frühzeitig Beeinträchtigungen oder Gefährdungen abzusehen und wenn möglich, zu minimieren oder auszuschalten. Aus diesem Grund ist die Aufgabe der Beratung in Fragen des Datenschutzes und der Informationsfreiheit sehr ernst zu nehmen (§ 24 Abs. 4 LDSG). Wenn Verletzungen des Datenschutzes gar nicht erst auftauchen, weil generelle Regeln und Herangehensweisen sinnvoll und datenschutzfreundlich ausgestaltet sind, stellt dies einen großen Erfolg eines gemeinsamen Herangehens mit den jeweils zuständigen und betroffenen Akteuren dar. Ungeachtet dessen behält die Bearbeitung individueller Eingaben ihre zentrale Rolle. Sie spiegelt die Sorgen und Nöte der Bürgerinnen und Bürger wider. Meine Behörde nimmt jede Eingabe ernst und setzt sich mit den angesprochenen Sachfragen und Problemen intensiv auseinander. Ziel ist die konstruktive Problemlösung.

Erste Ansprechpartner für den LfDI sind der Landtag und die Landesregierung. Hier können grundlegende Weichenstellungen beeinflusst werden, um die Wahrung des Datenschutzes in angemessener Weise sicherzustellen. Die enge und vertrauensvolle Kooperation mit dem Landtag und der Landesregierung ist dabei eine Voraussetzung für datenschutzfreundliche und grundrechtssensible Lösungen. Grundlage der Kooperation ist Prinzipienfestigkeit, denn die Grundrechtssicherung erfordert das Einnehmen klarer datenschutzrechtlicher Positionen.

Konstruktives Miteinander prägt auch die Zusammenarbeit mit der privaten Wirtschaft. Die Rolle als Aufsichtsbehörde stellt dabei Befugnisse zur Verfügung, die zur effektiven Durchsetzung des Datenschutzes in Anspruch genommen werden. Auch in der Rolle als Aufsichtsbehörde wird aber die Beratungsaufgabe nachhaltig wahrgenommen (§ 38 Abs. 1 Satz 2 BDSG). Wenn und soweit gemeinsame Lösungen mit der Wirtschaft erarbeitet werden können, die aufkommende Probleme und Fragen des Datenschutzes zur allseitigen Zufriedenheit aufgreifen, liegt dies im allseitigen Interesse.

Die neue europäische Datenschutz-Grundverordnung und die Datenschutz-Richtlinie für Polizei und Justiz, die 2016 verabschiedet wurden und 2018 wirksam werden, wollen ein europaweit hohes Datenschutzniveau schaffen und durchsetzen (vgl. Tz. I-1.3.2). Es werden erhebliche Anstrengungen erforderlich sein, um dieses Ziel auch tatsächlich zu erreichen. Alle Akteure der Datenverarbeitung müssen mit den neuen Regelungen, mit allen Rechten und Pflichten vertraut gemacht werden. Dies betrifft staatliche Stellen ebenso wie Wirtschaftsakteure, insbesondere aber auch die Bürgerinnen und Bürger.

Ich beabsichtige, an die erfolgreiche Amtsführung meines Amtsvorgängers anzuknüpfen und gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern die zukunftsträchtigen Schwerpunkte fortzuentwickeln. Rheinland-Pfalz soll ein kommunikationsfreundliches Land bleiben. Zugleich fordern und erlauben die anstehenden rechtlichen Herausforderungen durch die europäische Datenschutzreform und das Transparenzgesetz das Setzen neuer Akzente. Ich trete für eine Kommunikationspartnerschaft zwischen Bürger und Staat ein. Der Staat muss dem Einzelnen ermöglichen, seine kommunikative Freiheit selbstbestimmt zu verwirklichen.

Prof. Dr. Dieter Kugelmann

I. Entwicklung des Datenschutzes

1 Internationales und Europa

1.1 Die internationale Ebene

Das Bewusstsein, dass eine Reihe der vielfältigen Fragestellungen des Schutzes der Persönlichkeit und der personenbezogenen Daten nur auf der internationalen Ebene zu beantworten sind, ist angesichts der Globalisierung von Wirtschaft und Gesellschaft gewachsen. Die Vereinten Nationen entfalten inzwischen durchaus vielfältige Aktivitäten im Zusammenhang mit dem Schutz der Privatheit.

Die Vereinten Nationen haben eine Resolution zum Recht auf Privatheit im digitalen Zeitalter verabschiedet (Resolution no. 68/167 on The Right to Privacy in the Digital Age, von der Generalversammlung angenommen am 18. Dezember 2013). Die Generalversammlung der Vereinten Nationen ruft die Staaten dazu auf, das Persönlichkeitsrecht und personenbezogene Daten in der digitalen Welt ebenso zu schützen wie in der analogen Welt. Zu diesem Zwecke sollen die Staaten ihre Verfahren und Maßnahmen bei der Überwachung von Kommunikation und dem Sammeln von personenbezogenen Daten überprüfen und sicherstellen, dass die innerstaatlichen Überwachungspraktiken im Einklang mit den internationalen Menschenrechtsnormen stehen (Resolution Nr. 68/167 Nr. 4 lit. c).

Darüber hinaus sollen Aufsichtsmechanismen (effective domestic oversight mechanisms) eingerichtet werden. Sie sollen auf gerichtlicher, administrativer oder parlamentarischer Ebene als Kontrollinstrumente bei der Überwachung von Kommunikation und dem Abfangen personenbezogener Daten dienen.

Im Rahmen der Vereinten Nationen spielt die universelle Wahrung der Menschrechte auf Privatheit eine zunehmende Rolle. Dies hat auch institutionelle Folgen. Der Menschenrechtsrat der Vereinten Nationen nahm im März 2015 in seiner 28. Sitzung eine Resolution an, durch die das Mandat eines Sonderberichterstatters für Datenschutz geschaffen werden sollte (Resolution A/HRC/28/39) und ernannte im Juli 2015 Prof. Joseph Cannataci zum ersten Sonderberichterstatter für den Schutz des Rechts auf Privatheit („Special Rapporteur on the Right to Privacy"). Er soll das Menschenrecht auf Privatheit im digitalen Zeitalter überwachen (vgl. Art. 12 Allgemeine Erklärung der Menschenrechte). Er kann dabei keine rechtlich verbindlichen Beschlüsse oder Maßnahmen erlassen, sondern hat durch Empfehlungen und Berichte eher beratenden Charakter im Rahmen der Vereinten Nationen (vgl. DuD 2015, Interview with the UN Special Rapporteur on the Right to Privacy, S. 786 f.).

Die Verhandlungen zu Handelsabkommen mit den USA und anderen Staaten sind fortgeschritten und teils abgeschlossen, so mit Kanada. Die Wahrung von Belangen des Verbraucher- und Umweltschutzes haben insbesondere die Diskussionen um die Vereinbarungen mit den USA geprägt. Ziel ist zunächst der Abbau von Handelshemmnissen. Während das Transatlantic Trade and Investment Partnership (TTIP) den transatlantischen Handel zwischen den vertragsschließenden Staaten liberalisieren will, geht es im Trade in Services Agreement (TISA) um die Liberalisierung bei transatlantischen Dienstleistungen. Im Zusammenhang des Handels ist der Datenschutz von den Vereinbarungen nicht unmittelbar betroffen. Da es aber im Bereich der transatlantischen Dienstleistungen auch um Fragen des E-Commerce, der Finanzdienstleistungen und der IT-Dienstleistungen geht, dürften die europäischen Datenschutzbestimmungen für den Datentransfer zwischen Europäischer Union und USA für die weiteren Verhandlungen über TTIP und TISA spielen. Dabei müssen von der Kommission die aktuellen Entwicklungen zum Datentransfer nach dem Safe Harbor-Urteil des Europäischen Gerichtshofs (vgl. Tz. I-1.4, I-1.5) beachtet werden.

Für den Datenschutz besteht Anlass zur Wachsamkeit. In der Entschließung „Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten“ der Datenschutzkonferenz vom 13. März 2013 wird gefordert, bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus den Augen zu verlieren und das durch die Europäische Grund-

rechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards zu wahren (vgl. http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=085_freihandelszone).

Im Freihandelsabkommen der Europäischen Union mit Kanada (CETA) ist der Datenschutz ausdrücklich ausgenommen. CETA gilt als Vorbild für TTIP. Es ist zu hoffen, dass diese Regelung übernommen wird. Auf eine Kleine Anfrage im Deutschen Bundestag hat die Bundesregierung betont, sie vertrete die Position, das Freihandelsabkommen dürfe nicht zu einer Absenkung von Datenschutzstandards führen und müsse nicht nur von der Europäischen Union, sondern auch von den Mitgliedstaaten ratifiziert werden (BT-Drs. 18/2687, S. 2 und 5). Dies ist zu begrüßen.

Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in Straßburg zum Schutz des Privatlebens nach Art. 8 EMRK betrifft immer wieder auch staatliche Maßnahmen der Überwachung gegenüber Einzelnen. Die Entscheidung des Europäischen Gerichtshofs für Menschenrechte vom 4. Dezember 2015, (Beschwerde Nummer 47143/06, Roman Zakharov v. Russia) steht vor dem Hintergrund der Erkenntnisse und Diskussionen über die Tätigkeiten von Sicherheitsbehörden, die in Europa geführt werden. Der Gerichtshof hat entschieden, dass eine Telefonüberwachung insbesondere dann eine ungerechtfertigte Verletzung von Art. 8 EMRK darstellt, wenn die nationalen Gesetze in Bezug auf die Überwachung nicht klar definiert sind. Es müsse Möglichkeiten geben, sich gegen den Missbrauch von Überwachungsmaßnahmen zu wehren. Insbesondere müsse ersichtlich sein, wann und unter welchen Umständen man überwacht werden kann, welche Gruppe von Personen eventuell Opfer von Überwachungen sein können, wie lange die Überwachung anhält und wo ihre Grenzen sind, wie die gewonnenen Daten ausgewertet, genutzt und gespeichert werden, an welche Personen und Behörden die Daten weitergeleitet werden dürfen und wann die gewonnenen Daten gelöscht werden müssen.

1.2 Die Ebene der Europäischen Union

Das sog. „Umbrella Agreement" zwischen der Europäischen Union und den USA soll den Austausch persönlicher Daten für Strafverfolgungszwecke regeln. Ziel ist es, dass EU-Bürgerinnen und -Bürger ihre Datenschutzrechte vor US-Gerichten geltend machen könnnen (Agreement between the United states of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offenses, 15. September 2015).

Vertreterinnen und Vertreter der EU-Kommission und der US-Regierung haben am 15. September 2015 dieses Rahmenabkommen zum transatlantischen Datenschutz unterzeichnet. Darin wird der Umgang mit personenbezogenen Daten geregelt, die Ermittlungsbehörden untereinander austauschen, und es bietet nunmehr EU-Bürgerinnen und -Bürgern die Möglichkeit, ihre Datenschutzrechte vor US-Gerichten einzuklagen.

Inzwischen hat der US-Kongress vor dem Hintergrund des Rahmenabkommens ein Gesetz („Judicial Redress Bill") beschlossen, das EU-Bürgerinnen und -Bürgern den Weg vor US-Gerichte freimacht. Auf europäischer Seite steht die Zustimmung des EU-Parlaments zum Abkommen noch aus.

Das sog. „Umbrella Agreement" bezieht sich ausschließlich auf Daten, die zielgerichtet in die USA zur Verfolgung von Straftaten übermittelt worden sind und lässt den Austausch von Daten ungeregelt, die etwa kommerziellen Zwecke dienen. Neben der Einklagbarkeit von Rechten Betroffener sind darin Bestimmungen zu Speicherfristen und der Weitergabe von Daten an andere Behörden sowie Drittstaaten enthalten. Zudem gesteht das Abkommen EU-Bürgerinnen und -Bürgern unter gewissen Bedingungen das Recht zu, Einsicht in die über sie gespeicherten Daten zu nehmen und diese ggf. zu berichtigen.

Das Abkommen enthält keine festgeschriebenen Höchstspeicherfristen, sondern lediglich die Formulierung, dass Daten so lange gespeichert werden dürfen, wie es „notwendig und angemessen"

erscheint. Auch das Recht auf Einsichtnahme in die Daten ist mit Einschränkungen versehen: Ausnahmen sind etwa dann vorgesehen, wenn die „öffentliche und nationale Sicherheit“ betroffen sein sollte.

Der Vertrag war notwendig geworden, da es im Zusammenhang mit der Übertragung von Kontoinformationen (SWIFT) und Flugpassagierdaten (PNR) an US-Behörden zu Konflikten gekommen war. Die 2010 begonnenen Verhandlungen hatten sich zum Ziel gesetzt, solche Grundsatzfragen zu klären, die Mängel beim Datenschutz zu beheben und dafür zu sorgen, dass EU-Bürgerinnen und -Bürger ihre Rechte auch vor US-Gerichten durchsetzen können.

An zahlreichen Einzelpunkten wird aus datenschutzrechtlicher Sicht Kritik geübt (s. „EU-US Umbrella Data Protection Agreement : Detailed analysis“ by Douwe Korff, http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/).

Angesichts des begrenzten Anwendungsbereichs kann dieses Abkommen ohnehin nur als ein erster Schritt auf dem Weg zu einem höheren Datenschutzniveau in den USA gesehen werden. Dennoch sieht der LfDI diesen Schritt als wichtig an, da damit erstmals die Rechte der EU-Bürgerinnen und -Bürger in den USA einklagbar sein werden und die Informationsrechte von EU-Bürgerinnen und -Bürgern auch gegen US-amerikanische Stellen dem Grunde nach anerkannt werden.

Unter dem Oberbegriff der Netzneutralität wird diskutiert, wie und zu welchen Kosten der Zugang zu Inhalten gewährleistet wird, die von Diensteanbietern im Internet zur Verfügung gestellt werden. Das Europäische Parlament hat am 27. Oktober 2015 die Verordnung „über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten sowie die Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union“ verabschiedet. Hinter dieser unscharfen Formulierung verbirgt sich eine medial als Kompromiss der Institutionen der Europäischen Union bezeichnete gesetzliche Verankerung der Netzneutralität und der Abschaffung der Gebühren für Roaming. Im nationalen Recht hat sich Netzneutralität bisher in der Regelung des § 41a Abs. 1 TKG manifestiert, der eine diskriminierungsfreie Datenübermittlung und einen diskriminierungsfreien Zugang zu Inhalten gewährleisten soll.

Das Europäische Parlament setzt sich weiter mit Nachdruck für die Bürgerrechte ein. Mit der Entschließung des Europäischen Parlaments vom 29. Oktober 2015 zur Weiterbehandlung der Entschließung des Europäischen Parlaments vom 12. März 2014 zur elektronischen Massenüberwachung der Unionsbürger (2015/2635(RSP)) geht es umfassend auf die aktuellen Gegebenheiten ein. Die Datenschutzreform der Europäischen Union oder das Safe Harbor-Urteil werden ebenso bewertet wie das Rahmenabkommen mit den USA. Im Vordergrund stehen aber die demokratische Kontrolle der Nachrichtendienste und die Wiedergewinnung des Vertrauens der Bürgerinnen und Bürger in die Vertraulichkeit der Kommunikation vor dem Hintergrund der Datenübermittlung in Drittstaaten und ihrer technischen Gestaltung.

1.3 Die europäische Datenschutzreform

Die Europäische Union will den digitalen Binnenmarkt weiter entwickeln. In den weiteren Zusammenhang dieses wirtschaftlich ausgerichteten Unterfangens zählt auch die Reform des Datenschutzes. Sie verfügt über eine wirtschaftliche und eine grundrechtliche Stoßrichtung. Da sich jede europäische Regelung an der Grundrechtecharta messen lassen muss, ist die angemessene Gewährleistung der Rechte auf Privatheit und Datenschutz nach Art. 7, 8 GRCh unabdingbare Voraussetzung und Leitlinie der neuen Regelungen.

1.3.1 Entwicklung und Stand der Europäischen Datenschutzreform

Die Verhandlungen über den europäischen Datenschutz sind Ende 2015 abgeschlossen worden. Das Europäische Parlament hat seinen Standpunkt zur Datenschutz-Grundverordnung bereits im März 2014 festgelegt, dabei kam eine Mehrheit von 95 Prozent zustande. Der Rat der Innen- und

Justizminister hat im Juni 2015 nach mehr als drei Jahren Verhandlungen seinen Gemeinsamen Standpunkt beschlossen. Auf der Grundlage des Kommissionsentwurfs von 2012 liegen damit die drei Entwürfe vor, die im Rahmen des Trilogs miteinander in Einklang gebracht wurden. Der Trilog wurde im Dezember 2015 erfolgreich abgeschlossen, die Verordnung wird im Jahr 2016 formell verabschiedet.

Das gilt auch für die Richtlinie zum Datenschutz in Polizei und Justiz. Hier hat der Rat der Justiz- und Innenminister erst am 9. Oktober 2015 seinen Standpunkt angenommen. Die Richtlinie wurde im Laufe der Diskussion offensichtlich vernachlässigt. Erst die luxemburgische Ratspräsidentschaft hat die Richtlinie verstärkt auf die Agenda gesetzt.

1.3.2 Grundverordnung und JI-Richtlinie

Nach der Datenschutz-Grundverordnung lassen Öffnungsklauseln eine Rücksichtnahme auf das innerstaatliche Recht zu. Gerade die Bundesregierung hat in den Verhandlungen verstärkt darauf gedrungen, spezielle Regelungen insbesondere für den öffentlichen Bereich zu schaffen, so dass das innerstaatliche Recht dem Grunde nach bestimmte Bereiche weiterhin regeln kann. Dabei zielt die Bundesregierung etwa auf die Abgabenordnung, das Sozialrecht oder die Schulgesetze. Eine europäische Harmonisierung soll zuvörderst für die Datenverarbeitung durch Private erfolgen. Die Bundesregierung hat die Linie verfolgt, dass eine Erhaltung des in der Bundesrepublik Deutschland geltenden Datenschutzniveaus gesichert werden solle. Sie sieht im Gesamtpaket etwa unter Einbeziehung der erweiterten Informationspflichten dieses Ziel als erreicht an.

Wesentliche Fortschritte liegen in der Verbürgung der Rechte der Einzelnen auf Vergessen werden, also auf Löschung von Daten, und auf Datenportabilität, also auf die Mitnahme von Daten beim Wechsel des Anbieters. Klarere und ausführlichere Regelungen der Einwilligung und der Profilbildung durch Diensteanbieter wären wünschenswert gewesen. Das grundlegende Ziel, einen Mindeststandard für Private in der Europäischen Union zu schaffen, wird erreicht, allerdings vielfach auf Kosten der Präzision und Detailgenauigkeit der Regelungen. Nach dem Marktortprinzip unterliegt jedes Unternehmen, das auf dem europäischen Markt auftritt, unabhängig von seinem Sitz, den Datenschutzregeln der Europäischen Union. Die Aufsichtsbehörden werden gestärkt und die Sanktionen erweitert, um die Einhaltung des europäischen Datenschutzrechts effektiv zu kontrollieren. Dies wird auch verstärkte Anstrengungen des LfDI erfordern, die zu einem erhöhten Bedarf an Personal und Ressourcen führen.

Die Richtlinie für den Datenschutz in Polizei und Justiz (JI-Richtlinie) zielt auf die Sicherung eines Standards von Datenschutz auf dem Gebiet der Gefahrenabwehr und der Strafverfolgung. Die Datenschutz-Grundverordnung findet keine Anwendung, soweit die JI-Richtlinie greift, die Abgrenzung der Anwendungsbereiche hängt also von der Reichweite der JI-Richtlinie ab. Ziel ist, die gesamte Aufgabenerfüllung der Polizei unter einen Rechtsakt zusammenzufassen, nämlich unter die JI-Richtlinie. Sie betrifft grenzüberschreitende Vorgänge ebenso wie rein innerstaatliche Vorgänge. Die JI-Richtlinie ist entgegen anderslautenden Vorentwürfen auch anwendbar, wenn es um die Prävention einer Straftat geht. Sie enthält allerdings keine Präzisierungen der Verhältnismäßigkeit, die Bestimmung zu Benachrichtigungspflichten bleibt ungenau und insbesondere fehlt die Festlegung einer strengen Zweckbindung, die gerade auf dem Gebiet von Polizei und Justiz eine entscheidende Rolle spielt. Da es sich um eine Richtlinie handelt, können solche Mängel bei der Umsetzung behoben werden, indem vorhandene Regelungen ausgeschärft und in ihrem Anwendungsbereich auf eventuell noch nicht angemessen geregelte Erhebungen, Verarbeitungen und Übermittlungen von Daten erstreckt werden.

1.3.3 Anpassungsbedarf im innerstaatlichen Recht

Die Öffnungsklauseln der Grundverordnung eröffnen den Gesetzgebern in Bund und Ländern Spielräume. Vorrangig ist der Bundesgesetzgeber aufgerufen, eine Nachfolgeregelung zum geltenden Bundesdatenschutzgesetz zu beschließen. Darüber hinaus sind sämtliche Gesetze auf ihre Vereinbarkeit mit der Grundverordnung zu prüfen. Da eine Vielzahl von Gesetzen auch Bestimmun-

gen zum Datenschutz enthält, ist dies eine Herkulesaufgabe, die vor der im September 2017 stattfindenden Bundestagswahl wohl kaum vollständig zu erfüllen ist.

Diese Aufgabe kommt auch auf den Landesgesetzgeber in Rheinland-Pfalz zu. Die Landesgesetze in ihrer Gesamtheit stehen auf dem Prüfstand. Ihre einschlägigen Regelungen müssen der Grundverordnung entsprechen. Änderungen des Landesdatenschutzgesetzes dürften unabweisbar sein. In Umsetzung der JI-Richtlinie ist das Polizei- und Ordnungsgesetz anzupassen. Dabei ist darauf zu achten, dass die Vorgaben und Standards des Datenschutzes nicht ohne Not gesenkt werden, sondern auf hohem Niveau erhalten bleiben und fortentwickelt werden.

1.4 Die Rechtsprechung des Europäischen Gerichtshofs

Der Europäische Gerichtshof in Luxemburg wird immer mehr zum engagierten Verteidiger des Datenschutzes. Inhaltliche Maßstäbe der Grundrechte an den Schutz der Privatheit und den Datenschutz folgen aus Art. 7 und Art. 8 GRCh. Dies betrifft auch Datenübermittlungen an Staaten außerhalb der Europäischen Union. Die Verantwortlichkeit für den Datenschutz wird weit verstanden. Der Europäische Gerichtshof geht von weit reichenden grenzüberschreitenden Auswirkungen von Maßnahmen aus, die das Recht in der digitalisierten Welt schützen sollen. Der Europäische Gerichtshof macht deutlich, dass in einem Bereich, in dem er umfangreiche Zuständigkeiten hat und künftig aufgrund der Grundverordnung noch umfangreichere Zuständigkeiten haben wird, die Sicherung der Grundrechte bei ihm in guten und energischen Händen liegt. Er kann dabei auf ältere Rechtsprechung zurückgreifen, da die Datenschutzrichtlinie schon seit 1995 das wesentliche Element des Datenschutzes in Europa ist und seine Auslegung hier weitreichende Folgen hatte. Es sei nur die Rechtsprechung zur völligen Unabhängigkeit der Datenschutzbeauftragten genannt (Urteil vom 9. März 2010, Rs. C-518/07, Kommission/Deutschland, NJW 2010, 1265). Nicht zuletzt gegenüber dem Bundesverfassungsgericht bezieht der Europäische Gerichtshof damit klar Position. Er ist auch Grundrechtsgericht.

Einen Paukenschlag bildete die Entscheidung zur Nichtigkeit der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung (EuGH, Urteil vom 8. April 2014 in den verbundenen Rs. C-293/12 und C-594/12, DVBl. 14, 708). Darin misst der Europäische Gerichtshof die Richtlinie am Maßstab der europäischen Grundrechte und erklärt sie für nichtig. Sie beinhaltet nach Auffassung des Europäischen Gerichtshofs einen Eingriff von großem Ausmaß und von besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf Datenschutz, ohne dass sie Bestimmungen enthielte, die eine Beschränkung des Eingriffs auf das absolut Notwendige gewährleisten könnten. Die Entscheidung stellt klar, dass eine umfassende Speicherung von Personen, deren Verhalten keinerlei Anlass für eine Strafverfolgung gegeben hat, nicht verhältnismäßig ist (Tz. 58). Führt man diesen Gedanken konsequent weiter, ist eine grundrechtlich haltbare Regelung der Vorratsdatenspeicherung nicht möglich.

Das Recht auf Vergessen werden („Right to be forgotten“) äußert Konsequenzen für die Provider und die Nutzerinnen und Nutzer. Der Europäische Gerichtshof (Urteil vom 13. Mai 2014, Rs. C-131/12 – „Google Spain“; vgl. auch EuGRZ 2014, 320 = NVwZ 2014, 857 = NJW 2014, 2257) hat es im Google-Urteil auf der Grundlage der Datenschutz-Richtlinie rechtlich entwickelt, die Grundverordnung, die im Entwurf schon zum Urteilszeitpunkt bestand, nimmt es auf und normiert es. Im Kern verfügt jede natürliche Person über das Recht auf Löschung von Inhalten gegenüber dem privaten Dienstanbieter. Darin äußert sich die Selbstbestimmung der Einzelnen, die eben auch dazu führen soll, dass „das Netz vergisst“. Nach geltendem deutschen Recht gibt es Rechte auf Löschung und Sperrung von Daten (§ 20 BDSG), die aber die Konstellation eines Rechts auf Vergessen werden nicht ganz erfassen. Denn gelöscht wird demnach nicht die Information, sondern lediglich der Eintrag in der Suchmaschine. Damit ist die Verlinkung beseitigt. Auf der ursprünglichen Website ist die Information aber noch vorhanden. Das Recht auf Vergessen werden ist ein Recht auf Erschweren der Auffindbarkeit. Der Europäische Gerichtshof betont nachdrücklich den effektiven Schutz der Grundrechte und auf der Basis der Datenschutz-Richtlinie

95/46 insbesondere des Schutzes der Privatheit (EuGH, Rs. C-131/12, Google Spain, Rn. 58, 66). Er verfolgt einen Ansatz, der das europäische Recht auf möglichst viele Akteure in der digitalisierten Wirtschaft ausdehnt.

Der Europäische Gerichtshof hat mit seinem Urteil vom 6. Oktober 2015 (EuGH, Rs. C-362/14 – „Schrems/Digital Rights Ireland“, NJW 2015, 3151) zur Nichtigerklärung der Safe Harbor-Entscheidung der Kommission eine grundlegende Weichenstellung für die internationale Durchsetzung des Datenschutzes vorgenommen. Datenschützer mahnen bereits seit 2010 an, dass die Übermittlung personenbezogener Daten in die USA auf tönernen Füßen steht und nicht auf das sog. Safe Harbor-Abkommen gestützt werden kann. Spätestens seit der Diskussion um den umfassenden Zugriff von US-Behörden auf die Daten europäischer Bürgerinnen und Bürger muss allen klar geworden sein, dass in den USA ein „angemessenes Datenschutzniveau“ nicht gegeben ist. Mit seinem Urteil hat der Europäische Gerichtshof eine entsprechende Entschließung der Europäischen Kommission für ungültig erklärt und klare Maßstäbe benannt, anhand derer die Datenschutzaufsichtsbehörden Datentransfers in die USA prüfen können. Besonders kritisch bewertet der Europäische Gerichtshof den generellen Zugriff von Sicherheitsbehörden auf personenbezogene Daten und sieht darin den Wesensgehalt des Grundrechts auf Privatheit sowie des Grundrechts auf effektiven Rechtsschutz verletzt. Diese grundrechtlichen Feststellungen gelten allgemein für jede Datenübermittlung von der Europäischen Union in einen Drittstaat.

Der Europäische Gerichtshof hat mit seiner Safe Harbor-Entscheidung die umfassende Zuständigkeit der unabhängigen Datenschutzbehörden in Europa bestärkt, die auch durch die Europäische Kommission nicht eingeschränkt werden kann. Der Europäische Gerichtshof hat das eigenständige Prüfungsrecht des nationalen Datenschutzbeauftragten betont und letztlich zu einer Prüfungspflicht verstärkt. Es wäre ein Widerspruch, eine unabhängige Datenaufsicht zu fordern, ihr aber keine angemessenen Zuständigkeiten und effektiven Befugnisse einzuräumen. Dazu zählen eigenständige Klagerechte. Die Datenschutz-Grundverordnung enthält einschlägige Vorgaben, die der Europäische Gerichtshof teils vorwegnimmt. Das Urteil des Europäischen Gerichtshofs zu Safe Harbor führt zu einer Aufwertung der nationalen Datenschutzbehörden, die für die Prüfung zuständig sind.

1.5 Umsetzung der Safe Harbor-Entscheidung in Rheinland-Pfalz

Die Safe Harbor-Entscheidung des Europäischen Gerichtshofs konnte zwar nicht überraschen – wirft aber eine Reihe von Fragen bei den verantwortlichen Stellen auch in Rheinland-Pfalz auf. Viele dieser Fragen kann (nur) die örtlich zuständige Aufsichtsbehörde für den Datenschutz beantworten und damit den betroffenen Unternehmen eine gewisse Rechts- und Planungssicherheit geben.

Daher hat der LfDI bereits wenige Tage nach der Entscheidung des Europäischen Gerichtshofs in einem Positionspapier Antworten auf die wichtigsten nun aufgeworfenen Fragen gegeben und die folgenden Feststellungen getroffen:

Feststellungen zu Datenexporten in die USA

- Der Europäische Gerichtshof hat die Aufgabe der Datenschutz-aufsichtsbehörden betont, die Übermittlung von personenbezogenen Daten aus der Europäischen Union in die USA wirksam zu kontrollieren. Dem kommt der LfDI weiter nach.
- Um ein angemessenes Datenschutzniveau (§ 4b Abs. 2 Satz 2 BDSG) bei Übermittlungen von personenbezogenen Daten aus der Europäischen Union in Drittstaaten feststellen zu können, müssen zumindest folgende Garantien für den Datenschutz gegeben sein: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und verfassungskonformes 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.

- Der LfDI ist der Auffassung, dass in den USA, auch unter Berücksichtigung neuerer Entwicklungen, kein angemessenes Datenschutzniveau besteht (Feststellung des Anwendungsfalles von § 4b Abs. 2 Satz 2 BDSG). Er stützt sich dabei auf Erkenntnisse und Feststellungen des Europäischen Gerichtshofs zu Defiziten in US-Recht und -Praxis, auf Stellungnahmen der EU-Kommission sowie gemeinsame Beschlüsse der unabhängigen Datenschutzbeauftragten von Bund und Ländern.
- Eine Übermittlung von personenbezogenen Daten in die USA ist daher nur noch ausnahmsweise zulässig (§ 4c BDSG). Solche Übermittlungen bedürfen – abgesehen von den Sonderfällen des § 4c Abs. 1 BDSG – der ausdrücklichen Genehmigung des LfDI.
- Auf eine Einwilligung der Betroffenen (§ 4c Abs. 1 Satz 1 BDSG) wird sich die verantwortliche Stelle nur in seltenen Fällen stützen können, zumal die freie Widerruflichkeit solcher Einwilligungen keine Basis einer verlässlichen Datenverarbeitung bieten kann. Bei der Übermittlung von Beschäftigtendaten ist die Einwilligung ohnehin keine zulässige Grundlage für eine Datenübermittlung in die USA. Eine Einwilligung zum Transfer von Kundendaten kann unter engen Bedingungen, insbesondere bei vollumfänglicher und detaillierten Aufklärung der Betroffenen über die Gefährdungen ihrer personenbezogenen Daten bei der Übermittlung in einen Staat ohne angemessenes Datenschutzniveau zulässig sein. Die Einhaltung dieser Bedingungen wird der LfDI im Einzelfall prüfen.
- Eine Datenübermittlung aufgrund der Safe Harbor Entscheidung der EU-Kommission ist nach dem Urteil des Europäischen Gerichtshofs nicht mehr zulässig.
- Darüber hinaus entfaltet diese Entscheidung auch Auswirkungen auf andere Instrumente zur Legitimation des transatlantischen Datentransfers (§ 4c Abs. 2 BDSG).
- Das Urteil des Europäischen Gerichtshofs stellt auch die Wirksamkeit der Standard-Vertragsklauseln der EU-Kommission in Frage. Jedenfalls wird der LfDI im Einzelfall prüfen, ob Datenimporteure in den USA ihrer vertraglichen Verpflichtung nachgekommen sind zu garantieren, dass sie keinen Gesetzen unterliegen, die ihnen die Befolgung der Anweisungen des Datenexporteurs oder die Einhaltung ihrer vertraglichen Pflichten unmöglich machen, und nachteilige Gesetzesänderungen in den USA (hier: USA Patriot Act 2001 und seine Folgeregelungen) dem Datenexporteur mitzuteilen. Ebenfalls wird der LfDI prüfen, wie der Datenexporteur hierauf reagiert hat, ob er angemessene Konsequenzen gezogen und insbesondere von seinem vertraglichen Kündigungsrecht Gebrauch gemacht hat.
- Der LfDI wird auf absehbare Zeit auch keine Genehmigungen für Datenübermittlungen in die USA auf Grundlage von bindenden Unternehmensregelungen (BCR, § 4c Abs. 2 Satz 1 2. Halbsatz BDSG) erteilen können. Es ist schwer vorstellbar, dass verantwortliche Stellen ausreichende Garantien dafür bieten können, dass staatliche Stellen der USA nicht in grundrechtswidriger Weise auf die nach europäischem Recht geschützten Daten zugreifen können. Sofern verantwortliche Stellen der Auffassung sind, solche Garantien etwa durch den Einsatz von Verschlüsselungsverfahren bieten zu können, wird der LfDI dies im Einzelfall prüfen und bewerten.

Diese Feststellungen verband der LfDI die weiteren Folgerungen, die den betroffenen Unternehmen weitere Orientierung geben sollten:

Folgerungen für Datenexporte in die USA

- Unternehmen sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer in die USA datenschutzgerecht zu gestalten.
- Der LfDI wird Datenübermittlungen in die USA auf Grundlage der Safe Harbor-Entscheidung der EU-Kommission, die **vor** der Entscheidung des Europäischen Gerichtshofs durchgeführt wurden, nicht sanktionieren.
- Bis zum 31. Januar 2016 wird es Aufgabe der datenexportierenden Unternehmen sein, zu prüfen
  - auf welcher Rechtsgrundlage bislang Datenübermittlungen in die USA stattfinden,
  - insbesondere ob bisher Übermittlungen auf Grundlage der jetzt für ungültig erklärten

Safe Harbor-Entscheidung der EU-Kommission erfolgten,
  - ob die Entscheidung des Europäischen Gerichtshofs Grundlage einer außerordentlichen Kündigung bestehender Vertragsbeziehungen zu Safe Harbor-zertifizierten Unternehmen in den USA ist und
  - welche alternativen Übermittlungsmöglichkeiten in die USA bestehen.
- Unternehmen, die weiterhin Daten in die USA exportieren wollen, sollten sich dabei an der Entschließung der Datenschutzkonferenz vom 27. März 2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ und an der Orientierungshilfe „Cloud Computing“ vom 9. Oktober 2014 orientieren.
- Der LfDI steht im Rahmen dieses Prüfvorgangs den verantwortlichen Stellen beratend zur Seite. Er wird die verantwortlichen Stellen auf Alternativen zu Datenverarbeitungen in den USA hinweisen, also auf Dienstleister, die Datenverarbeitungen ausschließlich innerhalb der Europäischen Union oder in Staaten mit angemessenem Datenschutzniveau vornehmen. Dabei werden auch tragfähige Lösungen für Supportleistungen aus dem außereuropäischen Ausland und für 24/7-Dienstleistungen in den Blick genommen.
- Ab dem 1. Februar 2016 wird der LfDI stichprobenartig und gleichförmig prüfen, ob
  - die verantwortlichen Stellen in Rheinland-Pfalz Übermittlungen in die USA nur auf hinreichender Rechtsgrundlage, insbesondere mit der erforderlichen Genehmigung der Aufsichtsbehörde durchführen,
  - die verantwortlichen Stellen in Rheinland-Pfalz nicht rechtskonforme vertragliche Bindungen an Safe Harbor-zertifizierte Unternehmen in den USA aufgelöst und betroffene personenbezogene Daten in den USA haben löschen lassen,
  - die verantwortlichen Stellen in Rheinland-Pfalz bestehende rechtmäßige Alternativen zu Safe Harbor-zertifizierten Unternehmen in den USA geprüft haben und auch tatsächlich nutzen.
- Nach wie vor steht die Beratungsleistung für den LfDI im Vordergrund. Die Verhängung von Bußgeldern kommt allerdings dann in Betracht, wenn bei Kontrollen des LfDI offenbar wird, dass das Unternehmen keine bewertende Analyse von Datenübermittlungen in die USA vorgenommen und keine erkennbaren Anstrengungen unternommen hat, rechtmäßige Alternativen zu solchen Datenübermittlungen zu suchen und zu realisieren.

Eröffnung von 120 Auskunftsverfahren

Der „Paukenschlag aus Luxemburg“ kam zwar nicht unerwartet, traf aber viele Unternehmen unvorbereitet. Der LfDI nahm dies zum Anlass, die rheinland-pfälzischen Unternehmen auf die Problemlage hinzuweisen, seine Unterstützung anzubieten und im Rahmen von mehr als 120 Auskunftsverfahren die größten Unternehmen zu den Grundlagen von Datentransfers in die USA zu befragen. Der LfDI wollte wissen, auf welcher Rechtsgrundlage in Rheinland-Pfalz ansässige Unternehmen personenbezogene Daten in die USA übermitteln.

Die Ergebnisse der Auskunftsverfahren stellte der LfDI noch vor Jahresende 2015 der Öffentlichkeit vor: Der LfDI freute sich über die hervorragende Rücklaufquote von 95 Prozent; sie zeigte, dass die Unternehmen in Rheinland-Pfalz gegenüber der Aufsichtsbehörde dialog- und auskunftsbereit sind und die Thematik „Datentransfers in die USA“ als relevant erkannt haben.

53 Prozent der Unternehmen konnten die Fragen des LfDI vollständig, plausibel und fristgerecht beantworten. Für diese Unternehmen zahlte sich also die vorausschauende Positionierung in Sachen Datenschutz, etwa „No Cloud Policys“ oder die Bevorzugung von europäischen Dienstleistern mit hohem Datenschutzstandard aus.

47 Prozent der Unternehmen offenbarten allerdings erhebliche, teils gravierende Defizite im Umgang mit personenbezogenen Daten von Kundinnen und Kunden, Geschäftspartnerinnen und -partnern und Beschäftigten: Sie waren teilweise nicht in der Lage, die an sie gerichteten Fragen binnen gesetzter Frist vollständig zu beantworten. Das ist aus Sicht der LfDI nicht hinnehmbar, da die datenschutzrechtlich verantwortliche Stelle jederzeit fähig sein muss, den Umgang mit den eigenen personenbezogenen Daten, Datenflüsse

und deren Rechtsgrundlagen vollständig darzulegen.

Ein weiterer Teil der Unternehmen gab zwar an, keine Datentransfers in die USA vorzunehmen, setzte sich dann jedoch selbst dazu in Widerspruch. Diesen Unternehmen ist offensichtlich nicht klar, dass bei der Nutzung von Cloud-Diensten, von Google Analytics, Microsoft Office 365 oder Facebook regelmäßig personenbezogene Daten in die USA übermittelt werden – sei es beim Nutzen der Programme, bei Backups, Fernwartungen oder Updates – und dass sie hierfür verantwortlich sind. Teilweise meinten Unternehmen sogar, „Alltagsdaten“ wie Namen, Adressen oder Telefonnummern seien nicht schutzwürdig. Dies verletzt die Grundrechte der betroffenen Kundinnen und Kunden, Vertragspartnerinnen und -partner und Beschäftigten kann nicht toleriert werden. Hier sieht sich der LfDI noch vor ganz erheblicher weiterer Aufklärungsarbeit. Weitere Unternehmen gehen von einem „angemessenen Datenschutzniveau“ in den USA bzw. bei ihren US-Partnerfirmen aus. Damit setzen sie sich allerdings in Widerspruch zu den Feststellungen der EU-Kommission und des Europäischen Gerichtshofs.

Insgesamt also ein Ergebnis mit viel Licht, aber auch Schatten, das noch erhebliche Anstrengungen der Unternehmen und der Aufsichtsbehörde erfordert.

Der LfDI konstatierte noch ganz erheblichen Aufklärungsbedarf bei den Unternehmen, dem er durch Einzelberatungen, Veröffentlichungen und Veranstaltungen in Kooperation mit Verbänden und Kammern nachgekommen ist. Der LfDI wies die verantwortlichen Stellen weiter auf Alternativen zu Datenverarbeitungen in den USA hin, also auf Dienstleister, die Datenverarbeitungen ausschließlich innerhalb der Europäischen Union oder in Staaten mit angemessenem Datenschutzniveau vornehmen.

Der Weg zum „sicheren Hafen“ für personenbezogene Daten war am Ende des Jahres 2015 ist also noch lang – aber der LfDI Rheinland-Pfalz trug seinen Teil dazu bei, dass „Kurs gehalten“ werden konnte.

2. Die Ebene des Bundes

2.1 Allgemeines

Die Überwachung der Kommunikation durch ausländische Nachrichtendienste ist nach wie vor von großer Brisanz, auch wenn seit den Enthüllungen von Edward Snowden im Jahr 2013 die Empörung in der Öffentlichkeit eher zurückzugehen scheint. Den Hintergrund dürfte die Stärkung des Bedürfnisses nach Sicherheit bilden, die aufgrund der Bedrohungen durch den internationalen Terrorismus und die konkreten Anschläge insbesondere von Paris und Istanbul, aber auch in arabischen oder afrikanischen Staaten die öffentliche Meinung beherrscht. Immerhin ist das Thema der Überwachung aber deutlich stärker als Dauerthema im Bewusstsein vieler Bürgerinnen und Bürger verankert und hat auch zu politischen Reaktionen geführt.

Der Deutsche Bundestag hat auf Antrag aller Fraktionen (BT-Drs. 18/843) am 20. März 2014 einen Untersuchungsausschuss zur NSA-Affäre eingesetzt. Zweck ist, Umfang und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufzuklären. Die Beziehungen der Geheimdienste sind dem Charakter nach undurchsichtig, allerdings begründet genau dies die Notwendigkeit demokratischer Kontrolle. Die Kooperation der deutschen Nachrichtendienste mit Diensten anderer Staaten muss auf der Grundlage des deutschen Verfassungsrechts erfolgen. Im Mittelpunkt des öffentlichen Interesses steht die Zusammenarbeit des Bundesnachrichtendienstes mit den US-amerikanischen Diensten, die offenbar viele Erscheinungsformen hat und insbesondere den Datenaustausch betrifft.

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I 2015, S.1324) hat eine Steigerung der IT-Sicherheit zum Ziel und betrifft damit auch die Sicherheit der Datenübermittlung und Datenverarbeitung. Betreiber sogenannter „kritischer Infrastrukturen“, wozu auch die Betreiber von Webseiten zählen, müssen ein Mindestniveau an IT-Sicherheit einhalten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bzw. der Bundesnetzagentur IT-Sicherheitsvorfälle melden. Diese Meldepflichten bezwecken die Sicherstellung von Selbstkontrolle und Fremdkontrolle.

Nach langen Diskussionen und politisch befördert von den Terroranschlägen des Jahres 2015 ist die Neuregelung der Vorratsdatenspeicherung zum 18. Dezember 2015 in Kraft getreten. Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I 2015, 2218) versucht, die eingrenzenden Vorgaben des Bundesverfassungsgerichts (BVerfGE 125, 260) und des Europäischen Gerichtshofs (Rs. C-293/12, C-594/12 – vgl. oben) aufzugreifen (Roßnagel, NJW 2016, 533). Die Speicherfrist beträgt grundsätzlich zehn Wochen, Inhaltsdaten sollen nicht gespeichert werden. Angesichts der deutschen und europäischen Rechtsprechung ist aber der Spielraum so eng, dass das Gesetz letztlich nicht als verfassungsgemäß bewertet werden dürfte. Die Erhebung der Daten von Berufsgeheimnisträgern ist nicht effektiv ausgenommen und im Kern bleibt es bei der anlasslosen und verdachtslosen Speicherung der Kommunikationsdaten einer Vielzahl von Personen. Aufgrund der technischen Entwicklung sind Daten zudem immer schwerer abgrenzbar, so speichern Mobilfunkbetreiber wohl die Inhalte von SMS mit, weil diese nicht von den Verbindungsdaten zu trennen seien. Die ersten Verfassungsbeschwerden sind im Februar 2016 bereits eingelegt worden, das Bundesverfassungsgericht wird das Gesetz auf seine Verfassungsmäßigkeit zu untersuchen haben.

2.2 Gesetz zur Bekämpfung von Doping im Sport

Im Dezember 2015 trat nach heftiger Diskussion das Gesetz zur Bekämpfung von Doping im Sport in Kraft (BGBl. I 2015, S. 2210). Zweck des Gesetzes soll es sein, „den Einsatz von Dopingmitten und Dopingmethoden im Sport zu bekämpfen, um die Gesundheit der Sportlerinnen und Sportler zu schützen, die Fairness und Chancengleichheit bei Sportwettbewerben zu sichern und damit zur Erhaltung der Integrität des Sports beizutragen.“

Der Staat muss mit den ihm zur Verfügung stehenden Mitteln zum Schutz der Gesundheit und

zum Schutz der Integrität des Sports sowie zur Kriminalitätsbekämpfung und Dopingbekämpfung beitragen. Angesichts der erheblichen Gesundheitsgefahren geht es darum, mit Nachdruck gegen den illegalen Markt im Dopingbereich vorzugehen. Staatlicherseits soll gegen Doping im organisierten Sport eingeschritten werden, damit nicht die ethisch-moralischen Grundwerte des Sports und damit seine Grundlagen beschädigt werden. Verwiesen wird dabei auf zwei völkervertragliche Verpflichtungen der Bundesrepublik Deutschland, Maßnahmen zur Dopingbekämpfung zu ergreifen (Internationales Übereinkommen vom 19. Oktober 2005 gegen Doping im Sport, BGBl. 2007 II S. 354, 355, und Übereinkommen vom 16. November 1989 gegen Doping, BGBl. 1994 II S. 334, 335). Art. 4 Abs. 4 des Gesetzes zu dem Übereinkommen vom 16.11.1989 und Art. 5 des Gesetzes zu dem Internationalen Übereinkommen vom 19. Oktober 2005 gegen Doping im Sport sehen vor, dass die Bundesrepublik Deutschland als Vertragsstaat Vorschriften gegen Doping sowie politische Maßnahmen durchführen oder Verwaltungspraktiken anwenden kann. Nach Art. 12 a) des Internationalen Übereinkommens vom 19. Oktober 2005 gegen Doping im Sport werden die Vertragsstaaten in geeigneten Fällen es fördern und erleichtern, dass Sportorganisationen und Anti-Doping-Organisationen in ihrem jeweiligen Hoheitsbereich Dopingkontrollen entsprechend den Vorgaben des Welt-Anti-Doping-Codes durchführen; hierzu gehören unangekündigte Kontrollen, Kontrollen außerhalb des Wettkampfs und während des Wettkampfs. Bereits in diesem Zusammenhang ist festzuhalten, dass die Erreichung der völkervertraglichen Verpflichtungen mit geltendem europäischen Datenschutzrecht (Art. 8 der GRCh sowie die Vorgaben der EG-Datenschutzrichtlinie 95/46/EG) und nationalem Datenschutzrecht (Art. 1 GG i.V.m. Art. 2 Abs. 1 GG und Vorschriften des Bundesdatenschutzgesetzes) im Einklang stehen muss.

Von besonderem Interesse aus Datenschutzsicht sind die §§ 8 bis 11 des Gesetzes (§ 8 – Informationsaustausch, § 9 – Umgang mit personenbezogenen Daten, § 10 – Umgang mit Gesundheitsdaten, § 11 – Schiedsgerichtsbarkeit). Das mit dem Gesetz verfolgte Ziel, eine gesetzliche Grundlage für Anti-Doping-Maßnahmen zu schaffen, ist aus datenschutzrechtlicher Sicht zu begrüßen, da es bei der Dopingbekämpfung zwangsläufig zu einer Vielzahl sensibler Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der zahlreichen Athletinnen und Athleten kommt.

Die Datenschutzaufsichtsbehörden erhielten bereits Beschwerden von betroffenen Sportlerinnen und Sportlern, die sich über die Verletzung ihres Grundrechts auf informationelle Selbstbestimmung bei der Vorbereitung, der Durchführung, der weiteren Behandlung von Dopingkontrollen sowie beim weiteren Prozedere beschweren. Im Zentrum der Beschwerden stehen das in Kanada gehostete Meldesystem ADAMS sowie Vorfälle bei der von vielen Athletinnen und Athleten als entwürdigend empfundenen Abgabe von Urinproben unter Aufsicht von Kontrollpersonen. Die Datenschutzaufsichtsbehörden stellten bei ihren Prüfungen teilweise massive Datenschutzverstöße fest, die jedoch wegen der besonderen Rahmenbedingungen des internationalen Anti-Doping-Systems nicht verhindert oder beendet werden konnten. Das Anti-Doping-System wird derzeit von vielen Beteiligten als weltweit vorgegeben und alternativlos dargestellt. Ohne dessen Akzeptanz wäre es – so die Argumentation der Sportlerinnen und Sportler – nicht möglich, sich an nationalen oder internationalen Wettkämpfen zu beteiligen.

Es wird von den Datenschutzaufsichtsbehörden anerkannt, dass ein globales System der Dopingbekämpfung bei internationalen Sportveranstaltungen notwendig ist. Dieses muss aber die Menschenrechte auf Privatheit und Wahrung der Intimsphäre sowie auf Schutz der persönlichen Daten angemessen berücksichtigen und im Einklang mit dem europäischen und deutschen Datenschutzrecht stehen.

Die Datenschutzbehörden sind seit einigen Jahren mit der Nationalen Anti Doping Agentur Deutschland (NADA) und dem Deutschen Olympischen Sportbund (DOSB) im Gespräch, um einen adäquaten Ausgleich zwischen Persönlichkeitsschutz und wirksamer Dopingbekämpfung zu erreichen. Auf Grundlage der in der Vergangenheit geführten Gespräche verfassten der LfDI und

das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein bereits am 26. Juli 2011 ein Positionspapier mit dem Titel „Datenschutz und Dopingbekämpfung“, in welchem die datenschutzrechtliche Problematik umfassend dargestellt und aufgearbeitet wird (vgl. 23. Tb., Tz. II-2.4; 24. Tb., Tz. II-7.6). Am 29. April 2015 fand ein Gespräch zwischen den Datenschutzbehörden und dem DOSB in Neu-Isenburg statt, um die beabsichtigten Regelungen des Anti-Doping-Gesetzes zu diskutieren.

Die bisherige rechtliche Legitimation für die personenbezogene Datenverarbeitung erfolgt über Einwilligungen der betroffenen Sportlerinnen und Sportler, die jedoch den nationalen wie den europäischen datenschutzrechtlichen Anforderungen nicht genügen. Die Einwilligungen werden unter Verletzung von Art. 8 Abs. 2 der GRCh und Art. 7a) der EG-Datenschutzrichtlinie 95/46/EG i.V.m. § 4a Abs. 1 BDSG nicht freiwillig erteilt, sind zu unbestimmt und erlauben zumindest teilweise unverhältnismäßige Eingriffe in das Recht auf informationelle Selbstbestimmung.

Aus Sicht der Datenschutzbehörden offenbart das nunmehr verabschiedete Gesetz gravierende Mängel: Durch die pauschale Bezugnahme im Gesetzestext auf „das Dopingkontrollsystem der Stiftung Nationale Anti Doping Agentur Deutschland“ (§ 8 Abs. 1, § 9, § 10 Abs. 1 und 2 des Gesetzes) entledigt sich der Gesetzgeber seiner Aufgabe, selbst einen Ausgleich der widerstreitenden einschlägigen Interessen, nämlich dem Interesse an einem fairen und gesundheitlich verantwortbaren Wettkampfsport einerseits und dem Interesse der Sportlerinnen und Sportler an der freien Ausübung ihres Berufs sowie an der Wahrung ihrer Privat- und Intimsphäre andererseits, zu finden. Durch die dynamisch angelegte Verweisung auf die jeweiligen Regelungen des Dopingkontrollsystems der NADA wird der Gesetzgeber seiner verfassungsrechtlichen Verpflichtung nicht gerecht, selbst eine angemessene Problemlösung zu finden. Weiterhin fehlen jegliche verfahrensrechtlichen Absicherungen, indem keine Aussage zu Auskunfts-, Benachrichtigungs-, Widerspruchs-, Berichtigungs- und Löschrechten der Sportlerinnen und Sportler getroffen wird. Organisatorische Vorkehrungen werden nicht ansatzweise geregelt, um die notwendige Datensicherheit (z.B. Zugangs-, Zugriffs-, Eingabe- und Weitergabekontrolle) zu gewährleisten.

Es besteht eine staatliche Schutzpflicht, für das Recht auf informationelle Selbstbestimmung einzutreten. Staatliche Stellen müssen die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitstellen (BVerfG, Beschluss v. 17. Juli 2013, 1 BvR 3167/08, Rn. 20). Diese Schutzpflicht zwecks effektiver Realisierung digitaler Grundrechte besteht in besonderem Maße bei internationaler arbeitsteiliger und sensibler Datenverarbeitung. Sie obliegt in erster Linie dem Gesetzgeber. Mit dem verabschiedeten Gesetz wurde der Gesetzgeber dieser Schutzverpflichtung nicht gerecht. Die vom Gesetz intendierte Verzahnung der Tätigkeiten staatlicher Behörden mit der NADA führt zu ganz erheblichen Spannungen mit den rechtsstaatlichen Vorgaben (Unschuldsvermutung, Garantie des Rechtswegs), an welche Staatsanwaltschaften und Strafgerichte gebunden sind.

3. Die Ebene des Landes

3.1 Allgemeines

Beratungs- und Serviceleistungen stehen für die Behörde seit Jahren im Vordergrund, sie sollen ausdifferenziert und gestärkt werden. Ganz in diesem Sinne hat der LfDI gemeinsam mit der Landesregierung im Oktober 2015 eine Landesdatenschutzkonferenz einberufen, auf der gerade kleinen und mittleren Unternehmen in Rheinland-Pfalz wichtige Hinweise zur Erhöhung des Datenschutzniveaus etwa im Wege der Auditierung und Zertifizierung gegeben wurden. Wenn und soweit dies möglich und erforderlich ist, soll auch die kommunale Ebene auf den Gebieten Datenschutz und Informationsfreiheit unterstützt werden (vgl. Tz. III-2.3, III-14.7).

Im Hinblick auf private Unternehmen sind die Aufgaben als Aufsichtsbehörde zu erfüllen und zugleich die Gegebenheiten der digitalen Wirtschaft zu berücksichtigen. Aufsichtsbehördliche Mittel wie Bußgelder stehen zur Verfügung, eine konstruktive und transparente Beratung und Information wie in der Folge der Safe Harbor-Entscheidung des Europäischen Gerichtshofs (vgl. Tz. I-1.4, I-1.5) ist aber als ebenfalls wichtiges Mittel zur Wahrung des Datenschutzes im nicht-öffentlichen Bereich zu werten.

3.2 Änderung der Gemeinde- bzw. Landkreisordnung

Mit dem Landesgesetz zur Verbesserung direktdemokratischer Beteiligungsmöglichkeiten soll u.a. die Öffentlichkeit von Rats- und Ausschusssitzungen gestärkt werden. Mit den Änderungen, die insgesamt der Willensbildung und der Kontrolle der kommunalen Vertretungskörperschaft und ihrer Mitglieder durch die Öffentlichkeit dienen sollen, wird auch einer Empfehlung der Enquête-Kommission des Landtags „Aktive Bürgerbeteiligung für eine starke Demokratie“ entsprochen.

Die Änderungen stehen im Zeichen der Förderung von Transparenz im kommunalen Verwaltungshandeln. Als Mittel zum Zweck dient insbesondere das Internet. Von wesentlicher datenschutzrechtlicher Bedeutung war dabei eine rechtssichere Regelung der sog. Medienöffentlichkeit, um über digitale Aufzeichnungen und Bild- und Tonübertragungen von Rats- und Ausschusssitzungen die Einwohnerinnen und Einwohner am kommunalen Geschehen teilhaben zu lassen. Wesentliche Rechtsgrundlagen sind nunmehr § 35 Abs. 1 S. 4 bis 6 GemO, § 28 Abs. 1 S. 4 bis 6 LKO und § 7 Abs. 3 BezO.

Bereits 2013 hatte sich der LfDI dahingehend positioniert, dass ein sog. Livestream von öffentlichen Ratssitzungen ohne spezifische Rechtsgrundlage nur mit Einwilligung aller möglicherweise Betroffenen umsetzbar ist. Begründet wurde dies damit, dass eine Rechtsgrundlage dafür nicht in § 35 Abs. 1 GemO (§ 28 Abs. 1 LKO) als die lediglich die Saal- bzw. Sitzungsöffentlichkeit regelnde Vorschrift gesehen werden kann. Denn Ziel dieser Vorschrift ist es, den Bürgerinnen und Bürgern zum Zweck der demokratischen Kontrolle und Teilhabe Einblick in die Tätigkeit kommunaler Vertretungskörperschaften zu gewähren. Deshalb ist die Öffentlichkeit lokal begrenzt, eine weltweite Zugriffsmöglichkeit bzw. Verbreitung über das Internet nicht erforderlich und über diese Vorschrift (bisher) nicht zulässig.

Aus der Sicht des Informationsfreiheitsbeauftragten ist im Sinne der Transparenz festzuhalten, dass Bemühungen, politische Prozesse einer breiten Öffentlichkeit zugänglich zu machen, grundsätzlich begrüßens- und unterstützenswert sind.

Da ein Livestream auf der Grundlage einer Einwilligung aller Ratsmitglieder und sonstiger möglicherweise Betroffenen, wie z.B. Beschäftigte oder Zuhörerinnen und Zuhörer, in der Praxis nicht oder nur schwer umsetzbar gewesen wäre, konnte nur der Erlass einer entsprechenden gesetzlichen Grundlage weiterhelfen. Dieser Standpunkt hatte auch seinen Niederschlag in der Verwaltungsvorschrift zu § 41 GemO gefunden.

Zur Einführung der Medien- anstelle der Saalöffentlichkeit hat der LfDI mit seiner Stellungnahme im Gesetzgebungsverfahren angeregt, eine Befristung der Veröffentlichung und die anschließende Entfernung einer Aufzeichnung aus dem Internetangebot in die Vorschrift aufzunehmen. Dabei wäre für eine adäquate Dauer der Veröffentlichung ein nachlassendes Informationsinteresse der Öffentlichkeit über Angelegenheiten einer örtlichen Gemeinschaft zu würdigen. Leider wurde dieser Ergänzungsvorschlag nicht berücksichtigt.

Gemäß der Gesetzesbegründung überlassen es die o.g. Vorschriften den Mandatsträgerinnen und -trägern vor Ort, die Hauptsatzung entsprechend zu ändern, wenn sie Bild- und Tonaufnahmen sowie Bild- und Tonübertragungen wollen. An dieser Stelle kann auch Näheres zur Art und Weise geregelt werden, wie z.B.

- eine Befristung der Veröffentlichung;
- eine zeitversetzte Übertragung;
- eine sog. Podcast-Lösung. Damit ist gemeint, dass die Bürgerinnen und Bürger ebenfalls zeitversetzt ganz gezielt auf den Filmbeitrag zu einem bestimmten Tagesordnungspunkt zugreifen können.

II. Ausgewählte Schwerpunkte

1. Bildung und Erziehung

(Basierend auf einem Vortrag, den der LfDI am 18. Mai 2015 vor der Gemischten Kommission der Kultusministerkonferenz gehalten hat.)

Die digitale Entwicklung geht rasant weiter. Anfang 2010 hatte Facebook noch 5,7 Millionen aktive Nutzerinnen und Nutzer in Deutschland, im Mai 2015 sind es 28 Millionen. Den Messengerdienst WhatsApp gab es damals noch gar nicht. Mittlerweile verwenden ihn weltweit mehr als 800 Millionen Nutzerinnen und Nutzer. Einige Dienste, wie z.B. mySpace mit ehemals 200 Millionen Mitgliedern sind vom Markt verschwunden; die datenschutzfreundlichen VZ-Netzwerke hat dasselbe Schicksal ereilt. Andere Dienste sind neu hinzugekommen. Hierzu zählen etwa Instagram, Snapchat oder die problematische Selbstdarstellungsplattform für Jugendliche mit dem Namen „youNow“.

Angesichts dieser rasanten technischen Veränderungen stellt sich die Frage, ob die „Digitale Bildung“ in den Schulen mit dieser Entwicklung Schritt halten kann.

In Rheinland-Pfalz wurde mit dem Regierungsprogramm „Medienkompetenz macht Schule“ die „digitale Bildungsarbeit“ vorangebracht: Das 2007 gestartete Projekt sah neben der informationstechnischen Ausstattung der Schulen vor, dass Schülerinnen, Schüler, Lehrkräfte und Eltern ihre Kompetenzen in Bezug auf digitale Medien und das Internet ausbauen konnten; u.a. wurden rund 2.100 Lehrkräfte für die Aufgabe eines Jugendmedienschutzberaters qualifiziert und mehr als 1.300 Schülerinnen und Schüler zu Medienscouts ausgebildet.

In einer Ende 2015 veröffentlichten Ländervergleichsstudie „Länderindikator 2015 – Schule digital“ der Deutschen Telekom Stiftung ist Rheinland-Pfalz unter den Top 3 vertreten. Die Studie basiert auf einer repräsentativen Befragung von 1.250 Lehrkräften bundesweit, in Rheinland-Pfalz wurden nach dem Zufallsprinzip 80 Lehrkräfte interviewt. Die Studie bescheinigt den Schulen in Rheinland-Pfalz unter anderem, dass sehr häufig digitale Medien im Unterricht eingesetzt werden, dass sie dafür über eine gute Ausstattung verfügen und dass in sehr hohem Maße detaillierte, schuleigene Konzepte zur Medienbildung vorhanden sind.

In seiner gegenwärtigen Fassung sieht das Zehn-Punkte-Programm „Medienkompetenz macht Schule“ der Landesregierung u.a. vor, Jugendmedienschutz und Datenschutz als Bildungsaufgabe zu implementieren, den MedienkomP@ss zu etablieren, den Ausbau der schulischen Infrastruktur zu forcieren und umfassende Informationen und Bildungsmedien bereitzustellen.

Um das Landesprogramm weiter zu entwickeln, wurde von Bildungsministerin Vera Reiß eine Expertenrunde ins Leben gerufen, die sich u.a. aus Vertretern der Universitäten Mainz und Trier, der Technischen Universität Kaiserslautern, der Landeszentrale für Medien und Kommunikation, dem Pädagogischen Landesinstitut sowie dem LfDI zusammensetzt. In der konstituierenden Sitzung machte die Ministerin deutlich, dass der Begriff „Medienkompetenz“ neu gefasst werden müsse hin zur „digitalen Kompetenz“ und dass eine Erhöhung der Verbindlichkeit von Medienkompetenzinhalten anzustreben sei.

Aus Sicht des LfDI ist dies zu unterstützen. Dies gilt sowohl für die Vermittlung von Medienkompetenz- und Datenschutzkompetenzinhalten in Bezug auf Schülerinnen und Schüler als auch im Rahmen der Fort- und Weiterbildung der Lehrkräfte.

Die sogenannte ICILS-Studie (International Computer and Information Literacy Study), die Ende 2014 veröffentlich wurde, zeigt insoweit die Dringlichkeit und den Bedarf: In der Studie wurden erstmalig die computer- und informationsbezogenen Kompetenzen von Schülerinnen und Schülern der 8. Jahrgangsstufe international vergleichend untersucht. Die deutschen Kinder landeten hier allenfalls im mittleren Bereich, in vielen Punkten belegten sie sogar nur die hinteren Ränge. Ein Drittel unserer Schülerinnen und Schüler verliert der Studie zufolge den Anschluss und kann mit den neuen Technologien nicht sinnvoll umgehen.

Die Studien bestätigen, was der LfDI nach über fünf Jahren des Schülerworkshop-Projektes an Erfahrungen sammeln konnte: Das Referententeam be-

richtet darüber, dass offenbar eine erhebliche Diskrepanz herrscht zwischen der Selbsteinschätzung der eigenen Kompetenz und dem tatsächlichen Wissen, das bisweilen eher als gering einzuschätzen ist und auf ein mangelndes Problembewusstsein und einen unreflektierten Umgang mit Medien schließen lässt.

Aus Sicht des LfDI sind aus dieser Bestandsaufnahme folgende Schlussfolgerungen zu ziehen:

1. Die vorliegenden Beschlüsse der Kultusministerkonferenz (KMK) müssen evaluiert werden. Nach der KMK-Erklärung zur Medienbildung in der Schule aus dem Jahr 2012 ist es nunmehr an der Zeit, eine Zwischenbilanz zu ziehen, um mit guten Beispielen zu in der KMK-Erklärung aufgeführten Handlungsfeldern der Medienbildung in der Schule Anregungen zu geben und so den weiteren Prozess zu befördern.

2. Wir brauchen in allen Bundesländern eine Bestandsaufnahme aller Maßnahmen, die von den Schulen derzeit zur Förderung der Medienkompetenz angeboten werden, und wir brauchen deren Evaluation, was wiederum heißt, dass dafür Bildungsstandards und Kriterien festgelegt werden müssen, die zudem über die Messung rein technischer Fertigkeiten hinausgehen müssen. Davon sind wir allerdings noch weit entfernt. Medienkompetenzvermittlung verläuft allem Anschein nach unter dem Motto: „Wo etwas unterrichtet wird, wird wohl auch etwas hängen bleiben." Der Bedeutung dieses Themas und den damit verbundenen Herausforderungen wird man damit aber nicht gerecht.

3. Medienführerscheine, Medienkompetenz, Medienbildung und Medienkunde greifen angesichts der Entwicklung zur totalen Digitalisierung unserer Lebenswelt zu kurz.

   Über die digitalen Medien hinaus gibt es digitale Entwicklungen, die nicht zu den Medien gezählt werden können, RFID etwa, NFC, Location-based Services und ähnliches mehr.

   Notwendig ist deshalb eine über die Medienbildung hinausgehende digitale Bildung. Diese umfasst zwar die Medienbildung, die aber selbst nur ein Baustein der digitalen Grundbildung ist. Insoweit geht die Bundesregierung in die richtige Richtung, wenn sie in ihrer Digitalen Agenda vom 20. August 2014 von einer Medien- und Informationskompetenz spricht, welche die Chancen und Risiken digitaler Technologie in den Blick nehmen muss.

4. Mittelpunkt einer digitalen Bildung kann etwa ein schulisches Kern- oder Leitfach sein, was nicht ausschließen muss, dass daneben Medienbildung auch noch fächerübergreifend vermittelt werden kann. Dies wird zumindest teilweise gefordert.

   Informatik als Wahlpflichtfach könnte nicht ausreichen, zumal sich immer mehr abzeichnet, dass die Nachfrage in den Schulen stetig ansteigt, so dass sie – jedenfalls in Rheinland-Pfalz – von den Schulen zum Teil schon gar nicht mehr befriedigt werden kann.

   Wichtig zumindest als Ergänzung sind fakultative Angebote und Pilotprojekte, auch mit externen Sachverständigen sowie Medienführerscheine und Datenschutzworkshops der Datenschutzbeauftragten.

   Informatik bereits in der Grundschule zu vermitteln, wie dies die Große Koalition gefordert hat, führt dabei sicherlich in die richtige Richtung. Entsprechende Forderungen greifen aber womöglich zu kurz, weil sie im Zweifel den gesellschaftlichen und wertebezogenen Rahmen der digitalen Entwicklung nicht hinreichend behandeln und übrigens auch deren datenschutzrechtliche Auswirkungen vernachlässigen.

   Deshalb plädieren die Datenschutzbeauftragten dafür, den Datenschutz auch als Bildungsaufgabe zu begreifen und ihn in die Medienkompetenzförderung einzubeziehen, was allerdings eine sehr komplexe Aufgabe ist. Denn das beinhaltet die Vermittlung des dem Datenschutz zugrunde liegende Wertekanons, die Vermittlung der Funktionsbedingungen des digitalen Zeitalters, die Sensibilisierung für die Risiken, die mit diesen Funktionsbedingungen verbunden sind, die Vermittlung der Datenschutzrechte und der Möglichkeiten, sich im Netz selbst helfen zu können. Am Ende muss ein Bewusstsein dafür geschaffen werden,

dass es im Netz nicht nur Rechte, sondern auch Pflichten gibt, rücksichtsvoll und respektvoll mit den Daten und insbesondere Bildern anderer umzugehen.

5. Wenn man dieses Ziel wenigstens ansatzweise erreichen will, muss sichergestellt werden, dass die schulischen Angebote zur Förderung digitaler Kompetenzen mit der Geschwindigkeit, in der sich die digitale Technologie entwickelt, wenigstens im Ansatz Schritt halten. Nur dann können sie aktuell sein, nur dann sind sie hilfreich. Ohne digitale Lernplattformen, die bei Bedarf immer mit Updates aktuell gehalten werden können, wird dies nicht möglich sein.

Auf Bundesebene liegt seit März 2015 mit dem Antrag der Regierungskoalitionen ein viel versprechendes Papier vor (BT-Drs. 18/4422). Der Antrag zielt darauf ab, „durch Stärkung der Digitalen Bildung die Medienkompetenz (zu) fördern“: Darin wird u.a. gefordert, z.B. durch einen Länderstaatsvertrag folgende Punkte zu regeln:

- bundeseinheitliche Mindeststandards für digitale Informations- und Medienkompetenz und deren regelmäßige Überprüfung durch eine Ländervergleichsstudie;
- die Evaluation bestehender Programme zur Förderung der Medienkompetenz;
- die Förderung eines zeitgemäßen Informatikunterrichts ab der Grundschule;
- die Verankerung digitaler Bildungsinhalte in den Bildungsplänen der Länder,
- die Aufnahme digitaler Medienkompetenz in die Studiengangs- und Ausbildungscurricula sowie Prüfungsordnungen von Lehrkräften sowie die Schaffung bzw. den Ausbau spezieller Fortbildungsangebote für bereits ausgebildete Lehrkräfte.

Diese Forderungen sind aus Sicht des LfDI zu begrüßen, wobei es noch detaillierter Aussagen über die konkreten Bildungsinhalte bei der Umsetzung durch die Länder bedarf. Der LfDI wird sich in der genannten Expertenrunde für die Umsetzung der im Antrag genannten Forderungen auf Landesebene einsetzen. Anknüpfungspunkte finden sich in der europäischen Datenschutz-Grundverordnung.

2. Bußgeldverfahren gegen die Debeka

Die Ordnungswidrigkeitenverfahren, die der LfDI im Dezember 2013 gegen den Debeka-Krankenversicherungsverein a.G. (Debeka) und gegen seine Vorstandsmitglieder eingeleitet hatte, sind im Dezember 2014 mit einem Bescheid des LfDI im Wege der Verständigung abgeschlossen worden. Darin wurde die Debeka verpflichtet, eine Geldbuße in Höhe von 1,3 Millionen Euro zu zahlen – das ist die höchste Geldbuße, die jemals von einer deutschen Datenschutzbehörde verhängt wurde.

Anlass der Untersuchungen waren einige vom Unternehmen eingeräumte Fälle sog. Listenkäufe, bei denen einzelne Beschäftigte weisungswidrig Datensätze zu Anwärterinnen und Anwärtern im öffentlichen Dienst erworben und genutzt hatten. Diese Fälle wurden umfassend untersucht. Dabei wurde festgestellt, dass in einigen Fällen unter Missachtung des Datenschutzes Neukundinnen und -kunden für die Debeka durch Informationen von Kolleginnen und Kollegen gewonnen wurden. Einzelne Debeka-Beschäftigte hatten Listen oder Kontaktdaten möglicher Kundinnen und Kunden ohne deren Einverständnis erhalten und dafür zum Teil auch ein Entgelt bezahlt. Hierbei verstießen sie gegen unternehmensinterne Vorgaben, aber auch gegen geltendes Datenschutzrecht. Die Debeka musste feststellen, dass in der Vergangenheit nicht alle Aufsichtsmaßnahmen und Kontrollen etabliert und angewandt worden waren, die aus heutiger datenschutzrechtlicher Sicht den notwendigen Standards entsprechen. Seit 2013 sind solche Aufsichtspflichtverletzungen mit erheblich gesteigerten Bußgeldern bedroht, die nun erstmals auch verhängt wurden.

Insbesondere die Zusammenarbeit der Debeka mit Tippgeberinnen und -gebern wurde vom LfDI umfassend überprüft und bewertet. Das Datenschutzrecht steht nach Auffassung des LfDI dem Einsatz von Tippgeberinnen und -gebern allerdings nicht grundsätzlich entgegen. Unter beratender Einbeziehung des LfDI wurde der Vertrieb mit Tippgeberinnen und -gebern bei der Debeka so ausgerichtet, dass die Arbeit der Tippgeberinnen und -geber zukünftig die gesetzlichen Standards für den Datenschutz auch nach Einschätzung des LfDI sogar übertreffen wird. So ist etwa eine Weitergabe von Adressen über Tippgeberinnen und -geber zukünftig nur noch bei Vorliegen einer förmlichen Einwilligungserklärung jeder oder jedes einzelnen Betroffenen möglich.

Die Debeka und der LfDI sprechen übereinstimmend von einer sehr konstruktiven Aufarbeitung der datenschutzrelevanten Vorgänge im Vertrieb der Debeka. Dies führte letztlich dazu, dass eine langwierige gerichtliche Auseinandersetzung und Klärung mit für beide Seiten ungewissem Ausgang nicht gesucht, sondern – trotz teilweise unterschiedlicher Rechtsauffassungen – zur Erledigung aller im Raum stehender Vorwürfe das genannte Bußgeld gezahlt wurde. Die Verfahren gegen die Vorstände wurden ohne Bußgeldzahlungen eingestellt.

Bei der Höhe der Bußgeldbemessung wurden zugunsten der Debeka ihre umfassende Kooperation mit dem LfDI, ihre eigene Aufklärung sowie die zugesagte Stiftungsprofessur berücksichtigt. Auch die Bereitschaft der Debeka, bei der Anwerbung neuer Kundinnen und Kunden künftig strikt auf die Einhaltung einschlägiger Datenschutzvorschriften zu achten, wurde ebenso in die Bemessung einbezogen wie die vorbildliche Optimierung einer neuen, weitgreifenden internen Datenschutzstruktur.

Mit der Beendigung des Verfahrens konnten alle gegen die Debeka erhobenen Vorwürfe von Aufsichtspflichtverletzungen im Bereich des Datenschutzes aufgearbeitet werden. Vorstand und Aufsichtsrat des Unternehmens akzeptierten die Geldbuße, die umgehend beglichen wurde. Der LfDI und die Debeka konnten damit die Auseinandersetzung um die Vergangenheit abschließen und den Blick nach vorne wenden.

Das Unternehmen stellte darüber hinaus zusätzlich 600.000 Euro für eine Stiftungsprofessur bereit, die mittlerweile an der Johannes Gutenberg-Universität Mainz, Fachbereich Rechts- und Wirtschaftswissenschaften, eingerichtet werden konnte. Damit wird die Debeka die Grundlagenforschung für einen effektiven Datenschutz und dessen Implementierung in der Praxis nachhaltig fördern.

Der LfDI erklärte sich am 29. Dezember 2014 mit dem Ausgang des Verfahrens zufrieden. „Wichtiger als das verhängte Bußgeld ist mir zweierlei: Zum einen hat die Debeka ernsthafte und erfolgreiche Anstrengungen

unternommen, den Datenschutz in ihrem Vertriebssystem zu stärken. Ohne das kooperative Verhalten der Debeka wäre ein solch gutes Ergebnis nicht zu erzielen gewesen. Zum anderen geht von dem Verfahren das Signal aus, dass alle Unternehmen zukünftig mit noch mehr Nachdruck daran arbeiten müssen – und können! –, dass mit den persönlichen Daten von Interessenten, Kunden und Mitarbeitern vertrauensvoll und rechtskonform umgegangen wird."
Auch der Debeka-Vorstandsvorsitzende begrüßte die einvernehmliche Klärung der datenschutzrechtlichen Auseinandersetzung: „Der konstruktive Dialog mit dem LfDI hat zur Beseitigung von Fehlerquellen geführt und die grundsätzliche Zulässigkeit von Tippgebern bestätigt. Wir haben damit die Vergangenheit aufgearbeitet und schauen nun nach vorne. Mit den getroffenen Maßnahmen hält die Debeka die Datenschutzbestimmungen nicht nur ein – sie übertrifft sie sogar. Damit sind wir für die Zukunft bestens gerüstet. Wir freuen uns auch, an der Universität Mainz die wissenschaftliche Aufarbeitung von datenschutzrechtlichen Fragestellungen zu fördern."

Auch im öffentlichen Bereich wurden durch die Änderung der Nebentätigkeitsbestimmungen und durch die Aufarbeitung von Datenschutzverstößen erste wichtige Konsequenzen gezogen und die Überwachungs- und Kontrollmechanismen den heute geltenden Standards angepasst. Zukünftig sind Tätigkeiten als „Tippgeber“ ausdrücklich genehmigungspflichtig, so dass die jeweiligen Vorgesetzten bzw. Behördenleiterinnen und -leiter die Verantwortung dafür übernehmen müssen, wenn öffentlich Bedienstete „nebenher“ in diesem Bereich tätig werden. Dadurch soll insbesondere der illegale Zugriff auf dienstliche Verzeichnisse von Beschäftigten, Anwärterinnen und Anwärtern und Bewerberinnen und Bewerbern wirksam unterbunden werden.

Gegen Beschäftigte des öffentlichen Dienstes Rheinland-Pfalz geführte Ordnungswidrigkeitsverfahren mussten allerdings eingestellt werden. Da die Beschuldigten in vielen Fällen mit Kenntnis der Behördenleitung, teilweise sogar mit deren Genehmigung gehandelt hatten, konnte letztlich kein ausreichender Schuldvorwurf erhoben werden.

3. #watch22

Der Datenschutz wird üblicherweise unter rechtlichen, technischen und ggf. auch medienpädagogischen Gesichtspunkten behandelt. Der Kreis der Bürgerinnen und Bürger, die auf diese Weise erreicht werden, ist allerdings begrenzt.

Vor diesem Hintergrund entstand der Plan, sich dem Datenschutz einmal aus ganz anderer Perspektive zu nähern und vorhandenes Datenschutzverständnis zu bestärken und neues zu gewinnen: aus der Perspektive der Kunst und der Kultur. Auf diese Weise soll versucht werden, nicht nur den Verstand, sondern auch die Emotionen anzusprechen und so einen neuen Zugang zum Thema Datenschutz zu legen.

Im 22. Stock eines Mainzer Hochhauses präsentierte eine Ausstellung über vier Wochen im Mai 2015 20 künstlerische Arbeiten – überwiegend Medieninstallationen, aber auch andere Arbeiten – von rheinland-pfälzischen, deutschen und internationalen Künstlern, die sich mit der Privatsphäre und dem Datenschutz, d.h. der Sammlung, Vernetzung und Nutzung privater Informationen durch die globalen Informationstechnologien beschäftigen und breiteres Publikum für diese zentralen Fragen auf spielerisch-künstlerische Art sensibilisieren sollten. Begleitend dazu fanden in Kooperation mit zahlreichen Partnern aus Kultur, Wirtschaft und Politik Workshops, Diskussionen, Vorträge, Lesungen, Performances und Filmvorführungen statt.

Mit dem Begriff Datenschutz werden so vielfältige und unterschiedliche Aspekte in Verbindung gebracht wie Videoüberwachung, Vorratsdatenspeicherung, Internet der Dinge, Verlust der Privatheit, Internetspuren, Kontrolle am Arbeitsplatz, Mobilfunkortung. Auch bildende Künstlerinnen und Künstler beschäftigen sich mit diesen Themen. Dabei verfolgen sie die unterschiedlichsten Strategien. Sie zeigen Möglichkeiten der Tarnung und des Versteckens auf, sie nutzen dieselben Mittel wie die Überwacher und legen sie damit offen, sie ironisieren durch Übertreibung, sie täuschen Überwachung und Vernetzung vor, sie dokumentieren Fehler und Absurditäten der Datensammlung, oder sie publizieren bislang unbekannte Orte, Methoden und Techniken des „Big Brother“ – ob dieser nun die Gestalt von Behörden, Geheimdiensten oder internationalen Konzernen hat.

Kunstobjekte, Installationen, interaktiven Projekte, Performances oder Video- und Computerarbeiten stehen oft auf hohem technologischem Niveau. Die Künstlerinnen und Künstler sind zu Forschern, Erfindern, Technikern und Wissenschaftlern geworden. Denn ebenso wie die Sammlung, Vernetzung und Nutzung privater Daten heute immer die moderne Informationstechnologie voraussetzt, ist die künstlerische Sensibilisierung für diese Themen auf dieselben Techniken angewiesen und zählt damit in der Regel zur Medienkunst.

Fast immer findet sich in entsprechenden Arbeiten zudem ein spielerischer, teils ironischer Ansatz. Die Werke erschließen sich in der Regel sofort und setzen bei den Betrachtenden keine kunsthistorische Vorbildung voraus – sie sind unmittelbar optisch und akustisch zu erfassen und intuitiv verständlich. Grundeigenschaften der Medienkunst – Faszination durch Technologie und Überraschungseffekte durch neuartige Sichtweisen – machte sich die Ausstellung zunutze, um ein offenes Publikum für Fragestellungen des Datenschutzes zu sensibilisieren.

Die 20 größeren Arbeiten von deutschen (gerade auch rheinland-pfälzischen) und internationalen Künstlerinnen und Künstlern wurden ergänzt um Arbeiten von Studierenden der Hochschule Mainz sowie weiterer Ausbildungsstätten aus den Fachbereichen Medienkunst, Kommunikationsdesign, Film/Video und Fotografie.

Auch intuitiv erfassbare Kunstwerke bedürfen der begleitenden Erläuterung. Diese wurde sichergestellt durch Führungen für allgemeines Publikum und Gruppen (Schulen usw.), Künstlergespräche in der Ausstellung, praktische Workshops zu verschiedenen Themen (z.B. Umgang mit sozialen Netzwerken, Datenspuren im Internet, Crypto-Sessions, Selbstdatenschutz) sowie Vortragsveranstaltungen und Podiumsdiskussionen mit einschlägigen Referenten zu den Themen Privatheit, Digitale Revolution, Internet der Dinge usw.

Eine Unterbringung der Ausstellung in einer klassischen Institution (Museum, Kunsthalle) wurde bewusst vermieden, um eine möglichst breite Publi-

kumswirksamkeit außerhalb des Kunstkontexts zu erzielen, freie Hand in der Ausstellungsarchitektur zu haben und den besonderen, einzigartigen Charakter des Projekts zu betonen. Als idealer Ausstellungsort erwies sich das 22. Stockwerk im Turm A der Bonifaziustürme. Dies ist der höchste Aussichtspunkt von Mainz, sonst nicht öffentlich zugänglich und schon von daher besonders attraktiv. Die Ausstellungsetage (ca. 500 qm) ist entkernt und ermöglichte eine freie Gestaltung.

Ein umfangreiches Kulturprogramm sollte einerseits weitere Aspekte des Datenschutzes sichtbar machen und andererseits Publikumsgruppen aus anderen Sparten für das Kunst- und Kulturprojekt mobilisieren. Zahlreiche kulturelle und politische Institutionen haben begleitenden Veranstaltungen durchgeführt, u.a. das kommunale Kino CinéMayence, das Literaturbüro Rheinland-Pfalz, das Staatstheater, die Mainzer Kammerspiele, die Landeszentrale für politische Bildung Rheinland-Pfalz, die Verbraucherzentrale Rheinland-Pfalz, der Landesmediendienst mit dem Institut für Medienpädagogik und die Akademie der Wissenschaften und der Literatur.

Außerdem fand eine Zusammenarbeit mit dem Performance Art Depot (pad), dem Chaos Computer Club (Berlin und Mainz/Wiesbaden), der freien Theatergruppe Ignous, Theatergruppen der Universität Mainz, der Landeszentrale für Medien und Kommunikation, der Volkshochschule Mainz, dem Poetry Slam Mainz, dem Haus des Jugendrechts und dem Haus der Medienbildung statt.

Musikalische Werke mit unmittelbarem Bezug zum Darstellungsthema rahmten den Zyklus an Veranstaltungen ein. Eine Aufführung des Stücks „Ich akzeptiere die Nutzungsbedingungen“ (von Google) des bekannten zeitgenössischen Komponisten Moritz Eggert fand im Plenarsaal des rheinland-pfälzischen Landtags am 20. Mai 2015 statt. In dem Stück sind Auszüge aus den Nutzungsbedingungen von Google für Klavier und Bariton vertont.

Ein musikalisches Bühnenstück zu Überwachung, Angst, Macht und Voyeurismus schloss das Projekt ab. Die „Mono-Oper“ von Francis Poulenc – aufgeführt am 30. Mai 2015 im Foyer der Westdeutschen Immobilienbank Mainz – handelt von einer „gläsernen Sängerin“, die in einem von allen Seiten transparentem Bühnenkäfig mit einem unsichtbaren und unhörbaren Gegenüber telefoniert. Das Publikum wird dabei in die Rolle des Wissenden, Beobachtenden, Kontrollierenden gesetzt und beobachtet den höchst einseitigen Kommunikationsvorgang bis in den Tod der Sängerin hinein. Darüber hinaus fanden Straßenaktionen, Performances, Lesungen und Filmvorführungen statt.

Um die politische, rechtliche und technologische Seite des Datenschutzes in das Programm einzubinden, wurden eine Reihe von Veranstaltungen und Podiumsdiskussionen durchgeführt, etwa zur Abschaffung des Bargelds durch digitale Bezahlformen, zum Internet der Dinge oder zur Überwachungstätigkeit der NSA. Bekannte Persönlichkeiten wie Bundesjustizministerin a.D. Sabine Leutheusser-Schnarrenberger, die IT-Unternehmerin Yvonne Hofstetter oder Constanze Kurz vom Chaos Computer Club bereicherten das Veranstaltungsprogramm.

Auch spezielle Schülerworkshops, ein Coding Camp und mehrere sog. Crypto-Sessions wurden durchgeführt, in denen es darum ging, einem interessiertes Publikum zu zeigen, wie Daten verschlüsselt und Datenspuren im Netz vermieden werden können.

Das Gesamtprojekt wurde vom Essenheimer Kunstverein e. V. veranstaltet in Kooperation mit zahlreichen Partnerveranstaltern, die sich mit eigenen Mitteln am Programm beteiligten. Schirmherr war der LfDI, Hauptförderer der Kultursommer Rheinland-Pfalz.

In den vier Wochen zwischen Eröffnung und Finissage haben knapp 3.200 Besucherinnen und Besucher an #watch22 und seinen Programmpunkten teilgenommen. Besonders gut besucht waren die Eröffnungsveranstaltung im Bonifaziusturm, die Mainzer Museumsnacht im Turm, die Mono-Oper am 30. Mai 2015 sowie eine Kooperationsveranstaltung mit der Zukunftsinitiative Rheinland-Pfalz (ZIRP) zum Thema „Big Data – Smart Data“ am 13. Mai 2015.

Zahlreiche Berichte in Presse und Fernsehen, darunter in 3sat und dem SWR, rundeten die außergewöhnliche Veranstaltung ab.

4. Datenschutzfragen bei der Aufnahme und der Betreuung von Flüchtlingen und Asylbewerbern

Der Zustrom von Flüchtlingen und Asylbewerberinnen und -bewerbern hat unter datenschutzrechtlichen Aspekten ganz unterschiedliche Fragen hervorgerufen:

- Wie kann datenschutzkonform erreicht werden, dass die Registrierungen effektiver erfolgen können (Vermeidung von Mehrfacherfassungen etc.)?

  Diese in der Praxis drängende Frage wurde durch das Gesetz zur Verbesserung der Registrierung und des Datenaustausches zu aufenthalts- und asylrechtlichen Zwecken (Datenaustauschverbesserungsgesetz) einer im Grundsatz datenschutzgerechten Lösung näher gebracht. Kernpunkte des neuen Verfahrens sind die Erweiterung und bessere Nutzbarkeit des Ausländerzentralregisters sowie die Einführung eines besonderen „Flüchtlingsausweises“, der „Ankunftsnachweis“ genannt wird. Der LfDI hat zu dem Gesetzentwurf gegenüber der Landesregierung Stellung genommen und keine inhaltlichen Bedenken erhoben. Er hat für die Phase der Umsetzung darauf hingewiesen, dass auch hier die technisch-organisatorischen Standardanforderungen des Datenschutzes zu beachten sind: Vor allem ist ein adäquates Berechtigungskonzept umzusetzen, und es sind angemessene Zugriffsprotokollierungen vorzusehen.

- Wie können die ehrenamtlichen Helferinnen und Helfer (z.B. Sprachmittlerinnen und -mittler) in angemessenem Umfang datenschutzkonform über die zu betreuenden Flüchtlinge informiert werden?

  Basis muss die informierte Einwilligung der Flüchtlinge sein, solange die ehrenamtlichen Helfer nicht förmlich zu „Ehrenbeamten“ i.S. des Landesbeamtengesetzes ernannt worden sind.

- Dürfen Ortsbürgermeisterinnen und Ortsbürgermeister die Identitätsdaten der in ihre Gemeinde Zuwandernden erfahren?

  Auf der Grundlage des Melderechts ist dies für alle Personen, die ihren Wohnsitz in der Ortsgemeinde begründet haben, zulässig. Für Bewohnerinnen und Bewohner mit nur temporärem Aufenthalt in Gemeinschaftsunterkünften gilt dies aber nicht.

- Wie kann die Zusammenarbeit der Gemeinden mit der Bundesanstalt für Arbeit (bzw. den Jobcentern) datenschutzkonform erfolgen? Wie kann die Tätigkeit der „Jobpiloten“ unter dem Aspekt der Informationsverarbeitung in dieses Verfahren integriert werden?

  Hierfür reichen die geltenden Regelungen des Asylverfahrensgesetzes und des Aufenthaltsgesetzes (i.V.m. dem Landesdatenschutzgesetz) aus. Die Asylbewerberdaten, die nach dem Asylbewerberleistungsgesetz erfasst worden sind, unterliegen nicht dem Sozialgeheimnis. Soweit keine speziellen Datenverarbeitungsregeln existieren, kommt das Landesdatenschutzgesetz ergänzend zur Anwendung. Die Voraussetzungen einer zulässigen Übermittlung von Basisdaten der in Betracht kommenden Flüchtlinge an die „Jobpiloten“ liegen danach vor.

- Wenn Einwilligungen erforderlich sind: Wie sollen diese aussehen?

  Ausreichende Information und Freiwilligkeit sind die entscheidenden Anforderungen.

- WLAN in Flüchtlingsunterkünften: Ist eine Registrierung der Flüchtlinge zur Haftungsreduzierung des WLAN-Betreibers zulässig?

  Eine Registrierung ist zeitlich und im Datenumfang eng begrenzt sowie strikt zweckgebunden zulässig.

- Auf welcher Rechtsgrundlage können die ärztlichen Betreuerinnen und Betreuer bzw. Gesundheitsämter über die bei anderen Stellen (etwa den Erstaufnahmeeinrichtungen) erhobenen Daten ihrer Patientinnen und Patienten unterrichtet werden?

  Das Asylverfahrensgesetz verpflichtet zur ärztlichen Betreuung. Das dazu Erforderliche darf an

Nachbehandelnde weitergegeben werden, ansonsten sind Einwilligungen erforderlich.

- Unter welchen Voraussetzungen ist die Ausstellung von „Gesundheitspässen“ für Asylbewerberinnen und -bewerber bzw. Flüchtlinge zulässig?

  Die Ausstellung und Aushändigung der Daten (auch im Wege eines ausgefüllten Gesundheitspasses) an die Betroffenen bedarf keiner besonderen Rechtsgrundlage. Die Befugnis hierfür ergibt sich aus dem Behandlungsverhältnis mit den Betroffenen. Die Nutzung und Weiterverwendung der Daten im Rahmen einer neuen Behandlung bedarf der Einwilligung der Betroffenen, die dadurch konkludent erteilt wird, dass der Pass in Kenntnis der Freiwilligkeit an den neuen Behandelnden weitergegeben wird.

- Welchen Bedingungen muss eine technische Plattform für den Austausch von Gesundheitsdaten von Flüchtlingen zwischen den berechtigten Stellen entsprechen?

  Hier ist besonderer Wert auf die technisch-organisatorischen Datenschutzanforderungen nach § 9 LDSG zu legen, da besondere Arten von Daten i.S. des § 3 Abs. 8 LDSG betroffen sind.

- Welche datenschutzrechtlichen Bedingungen muss ein Geodatenportal „Erstaufnahmeeinrichtungen“ erfüllen? Dürfen dort Daten von Personen (Ansprechpartnerinnen und -partnern) zum Abruf bereit gehalten werden?

  Das Portal kann Daten von Ansprechpartnerinnen und -partnern enthalten, wenn diese Daten auf bloße dienstliche Erreichbarkeitsinformationen beschränkt sind (§ 33 LDSG). Zudem dürften die betroffenen Daten ohnehin bereits (an anderen Stellen im Netz) veröffentlicht sein.

- Darf die Polizei eine Liste der Flüchtlingsunterkünfte (einschließlich der Adressen privat vermieteter Wohnungen/Häuser) bei der Gemeinde anfordern und speichern?

  Eine gesetzliche Grundlage für die Datenerhebung, -speicherung und –übermittlung ist deshalb erforderlich, weil diese Adressdaten zumindest personenbeziehbare Daten der Eigentümerinnen und Eigentümer der Liegenschaften (der Vermieterinnen und Vermieter) sind. Eine Rechtsgrundlage hierfür kann allerdings grundsätzlich dem Polizei- und Ordnungsgesetz entnommen werden, wenn die Daten zur Gefahrenabwehr benötigt werden.

Der LfDI hat sich bemüht, alle an ihn gerichteten Fragen in einer praxisgerechten Weise so zu beantworten, dass die Persönlichkeitsrechte der betroffenen Flüchtlinge bzw. Asylbewerberinnen und -bewerber gewahrt bleiben.

Die bisherigen Rückmeldungen haben nicht ergeben, dass der Datenschutz insoweit als unpraktikabel angesehen worden wäre oder dass berechtigte und schutzwürdige Belange der betroffenen Flüchtlinge beeinträchtigt werden würden.

III. Sachgebiete des Datenschutzes – Ausgewählte Ergebnisse aus der Prüfungs- und Beratungstätigkeit des LfDI

1. Medien und Telekommunikation

1.1 smart TV – Ich weiß, was Du fernsiehst!

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals auch die Möglichkeit, ergänzende Angebote und Dienste aufzurufen. Den Zuschauerinnen und Zuschauern ist es damit möglich, simultan zum laufenden Programm zusätzliche Webinhalte auf dem Bildschirm anzeigen zu lassen. Auch Endgerätehersteller bieten über eigene Webplattformen für Smart-TV-Geräte verschiedenste Dienste an.

Für die Zuschauerinnen und Zuschauer ist aufgrund dieser Verzahnung der Online- mit der Fernsehwelt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internetdienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich dabei handelt, von wem dieser erbracht wird und an wen die Daten über dessen Nutzung fließen. Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal von Zuschauerin oder Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Diensteanbietern, über den das individuelle Nutzungsverhalten erfasst und ausgewertet werden kann.

Aus Sicht des LfDI muss die Möglichkeit, Fernsehprogramme anonym zu nutzen, erhalten bleiben. Gegenüber den Nutzerinnen und Nutzern muss Transparenz hergestellt werden, und es müssen ihnen Kontroll- und Steuermöglichkeiten zur Verfügung stehen. Sie müssen sich darauf verlassen können, dass Dritte nicht ungewollt und nicht beeinflussbar erfahren, was, wann und wie oft oder wie lange man fernsieht. Die Datenschutzaufsichtsbehörden haben hierzu eine gemeinsame Position formuliert und eine Orientierungshilfe veröffentlicht, in der die Anforderungen an eine datenschutzgerechte Gestaltung von Smart-TV dargestellt sind. Damit sollen Fernsehzuschauerinnen und -zuschauer, die parallel das Internet nutzen wollen, in die Lage versetzt werden, solche Geräte auszuwählen, die die Möglichkeit einer datenschutzfreundlichen Konfiguration und Nutzung bieten.

Smartes Fernsehen nur mit smartem Datenschutz
Gemeinsame Position der Aufsichtsbehörden im nichtöffnetlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich rechtlichen Rundfunkanstalten
http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=201405xxUmlauf_smarttv

Orientierungshilfe „Smart TV“
http://www.datenschutz.rlp.de/downloads/oh/oh_smart-TV.pdf

Das Bayerische Landesamt für Datenschutzaufsicht hat in einer bundesweit abgestimmten Prüfung Smart-TV Geräte von 13 Herstellern mit insgesamt ca. 90 Prozent Marktabdeckung in Deutschland untersucht, welche Daten bei Nutzung der Geräte fließen, an wen sie fließen, ob nur die Daten fließen, die für den Betrieb notwendig sind, und welche Möglichkeiten Fernsehnutzerinnen und -nutzer haben, dies zu erkennen und ggf. auf den Datenfluss Einfluss zu nehmen.

Ergebnisse der Smart TV Datenschutz-Prüfung:

http://www.datenschutz.rlp.de/de/aktuell/2015/images/BayLDA_SmartTV_Technische_Pruefung.pdf

Auf Bitte des LfDI hat sich auch ein rheinland-pfälzischer Hersteller an der Prüfung beteiligt und ein entsprechendes Gerät zur Verfügung gestellt. Hier hat die Prüfung ergeben, dass bei der Gerätesoftware, den Abläufen bei der Produktregistrierung und -aktualisierung sowie im Rahmen des Angebots eigener Informationsdienste Anpassungen erforderlich sind. Der Hersteller hat sich im Rahmen der Prüfung durchgängig kooperativ gezeigt und zugesagt, die notwendigen Änderungen vorzunehmen. Diese werden für künftige Modelle sowie für alle vergleichbaren Endgeräte (z.B. Satelliten-Receiver) umgesetzt.

1.2 Die AGB von Google – ist eine datenschutzgerechte Problemlösung absehbar?

Gemeinsam mit den Aufsichtsbehörden aus Frankreich, Großbritannien, Italien, Niederlande und Spanien hat der Hamburgische Datenschutzbeauftragte (der aufgrund des Hauptsitzes der Deutschlandniederlassung von Google primär zuständig ist) die Datenverarbeitung durch Google geprüft.

Google räumt sich in der Datenschutzerklärung das Recht ein, die gesetzlich vorgeschriebene Trennung der bei der Nutzung von verschiedenen Diensten entstehenden personenbezogenen Informationen zu überwinden und sämtliche Daten miteinander zu verbinden. Dadurch ist Google in der Lage, detaillierte Profile der einzelnen Nutzerinnen und Nutzer zu erstellen, die Auskünfte über die Interessen, Vorlieben, Kommunikationsbeziehungen und das Nutzungsverhalten der Betroffenen geben. Für die Betroffenen ist dies nicht transparent; aus der Datenschutzerklärung von Google ergibt sich dies nicht deutlich. Hierfür bedürfte es aber einer gesetzlichen Grundlage oder einer entsprechenden Einwilligung der Nutzerinnen und Nutzer.

Im September 2014 erließ der Hamburgische Datenschutzbeauftragte einen Verwaltungsakt gegen Google, die der LfDI inhaltlich in vollem Umfang unterstützte. In dieser wurde Google verpflichtet, die Nutzungs-, Bestands- und Inhaltsdaten von Nutzerinnen und Nutzern nur in dem durch das Telemediengesetz und das Bundesdatenschutzgesetz zulässigen Umfang zu Profilen zusammenzuführen.

Derzeit ist diese Verwaltungsanordnung Gegenstand eines Rechtsstreits vor dem Verwaltungsgericht Hamburg. Es ist bisher nicht abzusehen, wann das Gericht sich mit der Klage inhaltlich befassen wird.

Google hat allerdings auf die datenschutzrechtlichen Bedenken der Aufsichtsbehörden reagiert und mit der Umsetzung verschiedener Maßnahmen zur Verbesserung des Datenschutzes begonnen. Dazu gehört zum einen die Überarbeitung der Datenschutzerklärung (vgl. 25. Tb. des Hamburgischen Datenschutzbeauftragten, Tz. V-I.2).

Zum anderen verlangt Google im Hinblick auf die Erstellung von Profilen der Nutzerinnen und Nutzer seit Oktober 2015 von diesen eine Einwilligung in die dienstübergreifende Zusammenführung der Daten aus den verschiedenen Diensten. Außerdem werden die Nutzerinnen und Nutzer über verschiedene Einstellmöglichkeiten unterrichtet, mit denen sie auf den Umfang der Datenverarbeitung einwirken können. Dies ist jedenfalls ein positiver Beginn, auf die Datenschutzanliegen einzugehen. Derzeit dauert die Prüfung an, ob und welche weiteren Schritte von Google noch realisiert werden müssen, um den Datenschutzanliegen zu entsprechen.

1.3 Die Nutzung von Facebook-Fanpages durch Behörden

Das Datenschutzproblem, das sich durch die Nutzung von Fanpages bei Facebook durch Behörden stellt, ist seit vielen Jahren Gegenstand der Aufmerksamkeit des LfDI und wurde in den vergangenen Tätigkeitsberichten bereits ausführlich geschildert (vgl. 23.Tb., Tz. I-3.2.2; 24. Tb., Tz. II-7.4.4).

Facebook selbst hält sich nicht an die deutschen Datenschutzvorgaben beim Umgang mit den Nutzerdaten. Diese Anforderungen ergeben sich hauptsächlich aus dem Telemediengesetz. Danach sind die Nutzerinnen und Nutzer über den Umgang mit ihren Nutzungsdaten umfassend und deutlich aufzuklären. Eine Profilbildung in personenbezogener Form darf nicht stattfinden; hierfür müssen Pseudonyme gebildet werden, eine Reidentifizierung darf grundsätzlich nicht erfolgen. Die Nutzerinnen und Nutzer müssen außerdem die Möglichkeit haben, auch einer solchen Profilbildung zu widersprechen. Alle Nutzerinnen und Nutzer müssen die Möglichkeit haben, einen solchen Dienst nicht mit ihrem richtigen Namen, sondern unter einem Pseudonym zu nutzen. Schließlich darf ein Dienstebetreiber wie Facebook nicht mithilfe von Cookies oder auf sonstige Weise das Surfverhalten seiner angemeldeten Nutzerinnen und Nutzer im Netz umfassend verfolgen.

All diese Vorgaben missachtet Facebook, und Stellen, die in Form einer eigenen Facebook-Fanpage einen „Honigtopf“ aufstellen, erzeugen weitere Nutzungsdaten und tragen dazu bei, dass Facebook

fortfährt wie bisher. Hier besteht eine eigene Verantwortung besonders der staatlichen Stellen.

Die Datenschutzproblematik bei der Facebook-Nutzung wird noch dadurch verstärkt, dass nicht ausgeschlossen werden kann, dass alle von Facebook verarbeiteten Daten (sowohl Nutzungs- wie Inhaltsdaten) letztlich auf Servern landen, die dem rechtsstaatlich bedenklichen Zugriff der US-Sicherheitsbehörden (vor allem der NSA) unterliegen. Zudem ist aus Sicht US-amerikanischer Behörden das Unternehmen Facebook verpflichtet, seine Daten – gleich, wo sie verarbeitet werden – diesen Behörden auf Verlangen zur Verfügung zu stellen (vgl. auch Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015, Rs. C 362/14, und die Stellungnahme des Generalanwalts in diesem Verfahren, http://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-EuGH-Generalanwalt-nennt-Safe-Harbour-ungueltig-2823994.html).

Rechtlich ist diese Situation umstritten. Die erwartete gerichtliche Klärung ist bislang noch nicht erfolgt. Das Oberverwaltungsgericht Schleswig hat zwar entschieden, dass allein Facebook und nicht die Fanpage-Betreiber für die o.g. Rechtsverstöße verantwortlich sei (Urteil vom 4. September 2014, Az. 4 LB 20/13). Das inzwischen angerufene Bundesverwaltungsgericht hat hier aber – ebenso wie die Datenschutzbeauftragten des Bundes und der Länder – Zweifel. Es hat jedoch vorläufig von einer Entscheidung abgesehen und die offenen Fragen dem Europäischen Gerichtshof zur Beantwortung vorgelegt, weil aus seiner Sicht in diesem Zusammenhang das europäische Recht vorrangige Regeln enthalte, deren Auslegung Sache des europäischen Gerichts sei (Vorlagebeschluss des Bundesverwaltungsgerichts vom 25. Februar 2016, Az. 1 C 28/14).

Aus der Sicht des LfDI folgt daraus, dass seine Rechtsauffassung zunächst dem Grunde nach aufrecht erhalten wird: Der von ihm formulierte Handlungsrahmen für öffentliche Stellen, die Facebook-Fanpages betreiben und der die damit einhergehenden Rechtsverstöße minimieren soll, sollte von allen Fanpage-Betreibern beachtet werden.

Fundstelle des Handlungsrahmens:
http://www.datenschutz.rlp.de/de/faq.php?submenu=inet

1.4 Fragen zum Open Access über WLAN bei Kommunen

Datenschutzfragen stellen sich bei einem öffentlichen WLAN-Zugang bzw. beim „Freifunk“ in erster Linie dann, wenn der Anbieter des WLANs bzw. des „Freifunks“ (also z.B. eine Gemeinde) wegen der möglicherweise eingreifenden Störerhaftung die Nutzerdaten erfassen will. Dann nämlich würden sensible Nutzerdaten „auf Vorrat“ gespeichert werden.

Wenn darauf verzichtet werden würde (was aus der Sicht des Datenschutzrechts völlig unproblematisch wäre), würden an dieser Stelle keine Datenschutzprobleme entstehen.

Beim sog. „Freifunk“ gibt es unterschiedliche Modelle. Würde der „Freifunk“ durch einen privatrechtlich organisierten Verein (z.B. den „Freifunk-Verein“) erfolgen, wäre die Gemeinde für die Erhebung und Speicherung von Nutzungs- und Nutzerdaten nicht verantwortlich. Dann hätte allerdings dieser Verein sich bezüglich des Umfangs und der Dauer der Speicherung von Nutzungsdaten an den Grundsätzen der Erforderlichkeit und der Datensparsamkeit zu orientieren. Hier gilt das Prinzip der Datensparsamkeit: Nur die absolut erforderlichen Daten dürfen für eine begrenzte Zeit unter ausreichenden technisch-organisatorischen Sicherungen gespeichert werden.

Ein weiterer Aspekt tritt hinzu: Da im Allgemeinen keine Verschlüsselung für die Übertragung der Nutzerdaten zum Access-Point der verantwortlichen WLAN-Betreiber eingerichtet wird, sollten die Nutzerinnen und Nutzer auf diesen Schwachpunkt hingewiesen werden. Bezüglich der Speicherung von Nutzungsdaten durch den WLAN-Betreiber bestehen ebenfalls Informationspflichten gegenüber den Nutzerinnen und Nutzern sowie die Pflicht zur Einrichtung technisch-organisatorischer Sicherungsmaßnahmen gegen zweckwidrige Auswertungen.

1.5 Der Rundfunkbeitrag – er beschäftigt den Datenschutz noch immer

In den beiden letzten Tätigkeitsberichten hat der LfDI die Fragen dargestellt, die beim Erlass des Rundfunkbeitragsstaatsvertrags aus Datenschutz-

sicht bedeutsam waren (vgl. 23. Tb., Tz. II-1.1; 24.Tb., Tz. I-3.4.7). Er hat auch auf das seinerzeit vor dem Verfassungsgericht des Landes anhängige Verfassungsbeschwerdeverfahren gegen den Rundfunkbeitragsstaatsvertrag und seine Beteiligung daran hingewiesen. Im aktuellen Berichtszeitraum ist das Urteil gefällt worden (Urteil vom 13. Mai 2014, Az. VGH B 35/12): Das Verfassungsgericht hat alle erhobenen verfassungsrechtlichen Bedenken, auch die datenschutzrechtlich motivierten, (letztere in Übereinstimmung mit dem LfDI) für unbegründet angesehen. Damit befindet es sich im Gleichklang mit allen bisher mit diesen Fragen befassten Gerichten (z.B. auch dem Bayerischen Verfassungsgerichtshof, Urteil vom 18. April 2013 und dem Bundesverfassungsgericht vom 17. März 2016).

Im Berichtszeitraum wurde die von den Landesgesetzgebern geforderte Evaluation des Rundfunkbeitragsstaatsvertages vorgelegt. Es hat sich nicht ergeben, dass Unzuträglichkeiten in Bezug auf den Datenschutz festzustellen gewesen wären. Die Rundfunkanstalten sehen allerdings einen Bedarf an der Durchführung eines erneuten Abgleichs ihres gesamten Adressdatenbestandes mit dem Melderegister. Dies ist auf deutliche Kritik aller Datenschutzbeauftragten gestoßen. Dennoch wird der Rundfunkbeitragsstaatsvertrag entsprechend geändert werden. Dies ist zu bedauern. Zu begrüßen ist demgegenüber, dass die bislang nur in den Satzungen der Rundfunkanstalten verankerten datenschutzfreundlichen Konkretisierungen des Rundfunkbeitragsstaatsvertrages nunmehr in den Vertrag selbst aufgenommen werden sollen. Damit wird mehr Rechtssicherheit und Rechtsklarheit im Interesse des Datenschutzes geschaffen.

Durch das neue Beitragsmodell sind alle Eingaben entfallen, die die Tätigkeit der sog. „Gebührenbeauftragten“ betroffen haben. Dennoch gibt es immer wieder Nachfragen, die vor allem Zweifel daran äußern, ob der „Beitragsservice“ wirklich die Befugnisse hat und rechtlich wirksam ausüben darf, die er in Anspruch nimmt. Schwierigkeiten bereitet das Verständnis, dass die Rundfunkanstalten mithilfe dieser Institution hoheitlich tätig werden können. Hier ist der LfDI häufig damit befasst, die Rechtslage nachvollziehbar zu erklären.

1.6 Resignation oder Revanche? Die Methoden der Internetüberwachung durch die NSA und GCHQ und mögliche Gegenstrategien

Die Enthüllungen Snowdens zur Überwachung der Internetkommunikation haben ein Ausmaß der Überwachung offenbart, das selbst skeptischste Mutmaßungen übertroffen hat. Die Reaktionen schwanken zwischen Resignation und Revanche. Angesichts der Internetdominanz der USA und der technischen Fähigkeiten der NSA mögen Zweifel erlaubt sein, ob eine Gegenwehr überhaupt lohnt. Dennoch gibt es Möglichkeiten, der Sammelwut entgegenzutreten, um die Freiheit im Netz zu bewahren und digitale Grundrechte zu sichern.

1.6.1 Methodik und Reichweite der Überwachung

Die großflächige Überwachung der Internetkommunikation fußt im Wesentlichen auf zwei Ansätzen:

- Der Überwachung, Sammlung und Auswertung des über die globalen Kommunikationsverbindungen laufenden Datenverkehrs. Die Namen der entsprechenden Überwachungsprogramme lauten FAIRVIEW, STORMBREW, BLARNEY oder OAKSTAR, zusammengefasst unter dem Oberbegriff UPSTREAM. Erleichtert wird dies durch die Situation, dass ein Großteil der globalen Internetverbindungen über die USA führt oder von Ländern der sog. „Five Eyes“-Gruppe (z.B. Großbritannien) gebündelt wird. Hinzu kommt, dass die nationalen Telekommunikationsanbieter selbst nicht oder nur ausnahmsweise über eigene interkontinentale Verbindungen verfügen und sich hierzu globaler Provider bedienen, welche die Backbone-Strukturen des Internets betreiben. Bei einem Großteil davon handelt es sich um US-amerikanische Unternehmen.

- Der unter dem Namen PRISM laufenden Datensammlung direkt bei US-amerikanischen Anbietern von Internet- und Kommunikationsdiensten (Google, Facebook, Yahoo, Microsoft, Apple etc.). So vielfältig die von diesen angebotenen Dienste sind (E-Mail, Chat, Videoplattform, Videokonferenz, soziale Netzwerke, Cloud-Dienste usw.), so

vielfältig und zahlreich sind auch die dabei gewonnenen Daten.

Auch wenn Dienste eines europäischen Anbieters genutzt werden, erfolgen die Zugriffe aus Kapazitäts- oder Kostengründen häufig über die USA. Soweit die Zugriffe nicht verschlüsselt erfolgen, können auf diese Weise Verbindungs- und Inhaltsdaten abgegriffen werden. Der Anspruch der NSA auf eine möglichst vollständige Erfassung der Kommunikation wird mit offensivem Selbstbewusstsein vorgetragen. So meinte der ehemalige NSA-Chef Keith Alexander „Man braucht den Heuhaufen, um die Nadel zu finden".

Vor dem Angriff steht die Aufklärung; im Rahmen des HACIENDA-Projekts werden daher die IT-Systeme ganzer Länder automatisiert auf Schwachstellen, Verwundbarkeiten in der Infrastruktur der Netze und potentielle Nutzbarkeit hin untersucht.

Die dargestellten Verfahrensweisen betreffen zunächst die technischen Möglichkeiten der Überwachung. Der Natur von Nachrichtendiensten entsprechend bleibt vielfach offen, wie viele Personen konkret betroffen sind. Auch der im Juni 2014 erstmals veröffentlichte Transparenzreport der NSA bleibt hier in vielen Punkten unklar. Konkrete Hinweise auf die Reichweite der Internetüberwachung liefern jedoch Äußerungen, wonach unter Umständen die Kommunikationspartner der zweiten und dritten Ebene („two or three hops") überwacht werden. Oder, in der Terminologie sozialer Netzwerke, die Freunde von Freunden von Freunden. Bei angenommenen 150 elektronischen Kontakten einer Person innerhalb eines bestimmten Zeitraums (Telefonate, Textnachrichten, E-Mails, Postings, Kommentaren, Likes, Shares etc.) wären dies im dritten Schritt mehr als drei Millionen Betroffene. 90 Prozent davon sind unverdächtig.

1.6.2 Die Macht der Metadaten

Ein Effekt der Snowden-Veröffentlichungen ist, dass die Bedeutung der sog. Metadaten, d.h. die eine Kommunikation arrondierenden, von den eigentlichen Inhalten losgelösten Informationen, in das öffentliche Bewusstsein gehoben wurde. Zwar sind Informationsgehalt und Aussagekraft von Metadaten keine neue Erkenntnis, wie sehr sie Kommunikationsverhalten, Lebensumstände, Interessen, Vorlieben oder Mobilitätsverhalten der Nutzerinnen und Nutzer offenbaren und zum Teil voraussagen lassen, war in der allgemeinen Öffentlichkeit bislang jedoch weitgehend unbekannt. Dass Zeitpunkt, Ort, Dauer und Rufnummern eines Telefonats auch ohne den Inhalt des Gesprächs interessantes Wissen bergen, konnte man schon den eigenen Einzelverbindungsnachweisen entnehmen. Dass ein Tweet von 140 Zeichen mit seinen ca. 40 Metainformationen in weiten Teilen das kommunikative Umfeld des Absenders erkennen lässt, ist vielen nicht bekannt. Gerade soziale Netzwerke mit ihren verquickten Beziehungen eröffnen mit ihren Metadaten eine wahre Fundgrube der Erkenntnis. Die Geschäftsmodelle Facebooks und Googles basieren gerade auf dieser Transparenz ihrer Nutzerinnen und Nutzer.

Metadaten sind jedoch auch die eher unauffälligen Begleitdaten eines Internetzugriffs: IP-Adressen, Cookies, Browserdaten, App-IDs oder Geräte-Fingerprints. Diese werden ergänzend zu E-Mail-Adressen, Telefonnummern oder Login-Namen als „weiche Selektoren" genutzt, um im steten Datenstrom des Internets relevante Kommunikationspartner oder Datenzugriffe ausfindig zu machen. Auch wenn Nutzerinnen und Nutzer Cookies löschen, ihren Browser aktualisieren oder ein anderes Endgerät nutzen, beim nächsten E-Mail-Abruf, der nächsten Anmeldung am sozialen Netzwerk oder dem nächsten Besuch der Suchmaschine werden die Selektoren ergänzt bzw. auf den neuesten Stand gebracht und verknüpft.

Dies erlaubt über die Auswertungsprogramme XKEYSCORE und BOUNDLESS INFORMANT Abfragen nach dem Muster „Meine Zielperson nutzt Google Maps. Kann ich dies nutzen, um ihre E-Mail-Adresse herauszufinden? Wonach hat sie im Web gesucht?" oder „Meine Zielperson spricht deutsch und hält sich in Pakistan auf; wie kann ich sie ausfindig machen?"

Die Konzentration der Datensammlung auf Metadaten hat auch einen pragmatischen Grund: das Internetdatenvolumen ist letztlich zu groß, um dauerhaft alles zu erfassen. Auch die Heuhaufen-Doktrin erfordert eine Schwerpunktsetzung, und diese liegt bei der Erfassung, Speicherung und Auswertung von

Metadaten. Während die mit dem Schleppnetz der NSA erfassten Inhaltsdaten für drei Tage gepuffert werden, werden Metadaten in den beiden Hauptdatenbanken MARINA (Internet) und MAINWAY (Telefonie) bis zu einem Jahr vorgehalten. Filterungs- und Selektionsprozesse oder aktuelle Anforderungen entscheiden darüber, welche Daten für einen längeren Zeitraum oder dauerhaft gespeichert werden.

1.6.3 Gegenstrategien

Gründe genug also, um in Resignation zu verfallen. In der Tat, die Internetüberwachung reicht weit und wer in den Fokus der NSA gerät, hat wenig Möglichkeiten, sich dieser zu entziehen. Auch Revanchegelüste mögen angesichts einer empfundenen Hilflosigkeit verständlich sein, anzuraten ist beides nicht, bestehen auf unterschiedlichen Ebenen doch Möglichkeiten, der massenhaften Ausspähung entgegenzutreten.

- Persönlich haben die Nutzerinnen und Nutzer es in der Hand, auf Instrumente zurückzugreifen, die Vertraulichkeit oder Anonymität bieten. Auch die Empfehlungen der Datenschutzkonferenz gehen in diese Richtung. Trotz der technischen Kompetenz der NSA kann man laut Edward Snowden auf den Schutz durch starke Verschlüsselung vertrauen. Mag die NSA auch die eine oder andere Verschlüsselungslösung beherrschen, so lässt ihr Einsatz doch den Aufwand steigen und hilft, die Überwachung als Massenphänomen zurückzudrängen.

- Auf der technischen Ebene sollte daher der Einsatz von Verschlüsselungslösungen zum Regelfall werden. Erste Ansätze hierfür zeigen sich verstärkt auf Anbieterseite. Die Endnutzer wird man jedoch nur gewinnen können, wenn die Lösungen auch handhabbar sind.

- Das teils belächelte „Nationale Routing“ stellt einen weiteren Ansatz dar, die Zugriffsmöglichkeiten auf Datenströme zu reduzieren. Dabei geht es nicht um eine „Balkanisierung des Internets“, in Zeiten globalisierter Infrastrukturen ein ohnehin schwieriges Unterfangen, sondern um die Rückgewinnung der technologischen Souveränität, zumindest im Bereich der staatlichen Kommunikation.

- Auch auf der politisch-rechtlichen Ebene bietet sich eine Klaviatur an, auf der zu spielen sich lohnt. Die aktuelle Diskussion um das vom Europäischen Gerichtshof aufgehobene „Safe-Harbor-Abkommen“ zeigt, dass Datenschutzpolitik zunehmend Wirtschaftspolitik ist, bei der politische Instrumente eingesetzt werden können (vgl. Tz. I-1.4, I-1.5).

Vieles von dem, was Snowden enthüllt hat, hat seine Wurzeln im „9/11“-Anschlag in New York, und vieles geht auf eine blauäugige Unschuld zurück, mit der das Internet als neutrales Kommunikationsmedium betrachtet wurde. Für beides braucht es eine Neubewertung. Nicht resignativ, nicht revanchistisch sondern vorausschauend, klug und selbstbewusst. Wir können der Massenüberwachung des Internets etwas entgegensetzen und sollten dies auch tun.

2. Wirtschaft

2.1 Eingaben im privatwirtschaftlichen Bereich

Im öffentlichen Bereich nahm der Schutz des Grundrechts auf informationelle Selbstbestimmung seinen Anfang, mittlerweile ist die Datenverarbeitung durch private Stellen – inländische wie auch ausländische, die via Internet ihre Dienstleistungen anbieten, – von zentraler Bedeutung. Auch durch die Vielzahl der Datenschutzskandale der vergangenen Jahre in der Privatwirtschaft veränderte sich das Datenschutzbewusstsein in der Bevölkerung, denn besonders von diesem Bereich geht heutzutage ein ganz erhebliches Gefährdungspotential aus. Auch die Enthüllungen zum Datenhunger des staatlichen Geheimdienstes NSA untermauern diese Einschätzung. Sie betonen sie sogar, wenn man berücksichtigt, dass die NSA nur zum Teil eigenständige Datenerhebungen durchführt, in wesentlichen Bereichen aber auf die Datensammlungen von Privatunternehmen zugreift und diese auswertet: etwa die Verkehrsdatensammlungen privater Telekommunikationsfirmen oder die Datenspeicher von Facebook, Amazon und Co.

Dieser gesellschaftliche Wandel spiegelt sich auch in der Entwicklung der von Bürgerinnen und Bürgern an den LfDI gerichteten Eingaben im privatwirtschaftlichen Bereich wider. Im Berichtszeitraum 2014/2015 gab es rund 5.000 Anfragen. Davon erfolgten mehr als 700 in schriftlicher Form, die übrigen wurden fernmündlich an den LfDI herangetragen. Im Vergleich zum Berichtszeitraum 2012/2013 konnte hier ein weiterer Anstieg festgestellt werden, seinerzeit waren es knapp 4.000 Eingaben und Anfragen. Zu verzeichnen sind mittlerweile auch deutlich umfangreichere Rückfragen zur datenschutzrechtlichen Einschätzung einzelner Sachverhalte, was gewiss auf das gestiegene Datenschutzbewusstsein zurückgeführt werden kann. Aufgrund des Umfangs der schriftlichen und fernmündlichen Eingaben und Anfragen der Bürgerinnen und Bürger sowie verantwortlicher Stellen selbst sind beim LfDI allerdings personelle Kapazitätsgrenzen erreicht.

Schwerpunkte der Eingaben bilden nach wie vor die Bereiche Arbeitnehmerdatenschutz, Videoüberwachung, Werbung, Adresshandel, Internetnutzung, Wirtschaftsauskunfteien sowie Fragen zur Tätigkeit der betrieblichen Datenschutzbeauftragten. Generell ist – wie schon im vergangenen Berichtszeitraum – festzustellen, dass sich die Datenschutzprobleme im Bereich der Privatwirtschaft parallel zur exponentiellen Entwicklung der Kommunikationstechnik in immer kürzeren Zeiträumen steigern. Riesige Datenbestände mit teils sensiblen, in jedem Falle aber umfassenderen und damit höchst aussagekräftigen Informationen entstehen bei immer mehr privaten Unternehmen – Big Data ist keineswegs beschränkt auf die großen Unternehmen wie Amazon oder Google. Die Miniaturisierung von Datenträgern macht das unbefugte Kopieren und Übermitteln immer leichter, damit werden auch missbräuchliche Datenverwendungen in immer neuen Dimensionen möglich. Die Gefahren von Big Data im Internet, beruhend auf einer lückenlosen Erfassung und Auswertung des Nutzungsverhaltens, aber auch durch Identitätsdiebstähle, Phishing oder virtuellen Exhibitionismus sind ständige Begleiter aller Nutzerinnen und Nutzer. All das spiegelt sich auch in den Eingaben und Anfragen der Bürgerinnen und Bürger wider. Im privatwirtschaftlichen Bereich beschränkt sich die Beratungstätigkeit des LfDI aber nicht nur auf die von der Datenverarbeitung Betroffenen, sondern erstreckt sich weiter zunehmend auch auf die Unternehmen selbst. Wie sich die Situation mit Inkrafttreten der europäischen Datenschutz-Grundverordnung entwickeln wird, kann jetzt noch nicht zuverlässig eingeschätzt werden. Zu erwarten ist allerdings ein noch weiter gesteigertes Informations- und Beratungsinteresse, gleichermaßen auf Seiten der Bürgerinnen und Bürger wie auch der Unternehmen.

2.2 Videoüberwachung

2.2.1 Vollzug einer Erlaubnis für ein unbemanntes Luftfahrtsystem – „private Drohne“

Gegenstand der Betrachtung ist eine Allgemeinerlaubnis zum Aufstieg eines unbemannten Luftfahrtsystems (UAS, § 1 Abs. 2 Satz 3 LuftVG) gem. § 20 Abs. 1 Nr. 7 LuftVO.

Eine solche Erlaubnis wird von der Luftfahrtbehörde, der Fachgruppe Luftverkehr beim Landesbetrieb Mobilität, gemäß § 20 Abs. 4 S. 1 LuftVO erteilt,

wenn die beabsichtigten Nutzungen – wie z.B. das Erstellen von Luftbildaufnahmen (Foto- und Videoaufnahmen) – nicht zu einer Gefahr für die Sicherheit des Luftverkehrs oder die öffentliche Sicherheit oder Ordnung führen können, insbesondere im Fall von UAS die Vorschriften über den Datenschutz nicht verletzen.

In der Kurzinformation über die Nutzung von unbemannten Luftfahrtsystemen weist das zuständige Bundesministerium darauf hin, dass die Steuernden beim Gebrauch des Gerätes darauf achten müssen, dass datenschutzrechtliche Bestimmungen nicht verletzt werden.

Eine Erlaubnis ist mit zahlreichen Auflagen, Nebenbestimmungen und Hinweisen versehen. Beispielsweise dürfen Starts und Landungen nur mit Zustimmung der jeweiligen Grundstückseigentümerinnen und -eigentümer bzw. der Verfügungsberechtigten durchgeführt werden, und es besteht eine Anzeigepflicht für Aufstiege bei der örtlich zuständigen Ordnungsbehörde. Insbesondere datenschutzrechtlich relevant ist der in der Erlaubnis enthaltene Hinweis, dass mit Hilfe des UAS nicht in den räumlich-gegenständlichen Bereich der privaten Lebensgestaltung Dritter (z.B. Persönlichkeitsrecht, Urheberrecht) eingedrungen werden darf.

Mehrere Eingaben, mit denen Bürgerinnen und Bürger den LfDI auf den beabsichtigten Einsatz solcher Systeme aufmerksam machten, waren Anlass dafür, das Verfahren zur Erlaubniserteilung und deren Vollzug zu prüfen.

Problematisch war zunächst, dass Erlaubnisinhaberinnen und -inhaber einen Aufstiegsort im Bundesland Rheinland-Pfalz frei wählen können. Der Aufstieg eines unbemannten Luftfahrtsystems in einer Gemeinde kann einer bestimmten Erlaubnisinhaberin oder einem bestimmten Erlaubnisinhaber daher grundsätzlich nur zugeordnet werden, wenn er seiner Anzeigepflicht bei der Ordnungsbehörde nachkommt.

Aus diesem Grund ist es für die Erlaubnisbehörde mitunter schwierig, den jeweiligen Erlaubnisinhaber zu identifizieren. Im konkreten Fall war die Nachfrage bei der zuständigen Verbandsgemeindeverwaltung aber erfolgreich, zusätzlich konnte ein Hinweis auf die Veröffentlichung eines Filmes im Internet gegeben werden.

Zur Prüfung datenschutzrechtlicher Vorschriften im Antragsverfahren führte die Luftfahrtbehörde gegenüber dem LfDI weiterhin aus, dass im Rahmen der Neuerteilung einer Allgemeinerlaubnis darauf geschaut werde, ob Verstöße gegen u.a. Bestimmungen des Datenschutzes bekannt geworden seien. Eine nähere Prüfung der in der Vergangenheit von Antragstellenden erstellten Bilder oder Filme sei aber aufgrund der Vielzahl zu prüfender Anträge nicht leistbar.

Die Prüfung eines konkreten Falles hat im Hinblick auf die veröffentlichten Filme keine Verletzung der Privatsphäre oder von Vorschriften über den Datenschutz ergeben. Dritte und deren Lebensumstände waren nicht Ziel der Aufnahmen, die gerade im Falle eines Filmes über eine Pfarrkirche eher dokumentarischen Charakter aufwiesen. Deshalb wurde darauf verzichtet, zur weiteren Prüfung vom Erlaubnisinhaber das Flugbuch als Dokumentation des Flugbetriebes anzufordern.

Als Fazit kann festgehalten werden, dass die Beachtung bzw. Einhaltung von datenschutzrechtlichen Bestimmungen in diesem Zusammenhang weitgehend dem Verantwortungsbereich der Erlaubnisinhaberinnen und -inhaber überlassen bleibt. Jedenfalls fraglich ist daher, ob § 20 LuftVO als Vorschrift zum Schutz der Privatsphäre bzw. des Rechts auf informationelle Selbstbestimmung ausreicht bzw. als zweckdienlich bewertet werden kann.

2.2.2 Videoüberwachung, Wildkameras, Helmkameras

Videoüberwachung bleibt ein Schwerpunktthema des LfDI (vgl. 24. Tb., Tz. III-2.3). Insgesamt betrachtet nimmt die Zahl der Kameras im öffentlichen Raum weiter zu, gleichzeitig verbessert sich die Qualität der Aufnahmen (Auflösung/Digitalisierung der Bildverarbeitung) und der früher limitierende Faktor Speicherplatz hat durch die Verfügbarkeit günstiger Speichermöglichkeiten stark an Bedeutung verloren. Auch der Trend, ursprünglich zu anderen (privaten) Zwecken angefertigte Aufzeichnungen im Internet auf eigens dafür bereitstehenden Portalen zu veröffentlichen, setzt sich weiter fort.

Fotografieren, Filmen und „Hochladen“ sind mittlerweile ein und dasselbe (vgl. ausführlich hierzu 24. Tb., Tz. III-2.3.1).

Die Zunahme der Videoüberwachung spiegelt sich auch im weiteren Anstieg der Nachfragen und Beschwerden zu diesem Thema beim LfDI wider, nach wie vor betrifft etwa ein Drittel der mehr als 2.500 jährlichen Eingaben im privaten Bereich an den LfDI den Bereich Videoüberwachung.

Im öffentlichen Raum betrifft sie auch öffentliche Verkehrsmittel. Beim Neuerwerb von Beförderungsmitteln wird von Herstellern oft bereits eine komplette Überwachungstechnik im Paket angeboten. Verantwortlich für die Zulässigkeit der Videoüberwachung sind aber die Betreiber der Verkehrsmittel. Diese setzen darauf, dass Videoüberwachung das Sicherheitsempfinden von Fahrgästen und auch von Fahrerinnen und Fahrern erhöht, Vandalismusschäden vorbeugt und die strafrechtliche und zivilrechtliche Verfolgbarkeit solcher Schäden erleichtert. Dabei wird aber oft vergessen, dass durch eine solche dauerhafte Beobachtung erheblich in das Persönlichkeitsrecht der Betroffenen eingegriffen wird. Ein solcher Eingriff kann nur gerechtfertigt werden, wenn die berechtigten Interessen der Verkehrsunternehmen die der Betroffenen deutlich überwiegen.

Um Verkehrsunternehmen eine solche Interessenabwägung zu erleichtern, haben die Datenschutzaufsichtsbehörden Anforderungen an eine Videoüberwachung speziell in öffentlichen Verkehrsmitteln in einer Orientierungshilfe zusammengefasst. Dort wird dargestellt, unter welchen Voraussetzungen Videoüberwachung zum Einsatz kommen darf, welche begleitenden Maßnahmen zu treffen sind und wie mit den Aufzeichnungen verfahren werden muss. Ein besonderes Augenmerk wurde dabei auf die Beachtung der schutzwürdigen Interessen der Fahrgäste und auch der Beschäftigten gelegt.

Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ (http://www.datenschutz.rlp.de/downloads/oh/oh-vue-oepnv.pdf)

Solche Handreichungen der Datenschutzaufsichtsbehörden für den korrekten Umgang mit Videoüberwachungsanlagen gehören mittlerweile zum standardmäßigen Beratungsangebot des LfDI. Noch wichtiger bleibt es aber auch weiterhin, dass die Bürgerinnen und Bürger mit offenen Augen durch ihren Alltag gehen und nicht klaglos akzeptieren, wenn in ihrer Eisdiele, im Schwimmbad, in Toilettenbereichen oder im Zug nach Hause Videokameras installiert werden.

Bereits im Oktober 2013 hat der LfDI auf das Thema der Wildkameras aufmerksam gemacht, das vor Ort die Gemüter erhitzt und nach wie vor ein großes Medienecho findet (vgl. hierzu ausführlich 24. Tb., Tz. III-2.3.3). Als besonders hilfreich hat sich erwiesen, dass das Umweltministerium mittlerweile dazu übergegangen ist, bei der Verpachtung von staatlichen Jagdrevieren ein Verbot des Einsatzes von Wildkameras in die Pachtverträge aufzunehmen. Da hiervon etwa die Hälfte aller Jagdreviere betroffen ist, kann auf diese Weise ein wichtiger Beitrag zur Reduzierung der Kamerabestände geleistet werden.

Dennoch habe eine Vielzahl von Beschwerden über illegale Wildkameras den LfDI in den vergangenen zwei Jahren erreicht. Beim Vollzug des Wildkameraverbots hat sich allerdings als problematisch erwiesen, dass die Angaben über den Standort der Kamera nicht immer genau genug waren, um die Verantwortlichen ermitteln zu können. In einigen Fällen haben sich Jägerinnen und Jäger auch darauf berufen, dass die Kameras zwar in ihrem Revier hingen, aber nicht von ihnen, sondern von unbekannten Dritten angebracht worden seien. Ob in diesen Fällen die Kameras von rechtswidrig gefilmten Waldbesucherinnen und -besuchern abgehängt und in Gewahrsam genommen werden dürfen, ist gerichtlich bislang nicht geklärt. Eine gerichtliche Klärung im Streit um Wildkameras steht noch aus.

Helmkameras werden mittlerweile von vielen Freizeitsportlerinnen und -sportlern genutzt. Damit dokumentieren Skifahrerinnen und -fahrer, Surferinnen und Surfer oder Mountainbikerinnen und -biker ihre sportlichen Erlebnisse. Deshalb boomt die Branche dieser hippen Kameras, die wie ein zweites Paar Augen Extremsituationen aufzeichnen können – und damit zur Weiterverbreitung im Netz geradezu auffordern.

Der LfDI rät hier zu Vorsicht und Rücksichtnahme. Solange diese Aufzeichnungen im Kreise der Familie und Freunde bleiben, sind aus datenschutzrechtlicher Sicht keine durchgreifenden Bedenken zu erheben. Problematisch wird die Verwendung der Kameras aber dann, wenn Dritte, die von der Kameraaufzeichnung erfasst werden, ungewollt mit aufgenommen werden. Diese Betroffenen könnten sich dadurch in ihren Persönlichkeitsrechten beeinträchtigt sehen.

Werden die Aufnahmen noch dazu im Internet und damit weltweit abrufbar veröffentlicht, können Sportlerinnen und Sportler auch noch mit Vorschriften des Datenschutzrechts oder des Kunsturhebergesetzes in Konflikt kommen. Fotografieren oder filmen sie aus „touristischen Zwecken“, ist das in aller Regel nicht zu beanstanden. Kommen dabei aber andere Personen in den Fokus und wird die Helmkamera gezielt auf diese gerichtet, dann brauchen sie deren ausdrückliche Einwilligung, wenn sie die Aufnahmen veröffentlichen wollen. Besonders kritisch wird es dann, wenn die Sportlerinnen und Sportler die Videos auf YouTube, Blogs oder Facebook hochladen ohne die Einwilligung der auf den Videos abgebildeten Personen einzuholen.

Einerseits kann der LfDI dann Sanktionen – etwa ein Bußgeld – verhängen, wenn eine Beschwerde eingeht. Andererseits kann die Aufzeichnung für die Sportlerinnen und Sportler auch Nachteile bringen. Regelmäßig beschlagnahmen Ermittlungsbehörden die Kameras samt Videoaufzeichnungen, um Unfälle, Straftaten etc. aufzuklären – wie etwa im Falle des beim Skifahren fernab der Piste verunglückten Michael Schumacher. Das kann für die Ermittlungsbehörden sehr hilfreich sein – aber nicht immer im Interesse der Sportlerinnen und Sportler liegen. Die haben dann für ihre Regelverstöße oder gar Ordnungswidrigkeiten das Beweismaterial an die Polizei gleich mitgeliefert.

2.2.3 Nachbar überwacht Nachbar

Die Anzahl der Beratungsanfragen aus der Bevölkerung rund um das Thema Videoüberwachung steigt kontinuierlich. Weiterhin erreichen den LfDI vermehrt Beschwerden über Videoüberwachungsanlagen in der jeweiligen Nachbarschaft.

So gilt weiterhin das bereits im letzten Datenschutzbericht Gesagte (vgl. 24. Tb., Tz. II-2.3.2):

> Entweder zeigt die beanstandete Kamera z.B. auf den Garten der bzw. des Anderen oder aber auf den öffentlichen Verkehrsraum. Die Nachbarinnen und Nachbarn scheinen ihre Nachbarschaft zu überwachen – sehr zum Missfallen der Betroffenen. Dabei handelt es sich zwar nicht um eine „Wirtschaftsthematik“, wegen ihrer praktischen Bedeutung für die Arbeit des LfDI soll die „nachbarschaftliche Überwachung“ jedoch an dieser Stelle näher erörtert werden.
> Ob die von der Nachbarin oder dem Nachbarn betriebene Videoüberwachung zulässig ist, hängt zunächst von der Anwendbarkeit des Bundesdatenschutzgesetzes (§ 6b BDSG) ab. Das Bundesdatenschutzgesetz greift nur ein, wenn öffentlich zugängliche Räume beobachtet werden und es sich um eine Videoüberwachung zu gewerblichen Zwecken handelt. Liegen diese Voraussetzungen nicht vor, dann ist der LfDI nicht zuständig und kann dem Nachbarn leider nicht weiterhelfen. Das bedeutet allerdings nicht, dass damit die Überwachung auch zulässig wäre. Dann müssen vielmehr an Stelle des LfDI die Zivilgerichte über die Rechtmäßigkeit der Videoüberwachung entscheiden.

Eine von der deutschen Rechtslage abweichende Auffassung vertritt dagegen der Europäische Gerichtshof in seiner Rechtsprechung zur EU-Datenschutz-Richtlinie von 1995, in deren Umsetzung das Bundesdatenschutzgesetz erlassen wurde. Der Europäische Gerichtshof hat im Dezember 2014 ein Urteil (Rs. C-212/13) zur Videoüberwachung durch Privatpersonen erlassen und angenommen, dass eine Videoüberwachung dann nicht mehr zu persönlichen oder familiären Zwecken erfolgt, sobald (neben dem eigenen Grundstücksbereich) auch öffentlicher Verkehrsraum überwacht wird.

Diese Rechtsauffassung des Europäischen Gerichtshofs weicht von der gesetzlichen Regelung des Bundesdatenschutzgesetzes ab. Die tatsächliche Umsetzung dieses Urteils durch die Datenschutzaufsichtsbehörden in Deutschland kann allerdings erst dann erfolgen, wenn das Bundesdatenschutzgesetz durch den Gesetzgeber entsprechend angepasst worden ist. Bis dahin begrenzt der derzeitige Wortlaut der Ermächtigungsgrundlage Bundesdatenschutzgesetz das Tätigwerden der Aufsichtsbehörden. Auch Prüf- und Vollzugsmöglichkeiten ste-

hen den Datenschutzbeauftragten nicht zu, wenn Private zu persönlichen Zwecken Videoüberwachung betreiben. Es existieren keine Kontroll- und Betretungsrechte gegenüber den Betreiberinnen und Betreibern; so darf der LfDI etwa nicht die Videokamera, ihre Funktionsweise und Ausrichtung auf dem Grundstück der Privaten in Augenschein nehmen. Auch hat er keine Möglichkeit zu prüfen, ob es sich bei der Kamera um eine Attrappe handelt oder nicht. Auch diese Vollzugsfragen wird der Bundesgesetzgeber regeln müssen, bevor der LfDI selbst einschreiten kann.

Soweit der Einsatz von Videoüberwachung durch Private nur das allgemeine Persönlichkeitsrecht Betroffener beeinträchtigt, ist insoweit also ausschließlich der Zivilrechtsweg eröffnet. Werden von einer Videoüberwachung zu persönlichen oder familiären Zwecken auch Nachbarn oder Passanten erfasst, können diese als Betroffene ggf. Unterlassungs- und Beseitigungsansprüche gemäß §§ 823, 1004 BGB geltend machen und vor den Zivilrechtgerichten durchsetzen.

Ist demgegenüber das Bundesdatenschutzgesetz anwendbar und damit der LfDI für die Überprüfung der Videoanlage zuständig, so ist zu klären, ob die Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und ob Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Nachbarn überwiegen. Dies wird von manchen Betreiberinnen und Betreibern einer Videoüberwachungsanlage übersehen, da sie annehmen, dass allein ihr Hausrecht die Maßnahme rechtfertige.

Die Zulässigkeit der Videoüberwachung hängt dann unter Umständen auch von der Kameraeinstellung ab. Ist der öffentliche Verkehrsraum erfasst, ist die Videoüberwachung regelmäßig unzulässig. Die Aufgabe der Verkehrsüberwachung obliegt der Polizei, nicht einzelnen Bürgerinnen und Bürgern.

Ebenso muss die Erforderlichkeit einer Videoaufzeichnung gesondert geprüft werden. Zentral ist dabei die Frage, ob eine grundsätzlich zulässige Videoüberwachung (und -aufzeichnung) an allen Tagen rund um die Uhr erfolgen muss oder ob angesichts der Erkenntnislage – z.B. wenn eine Gefahr nur in den Abend- oder Nachtstunden bzw. am Wochenende droht – eine zeitlich eingeschränkte Beobachtung und Aufzeichnung genügt.

Bei Videoaufzeichnungen muss sich auch die Speicherdauer strikt am Erforderlichkeitsgrundsatz orientieren. Sofern es sich um eine datenschutzrechtlich zulässige Videoüberwachung handelt, wird eine Speicherdauer von bis zu 48 Stunden für zulässig, aber auch ausreichend angesehen. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Überwachungszwecks nicht mehr erforderlich sind. Eine über 48 Stunden hinausgehende Speicherung der Videoaufzeichnung verstößt grundsätzlich gegen § 6b Abs. 5 BDSG und muss unterbleiben. Verstöße können mit einem Bußgeld geahndet werden.

Als Faustregel gilt weiterhin: Wer fremde Grundstücke oder öffentlichen Verkehrsraum videoüberwacht, verstößt gegen geltendes Recht und kann vom LfDI oder von den Zivilgerichten zum Abbau der Überwachungsanlage verpflichtet werden.

Gesamtbewertung des LfDI

Insgesamt lässt sich die Videoüberwachung im öffentlichen Raum daher datenschutzrechtlich wie folgt bewerten:

- Jede Videoüberwachung ist ein Eingriff in das Persönlichkeitsrecht, denn alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.
- Die Videoüberwachung erfasst unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen.
- Daher ist Videoüberwachung immer begründungsbedürftig und darf immer nur offen erfolgen, sie ist stets auf das notwendige Maß zu beschränken und bedarf in zeitlicher Hinsicht der regelmäßigen Überprüfung (jährliche Evaluationspflichten).
- Vor der Einrichtung einer Videoüberwachung müssen alle Alternativen hierzu geprüft und bewertet werden. Videoüberwachung kann nur die ultima ratio sein.
- Jede Einrichtung einer Videoüberwachung muss der datenschutzrechtlichen Vorabkontrolle unterzogen werden (§ 4d Abs. 5 BDSG), gleichzeitig ist die Berufung eines betrieblichen Datenschutzbeauftragten vor Installation der Videoüberwachung verpflichtend.

- Der Zweck der Videoüberwachung muss konkret vor Beginn der Überwachung schriftlich festgelegt werden.
- Während der Videoüberwachung müssen die Zweckbindung, die differenzierte Abstufung zwischen Aufnahmearten, die deutliche Erkennbarkeit der Videoüberwachung sowie die Löschung der Daten binnen kurzer Fristen (48 Stunden) strikt und dauerhaft sichergestellt werden.
- Rechtskonforme Videoüberwachung ist planungsintensiv, kostspielig, aufwändig und nur begrenzt effektiv. Videoüberwachung ist nur bei optimaler technischer und personeller Ausführung erfolgversprechend und nur dann verhältnismäßig.
- Die Beweislast für die Zulässigkeit der Videoüberwachung liegt bei den Betreiberinnen und Betreibern.
- Die flächendeckende Videoüberwachung muss verhindert werden, da die Gefahr besteht, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.
- Rechtsverletzungen werden als Ordnungswidrigkeit mit hohen Bußgeldern verfolgt.

2.3 Landesdatenschutzkonferenz Rheinland-Pfalz

Die im ständigen Wandel begriffene digitale Welt bietet Unternehmen viele Chancen. Wirtschaftlicher Erfolg hängt jedoch zunehmend von einer professionellen Nutzung der Informationstechnologien ab. Zugleich stärkt ein kompetenter Umgang mit den Anforderungen des Datenschutzes das Vertrauen, das Kundinnen und Kunden den Unternehmen entgegenbringen. Ebenso wächst die Bedeutung der Datensicherheit – gerade für kleine und mittelständische Unternehmen (vgl. Tz. III-2.4). Weitreichende Auswirkungen auf die Wirtschaft insgesamt wird in diesem Zusammenhang die 2016 erwartete europäische Datenschutz-Grundverordnung haben.

Gemeinsam mit der Landesregierung hat der LfDI am 15. Oktober 2015 daher die erste Landesdatenschutzkonferenz Rheinland-Pfalz ausgerichtet. Auf dieser diskutierten Vertreterinnen und Vertreter aus Politik, Wirtschaft und Verbänden zusammen mit Datenschutzbeauftragten die Herausforderungen der Digitalisierung und die Auswirkungen der kommenden europäischen Datenschutz-Grundverordnung.

Dabei bestand Einigkeit darüber, dass Datenschutz und IT-Sicherheit angesichts einer Situation, in der Daten zum Produktionsfaktor geworden sind und persönliche und sachliche Informationen wirtschaftliche Potenziale erschließen, wichtige Voraussetzungen sind, um Vertrauen und Verlässlichkeit in einer digitalisierten Welt zu gewährleisten. Der wirtschaftliche Erfolg eines Unternehmens hängt heute und künftig noch stärker auch davon ab, wie gut es gelingt, sensible Datenbestände und die elektronische Kommunikation vor Datenverlust und Missbrauch zu schützen. Wichtige Bausteine sind aus Sicht des LfDI hierbei Auditierung und Zertifizierung. Sie schaffen Transparenz, Vertrauen und Sicherheit innerhalb des Unternehmens und gegenüber Kundinnen und Kunden sowie Geschäftspartnerinnen und –partnern (vgl. Tz. III-14.7).

Wie sehr Europa den Datenschutz beeinflusst bzw. wie eng Datenschutzfragen mit wirtschaftlichen Fragen verknüpft sind, zeigt sich einmal mehr am Urteil des Europäischen Gerichtshofs zur Frage der Datenübermittlung in die USA (vgl. Tz. I-1.4, I-1.5). Die Konferenz war sich einig, dass die Reform des Datenschutzes auf europäischer Ebene weitreichende Änderungen mit sich bringen wird. Ziel der Konferenz war es, die rheinland-pfälzische Wirtschaft verlässlich und innovativ auf die aktuellen Entwicklungen vorzubereiten. Mindestanforderungen des Datenschutzes in Europa können aus Sicht des LfDI einen fairen Wettbewerb unterstützen.

2.4 IT-Sicherheit und Datenschutz im Unternehmen

Die Spionage im Bereich der Wirtschaft gehört zu den klassischen Aufklärungszielen der Nachrichtendienste. Vor dem Hintergrund globalisierter Märkte und sich verändernder weltpolitischer Konstellationen hat die Bedeutung der Wirtschaftsspionage jedoch stetig zugenommen. Mit der fortschreitenden Digitalisierung der Wirtschaft rücken dabei zunehmend Angriffe auf IT-Strukturen durch staatliche Stellen, Wettbewerber oder Kriminelle in den Fokus. Informationen über Wettbewerber und Märkte, Technologien, Kundinnen und Kunden und aktuelles Know-how zur Produktentwicklung und Produktionstechnik wecken vielfältige Begehrlichkeiten.

Dies gilt auch für Rheinland-Pfalz. Die rheinland-pfälzische Wirtschaft weist eine ähnliche Struktur wie die Wirtschaft in Deutschland insgesamt auf: Der Anteil des produzierenden Gewerbes an der Bruttowertschöpfung beträgt rund 31 Prozent, der des Dienstleistungsbereichs ca. 68 Prozent. Chemie, Fahrzeugbau und Maschinenbau – Felder, in denen technologische Kompetenz und Know-how von essentieller Bedeutung sind – sind dabei die wichtigsten Industriebereiche. Hier gilt es, die digitalen Assets der Unternehmen – Konstruktions- und Produktionsdaten, Kundendaten, Technologien etc. – zu sichern und zu schützen. Gerade Innovationen, Ergebnisse aus Forschung und Entwicklung, Prozessabläufe und dergleichen sind begehrte Ziele. Mit einer Exportquote von über 50 Prozent im verarbeitenden Gewerbe weckt gerade Rheinland-Pfalz hier Begehrlichkeiten.

Die Digitalisierung des Geschäftsalltags nimmt stetig zu. So werden Geschäftsprozesse zunehmend ins Internet verlagert und IT-Strukturen durch den Einsatz mobiler Geräte und die Nutzung von Cloud-Lösungen auf Bereiche außerhalb des Unternehmens ausgedehnt. Die Einbindung von Geschäftspartnern, Dienstleistern und Lieferanten in Wertschöpfungsketten, E-Commerce-Lösungen und die elektronische Anbindung von Kundinnen und Kunden eröffnen zunehmend Zugriffsmöglichkeiten auf Unternehmensdaten durch externe Stellen.

Es dürfte heute wohl kein Unternehmen mehr geben, das nicht an das Internet angebunden und davon in mehr oder weniger großem Maße abhängig ist. Der wirtschaftliche Erfolg eines Unternehmens hängt daher auch davon ab, wie gut es gelingt, sensible Datenbestände und die elektronische Kommunikation vor Datenverlust und Datenmissbrauch zu schützen. Die stattfindende Transformation der Wirtschaft in die digitale Welt führt zu für die Unternehmen neuen Anforderungen an IT-Sicherheit und Datenschutz. Cyberattacken können zum Verlust von Geschäftsgeheimnissen führen und die Arbeitsfähigkeit eines Unternehmens bis hin zu dessen Bestand gefährden.

Aus Angst vor Reputationsverlust wagt kaum ein Unternehmen öffentlich über Sicherheitsprobleme zu sprechen. Nach einer Untersuchung des Branchenverbandes BITKOM hat jedoch nahezu jedes dritte Unternehmen in Deutschland in den vergangenen zwei Jahren Angriffe auf seine IT-Systeme verzeichnet.

Die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft spricht allein in Deutschland von jährlich 50 Milliarden Euro Schaden durch solche Wirtschaftsspionage. Andere Schätzungen gehen von bis zu 100 Milliarden Euro aus. Dies sind fast zwei bzw. vier Prozent des Bruttoinlandsprodukts Deutschlands. Bei einem rheinland-pfälzischen BIP-Anteil von ca. vier Prozent wäre dies zwischen zwei und vier Milliarden allein in Rheinland-Pfalz.

Die Datensicherheit liegt insbesondere in vielen mittelständischen Unternehmen im Argen. Nach einer Untersuchung des Branchenverbandes BITKOM sehen 57 Prozent der Unternehmen Angriffe auf IT-Systeme, etwa von Hackern, Kriminellen oder ausländischen Geheimdiensten als reale Gefahr an, weniger als die Hälfte hat jedoch einen Notfallplan für IT-Sicherheitsvorfälle. Lediglich 24 Prozent der mittelständischen Unternehmen verfügen über eine Sicherheitsstrategie, um sich gegen Angriffe zu schützen. Eine mögliche Erklärung könnte darin liegen, dass kleinere Unternehmen nicht über das nötige Problembewusstsein verfügen, aber auch, dass sie mit der Technik überfordert sind und Risiken verdrängen. Die Ergebnisse der Studie „IT-Sicherheitslage im Mittelstand“ legen nahe, dass es insbesondere auf drei Gebieten aktuellen Handlungsbedarf gibt: bei der E-Mail-Sicherheit, beim Einsatz mobiler Endgeräte und beim Cloud-Computing.

Studie „IT-Sicherheitslage im Mittelstand“
https://www.dsin-blog.de/sites/default/files/studie-mittelstand_2013_web.pdf

Sicherheitsmonitor der Initiative „Deutschland sicher im Netz“
https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsmonitor_2015_web.pdf

Die Einbindung von Produzenten, Lieferanten, Geschäftspartnern, Dienstleistern, Konzernunternehmen oder Kundinnen und Kunden in betriebswirtschaftliche, Konstruktions- oder Produktionssysteme muss daher mit Sicherheits- und Datenschutzkonzepten verbunden werden, um Risiken angemessen

begegnen zu können und Datenabflüsse zu vermeiden. Der Schutz der IT-Infrastruktur und der Kommunikation müssen als unternehmenskritische Faktoren gesehen werden, deren mangelnde Berücksichtigung Risiken für den Bestand eines Unternehmens oder seine Position im Markt bergen. Neben einer entsprechenden Sensibilisierung und Aufklärung der Unternehmensleitungen und Beschäftigten braucht es allerdings auch Sicherheits- und Datenschutzkonzepte, die Schutzmaßnahmen wie Zugriffsregelungen, Verschlüsselungslösungen oder den Schutz vor Schadsoftware gewährleisten.

Alle Informationen in einem Unternehmen absolut zu schützen ist dabei weder möglich noch sinnvoll. Primär sollten daher die Daten besonders geschützt werden, deren Verlust Geschäftsmodelle, den Bestand des Unternehmens, seine Marktstellung oder Reputation gefährdet oder Rechtspflichten verletzt. Daher gilt es, im Rahmen einer Schutzbedarfsanalyse zunächst diese unternehmenskritischen Daten zu identifizieren. Hierzu zählen nicht nur das unternehmerische, technologische Know-how, sondern, im Rahmen der Digitalisierung von Geschäftsprozessen und –modellen regelmäßig auch Kundendaten.

Neben Maßnahmen zum Schutz der IT-Infrastruktur sollte ein Ansatz verfolgt werden, der eine informationsbezogene Sicherheit in den Blick nimmt. Eine Strategie zum Schutz von Know-how sollte sich jedoch nicht nur auf IT-Systeme beziehen. Die Einbindung der beschäftigten und organisatorische Regelungen für den Umgang mit Unternehmensdaten müssen mindestens gleichberechtigt berücksichtigt werden.

Online-Check der Initiative „DSiN – Deutschland sicher im Netz“
https://www.sicher-im-netz.de/unternehmen

2.5 Vereinswesen

2.5.1 Videoaufzeichnungen von Fußballspielen niederer Spielklassen

Veranlasst durch eine Eingabe beschäftigte sich der LfDI im Berichtzeitraum mit der datenschutzrechtlichen Zulässigkeit der Aufzeichnung und Übertragung von Fußballspielen niederer Spielklassen. Konkret hatte er zu beurteilen, ob ein Fußballverein die Heimspiele seiner Mannschaft aufzeichnen darf, um diese als (Live-)Videostream auf der eigenen Homepage zu veröffentlichen bzw. auf einer Videoplattform wie z.B. Youtube zugänglich zu machen.

Datenschutzrechtlich ist insoweit zwischen der Spielaufzeichnung (Erhebung und Speicherung) sowie der anschließenden Veröffentlichung (Übermittlung) zu unterscheiden. Die Spielaufzeichnung ist an den Bestimmungen des Bundesdatenschutzgesetzes, die Veröffentlichung in erster Linie an dem vorrangig zu prüfenden Kunsturhebergesetz zu messen. Da die Veröffentlichung aber im Verhältnis zur Aufzeichnung als schwerwiegenderer Eingriff in das informationelle Selbstbestimmung der Betroffenen zu werten ist, sprechen aus Sicht des LfDI gute Gründe dafür, die Wertungen des Kunsturhebergesetzes bereits bei der Datenerhebung und –speicherung zu berücksichtigen.

Auf dieser Grundlage hat der LfDI unter Hinweis auf die sog. „Eisprinzessin-Alexandra-Entscheidung“ des Bundesgerichtshofs (Urteil vom 28. Mai 2013, Az. VI ZR 125/12) festgehalten, dass das Kunsturhebergesetz mit § 23 Abs. 1 Nr. 1 (Bildnisse der Zeitgeschichte) und Nr. 3 (Bildnisse von Versammlungen, Aufzügen und ähnlichen Vorgängen) zwei Tatbestände aufweist, die eine Veröffentlichung von Videoaufzeichnungen einer Sportveranstaltung – wenn auch nur mit lokaler Bedeutung – dem Grunde nach zulassen.

Es bedarf dabei aber stets einer Abwägung im Einzelfall, bei der das informationelle Selbstbestimmungsrecht und die Persönlichkeitsrechte (Recht am eigenen Bild, ggf. Recht am gesprochenen Wort) der Betroffenen einerseits mit dem Dokumentations- und Veröffentlichungsinteresse des Vereins sowie dem Informationsinteresse der Öffentlichkeit andererseits abzuwägen sind. Folgende Abwägungsfaktoren sind dabei aus Sicht des LfDI besonders zu berücksichtigen:

- Die Videoaufzeichnungen betreffen die Freizeitausübung von Spielerinnen und Spielern, Zuschauerinnen und Zuschauern sowie Schiedsrichterinnen und Schiedsrichtern. Sie genießen

daher einen höheren Schutz als Profisportlerinnen und Profisportler.
- Es ist demgegenüber zu berücksichtigen, dass die Spiele – anders als der „Freizeitkick“ mit Freunden – in eine Ligastruktur eingebunden sind. Anerkanntes Ziel ist insoweit, eine möglichst breite Öffentlichkeit für eine Sportart bzw. eine Sportveranstaltung zu erreichen.
- Der Grad der Betroffenheit der Einzelnen richtet sich dabei auch nach Art und Dauer der Aufzeichnung. Die Darstellung eines Spiels in voller Länge begründet einen stärkeren Eingriff als eine zeitlich begrenzte Aufnahme. Der Umstand, dass eine Aufnahme – z.B. bei Youtube – zeitlich unbegrenzt vorgehalten werden soll, erhöht die Eingriffsqualität. Eine Aufnahme, die ausschließlich die Totale eines Spieles zeigt, ist weniger einschneidend als Nahaufnahmen einzelner Spielerinnen oder Spieler.

Im konkreten Fall hat der LfDI folgende Modalitäten vorgeschlagen, die seitens des Vereins gerne aufgegriffen wurden:

- Die Aufzeichnungen werden auf die Totale beschränkt und zunächst nur auf der Homepage des Vereins als Livestream zugänglich gemacht.
- Der Umstand, dass Videoaufzeichnungen von einem Spiel gefertigt werden, ist unter Hinweis auf die verantwortliche Stelle an der Spielstätte gut sichtbar deutlich zu machen.
- Zuschauerinnen und Zuschauern wird die Möglichkeit eröffnet, sich außerhalb des Bildbereichs der Kamera aufhalten zu können. Einem Widerspruch durch die Gastmannschaft gegen die Videoaufzeichnung ist in geeigneter Form Rechnung zu tragen.
- Auf eine Veröffentlichung des Spiels in voller Länge auf Youtube sollte verzichtet werden. Wenn Videoaufzeichnungen längerfristig zugänglich gemacht werden sollen, sollten sich diese nur auf einzelne Spielszenen beziehen, die zuvor von der verantwortlichen Stelle unter Berücksichtigung der berechtigen Interessen der Betroffenen ausgewählt wurden.
- Nach spätestens drei Monaten – mit dem Verblassen des Informationsinteresses der Öffentlichkeit – sollten die Aufnahmen wieder gelöscht werden.

2.5.2 Austausch von Informationen aus einem erweiterten Führungszeugnis (§ 30a BZRG) zwischen einem Sportverband und seinen Mitgliedsvereinen

Ob und in welchem Umfang Informationen aus einem erweiterten Führungszeugnis zwischen einem Sportverband und einzelnen seiner Mitgliedsvereinen ausgetauscht werden dürfen, war Gegenstand einer Stellungnahme, die der LfDI gegenüber einem Sportverband abgegeben hat.

Der LfDI hat festgehalten, dass ein wirksamer Datenschutz bereits bei der Erhebung und Speicherung personenbezogener Daten ansetzt. Aus diesem Grund plädiert er dafür, die Wertungen des § 72a SGB VIII, der den Umgang mit erweiterten Führungszeugnissen im Bereich der Kinder- und Jugendhilfe restriktiv regelt – auch außerhalb des Sozialgesetzbuches VIII zu berücksichtigen. Die Datenerhebung und -speicherung bei Beschäftigten (§ 3 Abs. 11 BDSG) eines Vereins richtet sich zwar nach § 32 BDSG und bei Ehrenamtlichen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG jeweils i.V.m. § 30a BZRG. Bei deren Auslegung können aber die Wertentscheidungen des § 72a SGB VIII berücksichtigt werden, die die besondere Sensibilität der sich aus einem Führungszeugnis ergebenden Daten reflektieren.

Daraus folgt, dass nur der Umstand, dass Einsicht in ein Führungszeugnis genommen wurde, das Datum des Führungszeugnisses und die Information gespeichert werden darf, ob eine Person wegen einer einschlägigen Straftat rechtskräftig verurteilt worden ist. Verfahrenstechnisch ist sicherzustellen, dass nur einer zuvor speziell hierfür bestimmten Person die Einsichtnahme in die Führungszeugnisse gestattet ist (z.B. Kinder- und Jugendschutzbeauftragten). Darüber hinaus ist auf ein effektives Löschungsmanagement zu achten.

Was den Informationsaustausch zwischen Sportverband und den Mitgliedsvereinen anbelangt, ist zunächst festzuhalten, dass es sich jeweils um eigenständige verantwortliche Stellen im Sinne von § 3 Abs. 7 BDSG handelt. Der Austausch personenbezogener Daten zwischen ihnen ist daher als Datenübermittlung zu bewerten. Diese kann nach Auffassung des LfDI nur in Ausnahmefällen auf der

Grundlage von § 28 Abs. 2 Nr. 2a BDSG, d.h. zur Wahrung berechtigter Interessen eines Dritten, gerechtfertigt sein.

Ein regelmäßiger Austausch der Informationen, die sich aus dem Führungszeugnis ergeben, scheitert bereits daran, dass sowohl die Vereine als auch der Verband selbst die Möglichkeit haben, in den Grenzen der genannten Erhebungsvorschriften die für einen effektiven Kinder- und Jugendschutz relevanten Daten zu erheben. Der Datenaustausch ist in diesem Sinne nicht erforderlich und widerspräche dem Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG). Dieser gewährleistet, dass Daten grundsätzlich bei den Betroffenen zu erheben sind und sichert so, dass sich die Betroffenen auch gegen die Vorlage eines Führungszeugnisses entscheiden können.

In Anlehnung an die Stellungnahme der Bremischen Beauftragten für den Datenschutz und die Informationsfreiheit (vgl. hierzu deren 37. Tb., Tz. 5.8) hat der LfDI aber ausgeführt, dass er es nicht beanstanden würde, wenn im Einzelfall auf eine konkrete Anfrage hin eine Datenübermittlung erfolgt, die sich auf die Information beschränkt, dass keine Bedenken gegen eine Beschäftigung bestehen. In Fällen, in denen keine Informationen vorliegen oder Bedenken gegen eine Beschäftigung der Betroffenen bestehen, darf hingegen keine Auskunft erteilt werden. Der Anfragende ist dazu aufzufordern, sich selbst ein Führungszeugnis vorlegen zu lassen.

Für den LfDI sind weitere Konstellationen darstellbar, in denen eine Datenübermittlung ausnahmsweise gerechtfertigt sein kann. Denkbar ist z.B., dass der Verband oder ein Verein über Kenntnisse aus einem erweiterten Führungszeugnis verfügt, die für die jeweils andere Seite unter dem Gesichtspunkt des Kinder- und Jugendschutzes relevant sind, ohne dass für diese ein konkreter Anlass zur Anforderung des erweiterten Führungszeugnisses gegeben ist. Zu denken ist z.B. an Fälle, in denen sich der Verband berechtigt ein Führungszeugnis vorlegen lässt, das relevante Eintragungen enthält, der Betroffenen aber schon seit Längerem bei einem Mitgliedsverein tätig ist.

In einer solchen oder einer ähnlichen Situation kann im Einzelfall eine Abwägung ergeben, dass eine Datenübermittlung unter Berücksichtigung des besonderen Schutzbedürfnisses von Kindern und Jugendlichen gerechtfertigt ist. Maßgeblich sind dann die Umstände des Einzelfalls, wobei aber stets zu fordern ist, dass die Stelle, der die Daten übermittelt werden, selbst berechtigt wäre, sich ein erweitertes Führungszeugnis nach § 30a BZRG vorlegen zu lassen.

3. Beschäftigtendatenschutz

3.1 Datenschutz im öffentlichen Bereich

3.1.1 Personaldatenschutz und Informationsfreiheit

Der LfDI vertritt seit Jahrzehnten die sog. Amtsträgertheorie, wonach sich öffentlich Bedienstete im Rahmen ihrer nach außen gerichteten Tätigkeit grundsätzlich nicht auf ihr informationelles Selbstbestimmungsrecht berufen können (vgl. 6. Tb., Tz. 6; grundlegend: 13. Tb., Tz. 17.3). Im Rahmen seiner Organisationshoheit steht es dem Dienstherrn daher weitestgehend frei, darüber zu entscheiden, wie seine Bediensteten den Bürgerinnen und Bürgern gegenübertreten. Dies betrifft z.B. die Frage, ob Namensschilder getragen werden müssen, ob bei der Korrespondenz Vorname und Nachname anzugeben ist, ob an der Bürotür Namensschilder angebracht werden und ob Ansprechpartner mit ihren Zuständigkeiten und dienstlichen Erreichbarkeitsangaben im Internetangebot der Behörde veröffentlicht werden. Diese Organisationshoheit wird allerdings durch Fürsorgegesichtspunkte und gesetzliche Vorgaben beschränkt. Fürsorgegründe können insbesondere bei einer Gefährdungssituation für Bedienstete zum Tragen kommen. Gesetzliche Schranken finden sich z.B. im Kunsturhebergesetz, wenn es um die Veröffentlichung von Fotos im Internet geht (vgl. Tz. III-7.1.1).

Das Bundesverwaltungsgericht hatte diese Rechtsauffassung in seinem Beschluss vom 12. März 2008 (Az. 2 B 131/07) bestätigt und herausgestellt, dass die Form der Öffentlichkeitsarbeit im organisatorischen Ermessen der Behörde liege und kein Bediensteter einer Behörde einen Anspruch darauf habe, von Publikumsverkehr und von der Möglichkeit, postalisch oder elektronisch von außen mit ihm Kontakt aufzunehmen, abgeschirmt zu werden, es sei denn, legitime Interessen z.B. der Sicherheit gebieten dies.

Aus der Amtsträgertheorie ergibt sich indes kein Anspruch für Bürgerinnen und Bürger, bestimmte Beschäftigtendaten übermittelt zu bekommen. Dies hat das Verwaltungsgericht Neustadt in seinem Urteil vom 4. September 2014 (Az. 4 K 466/14.NW) deutlich gemacht: Im konkreten Fall ging es um die Herausgabe der Durchwahlnummern der Beschäftigten eines Jobcenters. Das Verwaltungsgericht prüfte den Herausgabeanspruch nach dem Informationsfreiheitsgesetz und vertrat die Auffassung, dass vorliegend ein Ausschlussgrund nach § 5 Abs. 1 IFG vorliege. Hiernach besteht ein Zugang zu personenbezogenen Daten nur, wenn das Informationsinteresse das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Nach Auffassung des Gerichts muss es sich hierbei um einen konkreten Vorgang handeln; die Befriedigung eines privaten Informationsinteresses reiche nicht aus. Im vorliegenden Fall wohnte der Kläger in Braunschweig und hatte keinen Bezug zum Jobcenter in Kaiserslautern. Das Verwaltungsgericht setzte sich in dem Urteil auch mit dem o.g. Beschluss des Bundesverwaltungsgerichts auseinander und führte hierzu aus:

> „Macht ein Hoheitsträger – wie hier – keinen Gebrauch davon, sich im Internet durch Offenbarung der Namen der Mitarbeiter und deren Durchwahlnummern zu präsentieren, so wird ihm diese Entscheidung nicht durch die Regelungen des IFG abgenommen."

3.1.2 Online-Zugriff des Personalrats auf Zeiterfassungsdaten

Zwischen Dienststelle und Personalrat kann es zu Konflikten kommen, wenn die Unterrichtung des Personalrats unter namentlicher Nennung von Beschäftigten im Raum steht. Im Berichtszeitraum musste sich der LfDI mit der Frage beschäftigen, ob der Personalrat auf die Daten der elektronischen Zeiterfassung zugreifen darf.

Datenschutzrechtlich handelt es sich bei Datenweitergaben innerhalb einer verantwortlichen Stelle um eine Nutzung, deren Zulässigkeit sich nach §§ 31 Abs. 1, 13 LDSG beurteilt. Hiernach ist die Weitergabe personenbezogener Personaldaten an den Personalrat zulässig, wenn dies entweder eine Rechtsvorschrift ausdrücklich vorsieht oder zur Aufgabenerfüllung des Personalrats erforderlich ist.

Das Landespersonalvertretungsgesetz selbst enthält keine Verpflichtung der Dienststelle, dem Personalrat personenbezogene Daten in Bezug auf die elektronische Zeiterfassung zur Verfügung zu stellen. Es kommt daher entscheidend darauf an, ob die Wei-

tergabe mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit zu vereinbaren ist. Die Anwendung des Erforderlichkeitsgrundsatzes beinhaltet eine Prüfung dahingehend, ob es für die Aufgabenerfüllung der Personalvertretung ausreichend ist, lediglich anonymisierte bzw. pseudonymisierte Daten zu erhalten. Wenn diese Frage zu bejahen ist, scheidet die Weitergabe personenbezogener Mitarbeiterdaten aus.

Das Bundesverwaltungsgericht hat die Frage, ob der Personalrat verlangen kann, dass ihm die in der elektronischen Arbeitszeiterfassung gespeicherten Daten unter Namensnennung der Beschäftigten zur Verfügung gestellt werden, konsequent nach dem datenschutzrechtlichen Grundsatz der Erforderlichkeit entschieden (Beschluss des Bundesverwaltungsgerichts vom 19. März 2014, Az. 6 P 1/13):

Die Auflistung anonymisierter Daten zur Kontrolle der Arbeitszeiten – so das Bundesverwaltungsgericht – sei für den Personalrat ausreichend; eines eigenen unmittelbaren Zugriffs auf die Datenbank bedürfe es daher nicht.

Wörtlich führt das Bundesverwaltungsgericht hierzu aus:

„Den vorstehenden Ausführungen ist zu entnehmen, dass der Auskunftsanspruch des Antragstellers zunächst auf die Überlassung der Arbeitszeitlisten ohne Namensnennung beschränkt ist. Dies entspricht dem Grundsatz der Erforderlichkeit nach § 68 Abs. 2 Satz 1 und 2 BPersVG. Damit wird zugleich dem Grundrecht der Beschäftigten auf informationelle Selbstbestimmung Rechnung getragen (vgl. Beschluss vom 4. September 2012 a.a.O. Rn. 28). Zwar sind die Angaben über die Arbeitszeiten der Beschäftigten sowie die dabei zu bewertenden Fallgestaltungen (Dienstreisen, Urlaub, Gleittage) grundsätzlich nicht als sensibel einzustufen. Doch verbietet es der Grundsatz der Verhältnismäßigkeit, dass der Personalrat diese Angaben einer bestimmten Person zuordnen kann, ohne dass dies für die Wahrnehmung seiner Kontrollaufgabe erforderlich ist. Hinzu kommt, dass aus den Arbeitszeitlisten auch die Fehlzeiten wegen Erkrankung ersichtlich sind (vgl. Nr. 3.5 Satz 1 und Nr. 4.6.1 Satz 4 DV). Diese Angaben sind in besonderer Weise schützenswert (vgl. § 3 Abs. 9 BDSG).

Aus alledem ergibt sich, dass die Überwachungsaufgabe des Antragstellers wegen der Einhaltung arbeitszeitrechtlicher Bestimmungen in einem zweistufigen Verfahren stattfindet. Auf der ersten Stufe muss sich der Antragsteller mit der Vorlage anonymisierter Arbeitszeitlisten begnügen. Soweit die Überprüfung der Listen Unstimmigkeiten zu erkennen gibt, hat der Antragsteller auf einer zweiten Stufe Anspruch auf Erläuterungen, welche auch zur Aufdeckung der Identität des betroffenen Beschäftigten führen kann, wenn anders eine Klärung der Angelegenheit nicht möglich ist. Entsprechendes gilt, wenn die Listen Hinweise auf besondere Fallgestaltungen enthalten, welche ein Tätigwerden des Antragstellers zum Schutz des betroffenen Beschäftigten gebieten.“

3.1.3 Online-Bewerbungen

Die klassische Bewerbungsmappe auf Papier wird zunehmend zum Auslaufmodell. Nur noch rund jedes vierte Unternehmen (27 Prozent) wünscht sich von Jobinteressentinnen und -interessenten schriftliche Bewerbungsunterlagen. Mehr als doppelt so viele Personalverantwortliche (58 Prozent) bevorzugen dagegen eine Bewerbung per Internet. Das hat eine Umfrage im Auftrag des Digitalverbands BITKOM unter 408 Personalverantwortlichen aus allen Branchen im Frühjahr 2015 ergeben.

Online-Bewerbungen sind auf zwei Wegen möglich. Entweder erfolgt die Zusendung der Unterlagen per E-Mail oder über ein eigenes Online-Bewerbungsportal, bei denen die Interessentinnen und Interessenten ein Formular mit persönlichen Angaben ausfüllen und eingescannte Dokumente wie Zeugnisse und Zertifikate hochladen können.

Bei der Übersendung per E-Mail ist Folgendes zu beachten: Normalerweise erfolgt die Übertragung von E-Mails im Internet ohne besondere Absicherung, d.h. die an der Übertragung beteiligten Stellen (z.B. Internetzugangsprovider, E-Mail-Dienstleister etc.) sind grundsätzlich in der Lage, neben den für die Zustellung erforderlichen Verbindungsdaten (E-Mail-Adressen) auch die Inhalte der Nachrichten zur Kenntnis zu nehmen und diese sogar zu verändern. Um sowohl die Vertraulichkeit der Übertragung als auch die Integrität der übermittelten Daten und Authentizität der Kommunikationspartner zu gewährleisten, sind zusätzliche Sicherungsmaßnah-

men zu treffen, wie z.B. die Nutzung kryptografischer Verfahren zur Verschlüsselung und der Einsatz elektronischer Signaturen.

In der täglichen Praxis haben sich darüber hinaus Lösungen entwickelt, mit denen auch ohne entsprechende Infrastrukturen eine hinreichend sichere Kommunikation möglich ist. Beispiele hierfür sind die Nutzung von verschlüsselten Containerformaten (z.B. ZIP-Dateien), die die eigentlichen Dokumente enthalten und zu deren Öffnung ein Passwort erforderlich ist. Die Containerdatei kann den Empfangenden per E-Mail zugesandt werden, das zum Öffnen erforderliche Passwort sollte auf einem anderen Übertragungsweg (z.B. telefonisch) übermittelt werden.

Sofern lediglich unveränderbare Text- oder Grafikinformationen übermittelt werden sollen, bieten sich offene Austauschformate wie z.B. PDF-Dateien an, die ebenfalls durch Passwortschutz gegen unbefugtes Öffnen geschützt werden können. In jedem Fall sollte mit den Bewerberinnen und Bewerbern vorab abgestimmt werden, welche Sicherungsmaßnahme unterstützt wird.

Kommt ein Online-Portal zum Einsatz, gelten folgende technische Anforderungen:

- Noch vor dem Aufrufen und Ausfüllen von Masken sollten Hinweise zum Verfahren und zur Datenverarbeitung erfolgen; diese beinhalten ebenfalls eine Aussage darüber, ob eine Bewerbung auch auf dem herkömmlichen Postweg möglich ist sowie dazu, ob die Daten von der einstellenden Stelle selbst verarbeitet werden oder ob externe Dienstleister im Wege einer Auftragsdatenverarbeitung zum Einsatz kommen.
- Für die Nutzung des Portals sollte eine Registrierung und Anmeldung mit Benutzername und Passwort vorgesehen sein.
- Für den Fall, dass das Passwort vergessen wurde, sollten Sicherheitsfragen hinterlegt sein.
- Die Betroffenen sollten eine Bestätigung über die erfolgte Übermittlung ihrer Daten erhalten (z.B. über eine Bestätigung-E-Mail).
- Übertragungsweg und Speicherung müssen gegen unbefugte Zugriffe abgesichert sein (z.B. durch eine verschlüsselte HTTPS-Verbindung).
- Die Speicherung in der Online-Datenbank sollte sechs Monate nicht übersteigen.
- Für die Kommunikation mit den Bewerberinnen und Bewerbern sollten eigene Funktionsadressen eingerichtet werden.

3.2 Datenschutz im privaten Bereich

3.2.1 Rechtsprechung des Bundesarbeitsgerichts stärkt den Datenschutz

Der Datenschutz gewinnt in der Arbeitswelt weiter an Bedeutung. § 32 BDSG regelt, unter welchen Voraussetzungen Arbeitgeberinnen und Arbeitgeber personenbezogene Daten ihrer Arbeitnehmerinnen und Arbeitnehmer erheben oder verwenden dürfen. Allerdings ist diese Vorschrift zu Recht als unscharf und schwer verständlich kritisiert worden. Umso wichtiger sind Vorgaben der Rechtsprechung. Das Bundesarbeitsgericht hat mittlerweile in einer Reihe von Entscheidungen klargestellt, welche Anforderungen die Arbeitgeberschaft beim Beschäftigtendatenschutz berücksichtigen muss. Letzthin hat das Bundesarbeitsgericht in einer durchaus als spektakulär zu bezeichnenden Entscheidung klargestellt, wie § 32 BDSG auszulegen ist – und hat bei Verstößen gegen den Beschäftigtendatenschutz sogar ein Beweisverwertungsverbot angenommen.

Die Arbeitsgerichte haben seit der Einführung von § 32 BDSG zum 1. September 2009 bereits in einer Reihe von Entscheidungen wichtige Vorgaben zum Beschäftigtendatenschutz gemacht. Neben dem Bundesarbeitsgericht haben auch andere Gerichte Entscheidungen mit erheblichen Auswirkungen auf die Datenschutzpraxis gefällt. Zuletzt verurteilte etwa der Bundesgerichtshof zwei Privatermittler wegen unzulässiger Überwachungsmaßnahmen zu Haftstrafen (vgl. Bundesgerichtshof ZD 2013, Seite 502 ff.; Urteil vom 4. Juni 2013 – 1 StR 32/13) Die Gerichte nehmen den Datenschutz jetzt erkennbar sehr ernst, mit drastischen Folgen vor allem für Unternehmen. Verletzungen der informationellen Selbstbestimmung werden zunehmend härter und konsequenter geahndet. Zugleich wählen die Gerichte als Anknüpfungspunkt nicht mehr allein das Allgemeine Persönlichkeitsrecht, sondern – systematisch richtig – das Bundesdatenschutzgesetz, insbesondere § 32 BDSG.

Mit einem Urteil zur Verwertbarkeit datenschutzwidrig erhobener Beweise (Bundesarbeitsgericht ZD 2014, Seite 260; Urteil vom 20. Juni 2013 – 2 AZR 546/12) schafft der 2. Senat nun weitere Klarheit. Anlässlich einer rechtswidrigen weil gegen Datenschutzrecht verstoßenden Spindkontrolle durch den Arbeitgeber stellt das Bundesarbeitsgericht fest, dass es sich bei der in Rede stehenden Schrankkontrolle tatbestandlich um eine Datenerhebung im Sinne des Bundesdatenschutzgesetzes handelt. Der hier einschlägige § 32 BDSG setze keinerlei technische Datenverarbeitung voraus, etwa dass die Datenerhebung zum Zwecke ihrer Nutzung und Verarbeitung in automatisierten Dateien erfolge. Die Vorschrift erfasse damit sowohl nach ihrem Wortlaut als auch nach ihrem Regelungszweck die Datenerhebung durch rein tatsächliche Handlungen – wie etwa eine Spinddurchsuchung.

Gleichzeitig bewertet das Bundesarbeitsgericht das Vorgehen des Arbeitgebers als datenschutzrechtlich unzulässig. Der persönliche Schrank eines Arbeitnehmers und dessen Inhalt seien Teil seiner Privatsphäre, in die nur nach Maßgabe des Verhältnismäßigkeitsgrundsatzes eingegriffen werden darf. Vorliegend beanstandet das Bundesarbeitsgericht, dass der Arbeitgeber den Eingriff nicht nach Information und in Anwesenheit des Arbeitnehmers durchführte, was ein milderer Eingriff gewesen wäre, sondern ohne dessen Beteiligung, also heimlich.

Da es im vorliegenden Fall an einer Rechtfertigung der Spinddurchsuchung nach § 32 BDSG fehle, seien die Erkenntnisse aus der Durchsuchung des Spinds auch nicht prozessual verwertbar. Zwar kenne die Zivilprozessordnung kein generelles prozessuales Verwendungs- bzw. Verwertungsverbot für rechtswidrig erlangte Informationen oder Beweismittel. Die Verwertung von Beweismitteln, die der Arbeitgeber rechtswidrig erlangt habe, scheide jedoch dann aus, wenn sich deren prozessuale Verwertung als erneuter bzw. fortgesetzter Eingriff in das allgemeine Persönlichkeitsrecht des Klägers darstelle, der nicht durch überwiegende Interessen des Arbeitgebers gerechtfertigt sei. Damit dürfte die gerichtliche Verwertung von datenschutzwidrig gesammelten Kündigungsgründen in der Praxis künftig in vielen Fällen ausscheiden.

Das Bundesarbeitsgericht stellt damit in seiner Entscheidung hohe Anforderungen an den Umgang mit Beschäftigtendaten. Gerade für Compliance-Kontrollen und interne Ermittlungen hat das Urteil erhebliche Folgen. Letztlich verpflichten die Richter den Arbeitgeber, bei kritischen Datenerhebungen oder der weiteren Verwendung von Daten genau darauf zu achten, aus den zur Verfügung stehenden, gleich effektiven Maßnahmen stets das mildeste Mittel mit der geringsten Eingriffstiefe auszuwählen. Dabei stellt das Bundesarbeitsgericht mit großer Klarheit heraus, dass heimliche Überwachungsmaßnahmen einen wesentlich massiveren Grundrechtseingriff darstellen als offene.

Das Urteil betrifft insbesondere auch Fallkonstellationen, in denen die Arbeitgeberseite den Beschäftigten Betriebsmittel zur Nutzung überlässt, die private Informationen betreffen; hier den Spind. Eine Übertragung dieser Grundaussagen des Bundesarbeitsgerichts auf vergleichbare Konstellationen – wie etwa die Kontrolle des (auch) zur privaten Nutzung überlassenen E-Mail-Zugangs der Beschäftigten – liegt dabei auf der Hand.

Der LfDI begrüßt die neue Richtung, welche die Rechtsprechung der Arbeitsgerichte damit eingeschlagen hat und sieht sich in seiner Beurteilung der Grenzen der Kontrollbefugnisse des Arbeitgebers und der Folgen von Datenschutzverstößen bestärkt. Diese Maßstäbe wird der LfDI auch seiner zukünftigen Tätigkeit im wichtigen Bereich des Beschäftigtendatenschutzes zugrunde legen.

3.2.2 IT-Nutzung am Arbeitsplatz (Orientierungshilfe)

Viele Beschäftigte haben heute an ihrem Arbeitsplatz neben Telefon und Faxgerät auch Zugang zum Internet und damit die Möglichkeit, per E-Mail, Chat oder VoIP zu kommunizieren. Arbeitgeberinnen und Arbeitgeber, deren Beschäftigte Informations- und Kommunikationstechnik (IuK) zu betrieblichen oder privaten Zwecken nutzen, erheben und verarbeiten dabei personenbezogene Daten der Beschäftigten selbst sowie ihrer inner- und außerbetrieblichen Kommunikationspartnerinnen und -partner und weiterer Betroffener (etwa in einer E-Mail erwähnter Dritter); insoweit haben die Arbeitgeberinnen und Arbeitgeber datenschutzrechtliche Anforderungen zu

beachten, die sich je nach Kommunikationszweck, -partner und -mittel unterscheiden und auch davon abhängen, ob den Beschäftigten neben der betrieblichen auch die private Nutzung der betrieblichen IuK ganz oder teilweise am Arbeitsplatz gestattet ist. Entsprechend differenziert sind die Anforderungen an die datenschutzgerechte Verwendung dieser Daten, insbesondere an Kontrollmaßnahmen der Arbeitgeberinnen und Arbeitgeber.

In der Praxis herrscht aufgrund der angesprochenen Vielfältigkeit der Nutzungs- und Überwachungsmöglichkeiten einerseits und der Differenziertheit der Rechtslage andererseits erhebliche Unsicherheit. Die Aufsichtsbehörde für den Datenschutz trifft regelmäßig auf Unternehmen, die trotz ihres Bemühens um faire und akzeptable Nutzungsbedingungen für die betriebliche IuK gravierende, teilweise sogar strafrechtlich relevante Fehler begehen. Andererseits kennen viele Beschäftigte häufig nicht die Grenzen zulässiger Nutzungen und fühlen sich unsicher, weil sie vermuten, dass ihnen die Arbeitgeberin oder der Arbeitgeber oder die EDV bei der IuK-Nutzung am Arbeitsplatz „über die Schulter guckt“ oder gar ihre private Kommunikation ausspäht. Betriebsräte schließlich suchen immer häufiger den Rat der Aufsichtsbehörde, weil sie zur IuK-Nutzung Betriebsvereinbarungen abschließen oder bestehende prüfen lassen wollen. In allen diesen Fällen kann eine Orientierungshilfe der Aufsichtsbehörde dabei helfen, bestehende Rechtsunsicherheiten durch klare Vorgaben zu beseitigen.

Der LfDI hat im Mai 2015 eine solche Orientierungshilfe erarbeitet (http://www.datenschutz.rlp.de/downloads/oh/oh_iuk_arbeitsplatz.pdf), sie stellt überblicksartig die bei der Nutzung der IuK geltenden datenschutzrechtlichen Anforderungen dar. Sie richtet sich an private Arbeitgeberinnen und Arbeitgeber, ihre Beschäftigten und Interessenvertretungen, ist aber grundsätzlich auch für den öffentlichen Dienst von Interesse, wobei dort zusätzlich landesspezifische Vorschriften etwa im Landesdatenschutzgesetz zu beachten sind. Die Orientierungshilfe bezieht nicht nur die aktuelle Rechtslage, insbesondere die Regelungen des § 32 BDSG, sondern auch arbeitsrechtliche Grundsätze mit ein, da sich der Erforderlichkeitsmaßstab des Bundesdatenschutzgesetzes auch am Arbeitsrecht orientiert.

3.2.3 Betriebsvereinbarungen als Erlaubnis zum Umgang mit Arbeitnehmerdaten

Das Bundesdatenschutzgesetz konkretisiert das Recht auf informationelle Selbstbestimmung und regelt, in welchem Umfang Eingriffe in dieses Recht zulässig sind. Fehlt es an einer Ermächtigungsgrundlage i.S.v. § 4 Abs. 1 BDSG, so ist das Erheben, Verarbeiten oder Nutzen personenbezogener Daten verboten. In Arbeitsverhältnissen kommt – neben gesetzlichen Ermächtigungsgrundlagen und der regelmäßig unpraktikablen Einwilligung – auch eine zwischen Arbeitgeberseite und Betriebsrat abgeschlossene Betriebsvereinbarung als Rechtsgrundlage für die Verwendung von Beschäftigtendaten in Betracht.

In einer Entscheidung aus dem Jahre 2013 (Bundesarbeitsgericht, NZA 2013, S. 1433; Beschluss vom 9. Juli 2013 – 1 ABR 2/13 (A)) bestätigte der 1. Senat des Bundesarbeitsgerichts, dass sorgfältig und angemessen gestaltete Betriebsvereinbarungen Gewähr für die Einhaltung der Vorgaben des Datenschutzes und des Betriebsverfassungsrechts bieten können. Betriebsvereinbarungen sind „sonstige Rechtsvorschriften” i.S.v. § 4 Abs. 1 BDSG. Im Ergebnis verschärft das Bundesarbeitsgericht mit dieser Entscheidung seine bisherige Rechtsprechung zum Umgang mit Arbeitnehmerdaten auf der Grundlage von Kollektivvereinbarungen.

Der LfDI sieht seine Rechts- und Beratungspraxis auch insoweit von der arbeitsgerichtlichen Rechtsprechung bestätigt, er hat auch im Berichtszeitraum auf Ansuchen von Arbeitgeber- wie auch von Arbeitnehmer- bzw. Betriebsratsseite abgeschlossene Betriebsvereinbarungen auf ihre Vereinbarkeit mit dem Bundesdatenschutzgesetz geprüft und Hinweise zur optimalen Umsetzung datenschutzrechtlicher Vorgaben in Kollektivvereinbarungen gegeben. Darüber hinaus hat er Verhandlungen zum Abschluss von Betriebsvereinbarungen in rheinland-pfälzischen Betrieben unterstützt und so dazu beigetragen, passgenaue datenschutzrechtliche Vereinbarungen auf Betriebsebene zu erstellen und umzusetzen.

4. Polizei und Verfassungsschutz

4.1 Prüfung der Antiterrordatei

Islamistische „Gefährder“ und „relevante Personen“ werden – bei Vorliegen der im Antiterrordateigesetz genannten Voraussetzungen – in der gemeinsamen Antiterrordatei der Sicherheitsbehörden des Bundes und der Länder (unter Einschluss der Verfassungsschutzbehörden) gespeichert (vgl. 24. Tb., Tz. 4.1.9 sowie 25. Tb. der BfDI, Tz. 5.2).

Aufgrund des Urteils des Bundesverfassungsgerichts zum Antiterrordateigesetz (Urteil des Ersten Senats vom 24. April 2013, Az. 1 BvR 1215/07) wurde die Verpflichtung der Datenschutzbeauftragten des Bundes und der Länder in das Gesetz aufgenommen, spätestens alle zwei Jahre die Durchführung des Datenschutzes beim Betrieb der Antiterrordatei zu prüfen (§ 10 Abs. 2 ATDG).

Dementsprechend hat der LfDI eine Prüfung im Land durchgeführt. Nach der Beantwortung eines umfangreichen schriftlichen Fragenkatalogs des LfDI durch das Landeskriminalamt wurden Kontrollbesuche beim Landeskriminalamt sowie in allen Polizeipräsidien des Landes durchgeführt.

Die Zahl der von den Polizeien des Bundes und der Länder in der Antiterrordatei gespeicherten Gefährder ist überschaubar. Aus Geheimhaltungsgründen darf die genaue Zahl der von Landesdienststellen veranlassten Speicherungen nicht bekannt gegeben werden. Die vom Bundesinnenminister veröffentlichte Zahl der im ganzen Bundesgebiet bekannten Gefährder von 427 Personen (Stand: November 2015) ermöglicht aber einen Rückschluss auf die rheinland-pfälzischen Zahlen.

Die Prüfung des LfDI hat Folgendes ergeben:

- Sämtliche gespeicherten Personen waren nach den Kriterien des Gesetzes rechtmäßig gespeichert.
- Die vorgesehenen und praktizierten Verfahren stellen eine ordnungsgemäße Datenlöschung im Falle des Wegfalls der Speichervoraussetzungen sicher.
- Die Quellen für die gespeicherten Dateien sind nachvollziehbar erfasst.
- Die Protokollierung der Zugriffe auf die Datei ist ausreichend, um nachvollziehen zu können, wer wann aus welchen Gründen Zugriff auf die Daten genommen hat.
- Das Zugriffsberechtigungskonzept entspricht den datenschutzrechtlichen Anforderungen.

Insgesamt hat sich kein Anlass für datenschutzrechtliche Beanstandungen ergeben.

4.2 Prüfung der Datei- und Aktenführung beim Landesverfassungsschutz

Im Berichtszeitraum wurde die Prüfung der Datei- und Aktenführung beim Landesverfassungsschutz abgeschlossen. Vor dem Hintergrund spektakulärer Feststellungen einer vergleichbaren Prüfung des niedersächsischen Verfassungsschutzes waren auch in Rheinland-Pfalz Befürchtungen laut geworden, dass eine überbordende Datenspeicherung in diesem Bereich erfolgen könnte. In Niedersachsen waren Hauptkritikpunkte, dass kritische Journalistinnen und Journalisten unberechtigt in den Systemen des Verfassungsschutzes gespeichert und dass Minderjährige erfasst worden seien, ohne dass es dafür eine Rechtsgrundlage gegeben habe.

Diese Aspekte wurden durch den LfDI – neben zahlreichen anderen – durch Stichprobenprüfungen von Akten und Dateispeicherungen besonders in den Blick genommen. Die sehr zeitaufwändige Prüfung mit zahlreichen Ortsterminen ergab allerdings, dass in Rheinland-Pfalz keine Rede davon sein kann, dass der Verfassungsschutz vergleichbare Fehler wie das niedersächsische Pendant begehen würde.

Der LfDI hatte nur Anlass, eher marginale Verbesserungsvorschläge im Bereich des technisch-organisatorischen Datenschutzes zu formulieren. Bei der Prüfung der materiellen Speichervoraussetzungen erfasster Personen sowie bei der Prüfung der zeitgerechten Datenlöschung hat sich kein Grund zur Kritik ergeben.

Unabhängig von dieser Prüfung, bei der der Verfassungsschutz sich als sehr kooperativ erwiesen hat, ist aber kritisch anzumerken, dass die ebenfalls beabsichtige Prüfung seiner Aktivitäten im Rahmen der Gemeinsamen Zentren der Sicherheitsbehörden zur Terrorismusbekämpfung bislang nicht zustande

kam. Hier wird der LfDI weiter aktiv bleiben, um auch hier keinen kontrollfreien Raum entstehen zu lassen.

4.3 Bodycams bei der Polizei

Aufgrund der hessischen Erfahrungen hat das Innenministerium des Landes den Einsatz von Bodycams durch Streifenpolizisten testweise ab April 2015 eingeführt. Zunächst wurde ein Pilotprojekt in Mainz und eines in Koblenz, Stadtteil Neuendorf, durchgeführt. Dazu wurde dem LfDI ein ausführliches schriftliches Konzept vorgelegt.

Die Bodycams sollen nicht nur der Eigensicherung der Polizeibediensteten, sondern auch der Beweissicherung (evtl. auch zugunsten der Betroffenen) dienen. Je nach der Einsatzsituation kommen als Rechtsgrundlagen verschiedene Alternativen in Betracht, die nach § 27 POG dem Grunde nach die Datenerhebung mittels Videoaufzeichnungen rechtfertigen können.

Da kein flächendeckender Einsatz geplant ist, sollen nur besonders gefährdete bzw. kriminalitätsbelastete Gebiete bzw. besondere Gefahrenlagen (etwa Großveranstaltungen) für das Pilotprojekt ausgewählt werden. Eine (verbindliche) Festlegung dieser Einsatzbedingungen ist auf dem Weg einer Verwaltungsvorschrift des Innenministeriums erfolgt. Hierin werden die Bedingungen der Aktivierung der Aufnahmen, der Nutzung und der Löschung detailliert vorgegeben.

Aufgenommen werden nicht nur Bilder, sondern auch Sprache. Die Rechtsgrundlagen in § 27 POG ermöglichen dies grundsätzlich, soweit sie anwendbar sind. Diesen Punkt sieht der LfDI aber besonders kritisch; er wird im Rahmen der vorgesehenen Evaluation ein besonderes Gewicht auf die Frage legen, ob diese intensive Form der Beobachtung und Aufzeichnung wirklich unerlässlich ist.

Alle Fragen sind im Vorfeld ausführlich mit dem Innenministerium besprochen und geklärt worden. Besonders bedeutsam ist aus der Sicht des LfDI, dass eine wissenschaftliche Begleitung zum Zweck der Evaluierung des Verfahrens erfolgt. Ein entsprechender Bericht soll im Laufe des Jahres 2016 vorgelegt werden.

4.4 Polizei im Dialog – das Telemediengesetz gilt für alle Internetdiensteanbieter

Die Polizei Ludwigshafen hat ein Portal im Internet eröffnet, das der Kontaktpflege mit den Bürgerinnen und Bürgern dienen soll. Es ist für Jeden unter der Bezeichnung „Polizei im Dialog“ abrufbar (https://pid.polizei.rlp.de).

Dieses Portal ist aus Datenschutzsicht grundsätzlich zu begrüßen, weil damit der Versuch unternommen wird, unabhängig von Facebook und in datenschutzkonformer Weise die Dialogfunktionen des Internets für einen intensiveren Bürgerkontakt zu nutzen (vgl. Tz. I-1.3).

Allerdings gelten die Schutzvorschriften des Telemediengesetzes in gleicher Weise für private wie für staatliche Internetdiensteanbieter. Darauf musste der LfDI die Polizei hinweisen, nachdem er die erste Version dieses Angebots im Netz zur Kenntnis bekommen hatte. Dies gilt vor allem bezüglich der Datenschutzerklärung (§ 13 Abs. 1 TMG), aber auch für den Umfang der bei einer Anmeldung geforderten Nutzerdaten. Diese haben sich auf das zu beschränken, was für die Erbringung der Dienstleistung erforderlich ist.

Die Polizei hat auf die Hinweise des LfDI rasch und positiv reagiert, so dass der derzeitige Internetauftritt aus der Sicht des LfDI datenschutzrechtlich unproblematisch ist.

4.5 PIAV – Polizeilicher Informations- und Analyseverbund

Die Polizeibehörden von Bund und Ländern sind gesetzlich verpflichtet, einen Informationsverbund zu betreiben, damit Gefahrenabwehr und Straftatenbekämpfung nicht durch Ländergrenzen behindert werden (vgl. insbesondere §§ 7 ff., 11 BKAG). Die traditionellen Systeme – insbesondere die Verbunddateien im Rahmen des INPOL-Systems – orientieren sich eng an den gesetzlichen Vorgaben. Die technische Weiterentwicklung und die praktischen Bedürfnisse der Polizeibehörden machen allerdings ständige Anpassungen erforderlich. Nunmehr ist eine grundlegende Neuentwicklung unter dem Namen „Polizeilicher Informations- und Analyseverbund – PIAV“ geplant.

Die Strukturen dieses Systems werden unter Datenschutzaspekten in einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und einiger Länder erörtert; an dieser Arbeitsgruppe ist der LfDI beteiligt. Die BfDI hat in ihrem letzten Tätigkeitsbericht die dabei erkannten und zu beantwortenden Datenschutzfragen im Einzelnen dargestellt (25. Tb. der BfDI, Tz. 5.13.2). Es ist deutlich geworden, dass mit diesem neuen System die „Belastbarkeit der bisherigen rechtlichen Regelungen“ des BKA-Gesetzes „ausgereizt“ wird, wie es die BfDI ausgedrückt hat.

Auf der Ebene des Landes müssen ebenfalls neue Strukturen geschaffen werden, um die Landesdaten in das neue Informationssystem einspeisen und um die Abrufmöglichkeiten datenschutzgerecht gestalten zu können. In diesem Zusammenhang haben mehrere Gespräche mit dem Innenministerium und dem Landeskriminalamt stattgefunden. Die bisherigen Planungen auf Landesebene tragen den Datenschutzanforderungen Rechnung.

4.6 Polizeigesetzliche Eingriffsregelungen auf dem Prüfstand (§ 100 POG)

In der 15. Legislaturperiode (die am 18. Mai 2011 endete) wurde durch Ergänzungen des Polizeigesetzes des Landes den Bedürfnissen der Sicherheitsbehörden nach neuen Eingriffsinstrumenten an zahlreichen Punkten Rechnung getragen. Im Vordergrund stand dabei das Anliegen, angesichts der zunehmenden Internetnutzung die Polizei in die Lage zu versetzen, ihre gefahrenabwehrenden und strafverfolgenden Aufgaben weiterhin effizient erfüllen zu können. Besonders bedeutsam für die datenschutzpolitische Diskussion war dabei die Einführung der „Quellen-Telekommunikationsüberwachung“ und der „Online-Durchsuchung“ (vgl. 23. Tb., Tz. II-4.1).

Die Ergänzung des Polizei- und Ordnungsbehördengesetzes enthält auch zahlreiche Regelungen, die dem Schutzbedürfnis der Bürgerinnen und Bürger vor einer extensiven Nutzung dieser neuen Instrumente Rechnung tragen. Neben der Vorschrift zur Pflicht der Polizeibehörden, besondere technisch-organisatorische Schutzvorkehrungen einzurichten (§ 41 POG), restriktiv formulierten Anwendungsvoraussetzungen dieser Eingriffsbefugnisse und regelmäßigen Berichtspflichten gegenüber dem Parlament (gem. §§ 29 Abs. 8 und 31 Abs. 7 Satz 2 POG) gehört dazu die Verpflichtung, folgende Eingriffsbefugnisse auf ihre Nützlichkeit und Angemessenheit in der Praxis wissenschaftlich prüfen zu lassen, zu „evaluieren“ (gem. § 100 POG):

- Verdeckte Datenerhebungen in oder aus Wohnungen (sogen. „Großer Lauschangriff“ gem. § 29 POG);
- Telekommunikationsüberwachung einschließlich der „Quellen-TKÜ“ (§ 31 POG);
- Auskunft über Nutzungsdaten der Internet- und Telekommunikationsnutzung (§ 31b POG);
- Online-Durchsuchung (§ 31c POG);
- Funkzellenabfragen (§ 31e POG);
- Rasterfahndung (§ 38 POG).

Im Gesetz ist als „Evaluationszeitraum“ der Zeitraum vom 1. April 2011 bis zum 31. März 2016 bezeichnet (§ 100 Abs. 1 Satz 1 POG). Im „Koalitionsvertrag 2011 bis 2016“ haben die Regierungsfraktionen allerdings vereinbart, die in § 100 POG vorgesehene Evaluierung bereits mit Ablauf des Jahres 2013 vorzunehmen (S. 82 des Koalitionsvertrages). Aus der Sicht des LfDI war diese Vereinbarung zu begrüßen. Damit ergab sich die Chance, frühzeitig Korrekturen im Sinne einer Stärkung der Bürgerrechte vorzunehmen.

Mit der Erstellung der wissenschaftlichen Vorbereitung und der Durchführung entsprechender Untersuchungen, die zur Grundlage des von der Landesregierung dem Parlament vorzulegenden Berichts werden sollten, wurde ein im Land ansässiges wissenschaftliches Institut für Rechtsfolgenabschätzung beauftragt. Dem LfDI übersandte die Landesregierung im April 2014 dann das Ergebnis dieser wissenschaftlichen Untersuchung sowie ihren Entwurf eines entsprechenden Berichts.

Der LfDI wies zunächst darauf hin, dass angesichts der geringen Fallzahlen der Nutzung der verschiedenen Eingriffsbefugnisse eine Bewertung der praktischen Folgen schwierig sei. Gerade auch unter dem Aspekt, welche Auswirkungen entsprechende polizeiliche Eingriffe auf die Betroffenen haben, sei mangels konkreter Erfahrungen eine Bewertung schwierig. Er gab auch zu bedenken, ob nicht die Nichtanwendung bestimmter Eingriffsbefugnisse als Argument gegen ihre Notwendigkeit angesehen

werden müsse. Außerdem formulierte der LfDI einige Vorschläge zur Änderung des geltenden Rechts; diese bezogen sich insbesondere auf die Unterrichtung Betroffener nach Abschluss der Ermittlungsmaßnahmen, um sie in die Lage zu versetzen, nachträglich ihre Rechte wahrzunehmen. Zudem ist die Transparenz staatlichen Handelns auch im Bereich der Gefahrenabwehr aus der Sicht des LfDI ein wichtiges Mittel, um die Legitimität staatlichen Handelns zu erhöhen und Vertrauen in den Rechtsstaat zu begründen.

Zu einer weiteren inhaltlichen Diskussion dieser Fragen kam es deshalb nicht, weil die Landesregierung in der Folge von ihrem Vorhaben der vorgezogenen Evaluation der genannten Eingriffsmaßnahmen im Polizei- und Ordnungsbehördengesetz Abstand nahm. Nunmehr soll erst zum gesetzlich vorgesehenen Zeitablauf (also nach dem 31. März 2016) eine solche Evaluation erfolgen.

Angesichts des Mangels an praktischen Erfahrungen bis Ende des Jahres 2013 ist diese Entscheidung sicherlich nachvollziehbar. Der LfDI ist zuversichtlich, dass er seine Anliegen auch in die im Laufe des Jahres 2016 zu erwartende Diskussion um die dann erfolgende Evaluation wirksam einbringen kann.

5. Gesundheit

5.1 Datenschutz bei Krankenhausinformationssystemen; Prüfungsreihe des LfDI

Schon seit geraumer Zeit beschäftigen sich die Datenschutzbeauftragten des Bundes und der Länder intensiv mit dem datenschutzgerechten Einsatz von Krankenhausinformationssystemen (KIS). Die in diesem Zusammenhang entwickelte Orientierungshilfe sowie die im Lande zur Umsetzung der datenschutzrechtlichen Vorgaben seitens des LfDI durchgeführten Maßnahmen waren bereits mehrfach Gegenstand des Tätigkeitsberichtes (vgl. 23. Tb., Tz. I-3.6; 24. Tb., Tz. II-7.1).

Im Berichtszeitraum hat der LfDI die im September 2013 begonnenen örtlichen Feststellungen bei einzelnen Krankenhäusern im Land fortgesetzt. Insgesamt wurden in der Prüfungsreihe bis Februar 2015 neun Einrichtungen unterschiedlicher Träger besucht. Schwerpunkt der Prüfungen waren neben dem Einsatz der Krankenhausinformationssysteme und der in diesem Zusammenhang vorhandenen technisch-organisatorischen Vorkehrungen zum Schutz der Patientendaten auch die flankierend ergriffenen Maßnahmen wie z.B. das Datenschutzmanagement der Einrichtung oder der Grad der Einbindung der Leitungsebene.

Hintergrund für die arbeitsintensiven Kontrollen war der sich schon im Jahre 2013 im Zusammenhang mit der Umfrage und den darauf hin erfolgten Kontakten andeutende Eindruck, dass die Kliniken zwar die Bedeutung datenschutzrechtlicher Vorkehrungen beim Einsatz von IT erkannt haben, gleichwohl im Alltag und angesichts der vielfältigen Herausforderungen, denen sich die Krankenhäuser stellen müssen, deren Umsetzung häufig aus dem Blick gerät. Im Ergebnis hat sich dieser Eindruck bei den durchgeführten Kontrollen bestätigt, wobei es durchaus bemerkenswerte Unterschiede in den einzelnen Häusern bei der Priorisierung des Datenschutzes und der hierfür erforderlichen Maßnahmen gab. Im Einzelnen:

Insgesamt offenbarten die Prüfungen recht schnell, dass trotz der allgemeinen Bereitschaft, die datenschutzrechtlichen Anforderungen zu erfüllen, in der Praxis teilweise noch gravierende Handlungsdefizite bei dem Betrieb der Krankenhausinformationssysteme bestehen. Problemfelder waren u.a. die zu weitgehende Gewährung von Zugangsmöglichkeiten zu den in den Informationssystemen vorgehaltenen Patientendaten, die regelmäßig fehlende digitale Archivierung, die unzureichende Protokollierung sowie die in allen Systemen fehlenden Löschungsmöglichkeiten. Darüber hinaus wurden teilweise externe Stellen ohne vertragliche Grundlage in die Verarbeitung von Patientendaten eingebunden.

Aber es gab auch positive Beispiele: in drei der besuchten Häuser waren sowohl das Datenschutzmanagement als auch die interne Revision der eingesetzten IT-Systeme vorbildlich. Ein wesentlicher Faktor hierfür war der Umstand, dass die Geschäftsführung selbst die Beachtung des Datenschutzes zur Chefsache machte: die Datenschutzbeauftragten wurden von Anfang in sämtliche datenschutzrelevanten Prozesse des Krankenhauses eingebunden. Alle zur Einhaltung des Datenschutzes und der IT-Sicherheit notwendigen Maßnahmen wurden von der Geschäftsführung selbst angeordnet.

Gleichzeitig haben auch die KIS-Hersteller signalisiert, dass sie in diesem Zusammenhang ihrer Verantwortung gerecht werden wollen. Dies gilt einerseits für die Entwicklung gegenwärtig nicht vorhandener Funktionalitäten, die für einen datenschutzgerechten Betrieb aber unverzichtbar sind, wie z.B. die Löschung oder die automatisierte Einräumung zeitlich beschränkter Zugriffsbefugnisse. Dies gilt andererseits aber auch für die effektive Unterstützung der Krankenhäuser bei der Nutzung der eingesetzten KIS. Es hatte sich nämlich im Rahmen der Prüfungen herausgestellt, dass teilweise aufgedeckte Defizite im KIS-Betrieb auf der Unkenntnis der Nutzerinnen und Nutzer oder der Komplexität der Systeme beruhen. Hier gilt es, benutzerfreundliche Lösungen zu erarbeiten.

Im Juni 2015 fand in Abstimmung mit dem LfDI ein von der Krankenhausgesellschaft Rheinland-Pfalz und dem Verband der Klinikdirektoren in Rheinland-Pfalz und dem Saarland getragener Workshop statt, der den Einrichtungen die Möglichkeit bot, sich gegenseitig über ihre bislang gemachten Erfahrungen bei der klinikinternen IT-Revision auszutauschen und zugleich unmittelbar mit KIS-Herstellern in

Kontakt zu treten. Die auf dem Gelände des Westpfalz-Klinikums in Kaiserslautern hervorragend organisierte und sehr gut angenommene Veranstaltung zeigte eindrucksvoll, wie sehr sich sowohl das Bewusstsein als auch die ergriffenen Maßnahmen bei den Häusern seit Beginn der bundesweiten Diskussion im Jahre 2011 verändert haben.

Fazit und Ausblick

Auch zu Beginn des Jahres 2016 werden noch nicht alle Vorgaben des Datenschutzes im digitalen Klinikalltag in Rheinland-Pfalz umgesetzt worden sein. Aber das ist vielleicht gar nicht so gravierend. Entscheidender ist vielmehr, dass zumindest die durch den LfDI betreuten Krankenhäuser mittlerweile die Erkenntnis gewonnen haben, den Einsatz digitaler Informationstechnik im Klinikbetrieb durch geeignete technische und organisatorische Maßnahmen zum Schutz der Patientendaten absichern zu müssen, und in diesem Sinne nunmehr auch tätig werden. Hierbei werden die Krankenhäuser in Rheinland-Pfalz auch weiterhin nicht alleine gelassen.

5.2 Datenschutz und IT-Sicherheit in der Arztpraxis

Schweigepflicht und Vertraulichkeit gehören zu den Basics jeder ärztlichen Versorgung. Gleichwohl sind vielen Heilberufsangehörigen die daraus resultierenden Konsequenzen für den Betrieb der eigenen Praxis kaum bekannt. Spätestens beim Einsatz moderner Informations- und Kommunikationstechnologie einschließlich der Nutzung von Webdiensten kann dies zum GAU führen. Mit der Anfang 2014 gestarteten gemeinsamen Initiative des LfDI und der Kassenärztlichen Vereinigung Rheinland-Pfalz möchte man dieser Gefahr entgegenwirken und die ärztlichen Behandlerinnen und Behandler für das ungeliebte Thema sensibilisieren.

Seit Übernahme der datenschutzrechtlichen Aufsichtszuständigkeit durch den LfDI im Bereich der niedergelassenen medizinischen Behandlungspraxen im Jahre 2009 haben die Anfragen und Beschwerden zur Datenverarbeitung deutlich zugenommen. Geschuldet ist dies einem weit verbreiteten Informationsdefizit bei den Praxisbetreibern (vgl. hierzu bereits 23. Tb., Tz. II-5.2.4 sowie 24. Tb., Tz. II-3.3). Manchen Ärztinnen und Ärzten oder Psychotherapeutinnen und -therapeuten ist einfach nicht bekannt, welche rechtlichen und technischen Anforderungen an einen sicheren Einsatz von Informationstechnologie im Praxisbetrieb bestehen. Unklarheiten gibt es auch über die Auswirkungen der ärztlichen Schweigepflicht auf den Praxisalltag oder den Umfang der den Patientinnen und Patienten zustehenden Einsichtsrechte.

Angesichts der damit verbundenen erheblichen Gefährdungspotentiale für den Umgang mit den sensiblen Behandlungsdaten und das informationelle Selbstbestimmungsrecht der Patientinnen und Patienten hat der LfDI im Januar 2014 zusammen mit der Kassenärztlichen Vereinigung Rheinland-Pfalz die Initiative „Mit Sicherheit gut behandelt“ gestartet. Ziel des Projektes ist es, die Adressaten einerseits für die Thematik zu sensibilisieren, andererseits sie über die bestehenden rechtlichen Vorgaben zu informieren und, soweit möglich, Handlungsempfehlungen zu geben.

Im Rahmen der Initiative wurden folgende Instrumente entwickelt:

5.2.1 Website „www.mit-sicherheit-gut-behandelt.de“

Auf der Website www.mit-sicherheit-gut-behandelt.de werden thematisch strukturiert umfangreiche Materialien, Handlungsanleitungen, Checklisten und Rechtsgrundlagen zur IT-Sicherheit und den Vorgaben des Datenschutzes bei dem Betrieb einer Arzt- oder Psychotherapeutenpraxis bereitgestellt. Damit können die Praxisbetreiberinnen und -betreiber die bereits zahlreich vorhandenen, aber bislang verstreuten Inhalte zu der Thematik auf einer einheitlichen digitalen Plattform leichter erschließen. Durch die in den einzelnen Seiten integrierten Links haben die Nutzerinnen und Nutzer die Möglichkeit, auch von anderen Stellen in diesem Zusammenhang verfasste Materialien und Serviceangebote zu finden und ggf. bei ihrem weiteren Vorgehen zu berücksichtigen.

5.2.2 Regionale Veranstaltungen

Im Laufe des Jahres 2014 haben die Kooperationspartner an den vier Standorten der Kassenärztlichen

Vereinigung Rheinland-Pfalz in Trier, Neustadt/Weinstraße, Mainz und Koblenz halbtägige Informationsveranstaltungen angeboten, in denen ausgewählte Themenfelder zu Fragen der IT-Sicherheit und zum Datenschutz aufbereitet und diskutiert wurden. Zudem bestand die Möglichkeit, konkrete Anliegen der Betroffenen aus ihrem ärztlichen Alltag mit den Referierenden zu klären. Mit den regionalen Veranstaltungen haben die Kooperationspartner einen direkten Dialog mit den Praxisinhaberinnen und –inhabern sowie deren Beschäftigte aufgebaut, der beiden Seiten wertvolle Erkenntnisse im Zusammenhang mit der Beachtung der bestehenden Anforderungen lieferte.

5.2.3 Beiträge in Publikationsorganen

Mit regelmäßigen Beiträgen zu Einzelthemen aus den Bereichen IT-Sicherheit und Datenschutz sowohl im Mitteilungsblatt der Kassenärztlichen Vereinigung Rheinland-Pfalz als auch dem rheinland-pfälzischen Ärzteblatt konnten die Betroffenen ebenfalls sensibilisiert und auf die Hilfestellungen der Initiative aufmerksam gemacht werden.

5.2.4 Kontakt mit Systemherstellern und Heilberufskammern

Eine Verbesserung von IT-Sicherheit und Datenschutz bei den niedergelassenen Ärztinnen und Ärzten und Psychotherapeutinnen und -therapeuten hängt nach Auffassung des LfDI nicht nur von den Anstrengungen der Praxisbetreiberinnen und -betreiber ab. So ist ein datenschutzgerechter Betrieb der Praxissoftware nur dann möglich, wenn die eingesetzten Systeme dies auch funktional zulassen. Ob dies der Fall ist, liegt in der Verantwortung der Systemhersteller. Zudem bilden die Vorgaben des Berufsrechts, insbesondere die ärztliche Schweigepflicht, den Rahmen für die Gestaltung und den Betrieb der Praxen. Deren Auslegung obliegt allerdings zum großen Teil den Standesorganisationen. Zur Erreichung des mit der Initiative verfolgten Anliegens war es deshalb unerlässlich, auch die Hersteller von Praxisverwaltungssystemen sowie die Heilberufskammern einzubinden. Nur in einem Zusammenspiel aller beteiligten Personen, Institutionen und Stellen können auf diesem Feld Fortschritte erzielt werden.

Fazit und Ausblick
Welche Erkenntnisse können schon jetzt aus der rheinland-pfälzischen Initiative gezogen werden? Es ist sicherlich beschwerlich, im Umfeld ärztlicher Tätigkeiten breites Interesse für Fragen des Datenschutzes zu wecken. Und es gelingt sicherlich nicht von heute auf morgen, alle in diesem Zusammenhang bestehenden Defizite flächendeckend zu beheben. Entscheidend ist jedoch, die an der ambulanten Heilbehandlung beteiligten Akteure gerade in Zeiten des Web 2.0 von der Notwendigkeit zu treffender Schutzvorkehrungen bei dem Einsatz moderner Informations- und Kommunikationstechnologie zu überzeugen. Dabei gilt es zu verdeutlichen, dass im Rahmen der Behandlung zustehende Patientenrechte nicht als generelles Misstrauen gegen das ärztliche Tun zu verstehen sind, sondern Ausdruck des unserer Gesellschaft zugrunde liegenden Rechtsstaates und der ihm angehörenden mündigen Bürgerinnen und Bürger. Gelingen diese Einsichten, werden sich auch die mit der Initiative beabsichtigten Verbesserungen im Praxisbetrieb umsetzen lassen. Die vom LfDI und der Kassenärztlichen Vereinigung Rheinland-Pfalz getragene Kooperation möchte hierzu einen Beitrag liefern.

5.3 Änderung des Heilberufsgesetzes, insbesondere Errichtung der Landespflegekammer

Im Berichtszeitraum wurde das Heilberufsgesetz grundlegend novelliert. Der LfDI konnte dabei eine Reihe bedeutsamer datenschutzrechtlicher Verbesserungen erreichen. Zugleich führte die in diesem Zusammenhang gesetzlich neu geschaffene Landespflegekammer im Vorfeld zu einer intensiven Beratung der Landesregierung sowie nach Inkrafttreten zu einem erhöhten Aufkommen von Eingaben.

5.3.1 Handlungspflicht der Heilberufskammern

Ein besonders Anliegen des LfDI war die gesetzliche Verankerung einer klaren Handlungspflicht der Heilberufskammern bei der Beseitigung berufsrechtswidriger Zustände. Konkret geht es um die Frage, welche Stellen Maßnahmen ergreifen müssen, wenn z.B. Arztpraxen aufgegeben und die dazu gehörenden Räume verlassen werden, ohne dass die Inhaberinnen und Inhaber zuvor die Patientenakten einer

sicheren und mit dem Berufsrecht in Einklang zu bringenden Verwahrung zugeführt hatten. In den dem LfDI vorliegenden Sachverhalten bestand jeweils akuter Handlungsbedarf, da die ärztlichen Unterlagen z.B. in gemieteten Räumen lagerten und die Gefahr bestand, dass die Vermieterinnen und Vermieter oder andere Personen sie unbefugt einsahen.

In der Vergangenheit hatten sich die betroffenen Heilberufskammern trotz der aus der Sicht des LfDI bereits vor der jetzigen Novellierung eindeutigen Rechtslage gegen eine ihnen zukommende Letztverantwortung gewehrt. Mit der nun in § 22 Abs. 2 Satz 2 HeilBG getroffenen Regelung, wonach die Kammern verpflichtet sind, Unterlagen im Rahmen der Verwaltungsvollstreckung zu verwahren und zu verwalten, soweit ein Kammermitglied seiner entsprechenden berufsrechtlichen Verpflichtung nicht nachkommt, sollten aber endgültig alle Unklarheiten beseitigt sein. Werden im Zusammenhang mit der Aufgabe einer Behandlungspraxis oder dem Tod einer Praxisinhaberin oder eines Praxisinhabers Umstände bekannt, die befürchten lassen, dass Patientendaten in unbefugte Hände geraten könnten, ist es Aufgabe der zuständigen Heilberufskammer, sofort tätig zu werden und geeignete Maßnahmen selbst zu ergreifen oder zu veranlassen, die die Praxisakten sichern und einer geordneten Verwahrung zuführen.

Aus Sicht des LfDI gilt die Handlungspflicht der Kammern auch dann, wenn Patientinnen und Patienten aufgegebener Praxen oder verstorbener Behandlerinnen und Behandler deren Rechtsnachfolger bzw. Erben erfolglos um die Bereitstellung der sie betreffenden Dokumentationen bitten. Wird beispielsweise die Herausgabe von Kopien der Behandlungsunterlagen an die Patientinnen und Patienten verweigert und ist dies der zuständigen Kammer bekannt, hat diese unverzüglich für einen ungehinderten Zugang der Betroffenen zu den ärztlichen Aufzeichnungen zu sorgen und die hierzu erforderliche Schritte einzuleiten. Die Landesregierung teilt auch insoweit die Rechtsauffassung des LfDI.

5.3.2 Berücksichtigung des Datenschutzes bei der Ausgestaltung des Berufsrechts

Aufgrund verschiedener im Laufe seiner Beratungstätigkeit festgestellter Regelungsdefizite regte der LfDI eine Präzisierung der im Heilberufsgesetz enthaltenen Vorgaben zur Ausgestaltung des Berufsrechts an. Konkret betraf dies die Aufbewahrung und Weitergabe der Behandlungsdokumentationen, die Sicherstellung der den Betroffenen zustehenden Auskunftsrechte sowie die Zulässigkeit einer Einbindung externer IT-Dienstleister. Die in § 24 Abs. 1 Nr. 2 HeilBG nunmehr enthaltenen Formulierungen verpflichten im Ergebnis die rechtsetzenden Heilberufskammern zur Anpassung der Berufsordnungen, sofern nicht bislang schon entsprechende Regelungen vorhanden waren. Dies trifft jedoch zumindest bezüglich der im Berufsalltag regelmäßig vorkommenden Kooperation von Heilberufspraxen mit externen IT-Dienstleistern leider nicht zu. Dennoch haben es die im Lande ansässigen Kammern bislang unterlassen, die Zulässigkeit der Einbindung und die dabei zu erfüllenden Anforderungen in den Berufsordnungen zu regeln. Der LfDI wird die rheinland-pfälzischen Heilberufskammern um Umsetzung der in § 24 Abs. 1 Nr. 2 HeilBG enthaltenen Vorgaben bitten.

5.3.3 Errichtung der Landespflegekammer

Die mit dem Inkrafttreten des novellierten Heilberufsgesetzes verbundene Errichtung der Landespflegekammer Rheinland-Pfalz wurde durch den LfDI von Beginn an begleitet, soweit dabei datenschutzrechtliche Fragestellungen zu klären waren. Eine besondere datenschutzrechtliche Relevanz kam hierbei dem von der Landesregierung beabsichtigten Austausch von Mitarbeiterdaten zwischen dem Gründungsausschuss der Landespflegekammer und den Arbeitgeberinnen und Arbeitgebern von Angehörigen der Pflegeberufe zu.

Der damit verbundene Eingriff in das informationelle Selbstbestimmungsrecht der Berufsangehörigen diente ausweislich der Gesetzesbegründung der Sicherstellung einer „breiten Registrierung“ der nach § 1 Abs. 1 HeilBG gesetzlich bestimmten Mitglieder zur Durchführung der Wahlen zur Vertreterversammlung. Die vorgesehenen Erhebungs- und Übermittlungsbefugnisse sollten insoweit zu einem

zügigen Aufbau der Landespflegekammer beitragen. Zudem sollten die erfassten Daten auch zum Aufbau eines Mitgliederverzeichnisses der Landespflegekammer genutzt werden.

Im Ergebnis erkannte der LfDI in den hierzu vorgesehenen gesetzlichen Regelungen keine Verletzung des Datenschutzes. Denn soweit mit den dargestellten Befugnissen der Aufbau und die Funktionsfähigkeit der Landespflegekammer unterstützt werden sollte, stand dies offenkundig im überwiegenden Allgemeininteresse. Auch die neu errichtete Landespflegekammer musste und muss die ihr zukommenden Aufgaben erfüllen können. Dies setzt eine möglichst zeitnahe und vollzählige Erfassung aller Mitglieder voraus, da nur diese die zur Handlungsfähigkeit der Kammer maßgeblichen Organe bilden können. Die Kammermitgliedschaft wiederum hängt nicht von dem Willen der Berufsangehörigen ab, sondern ist gesetzlich bestimmt. Vor diesem Hintergrund hatte der LfDI keine datenschutzrechtlichen Bedenken gegen die in § 111 Abs. 5 HeilBG enthaltene Regelung von Erhebungs- und Übermittlungsbefugnissen, bei der im Interesse eines schnellen Aufbaus des vollständigen Mitgliederverzeichnisses das individuelle Interesse an informationeller Selbstbestimmung zulässigerweise zurücktreten durfte.

5.4 Die Zukunft rückt näher: Telematik im Gesundheitswesen

Der Einsatz telematischer Anwendungen im Bereich der gesundheitlichen und pflegerischen Versorgung ist das Zukunftsthema schlechthin. Allerorten werden Projekte ins Leben gerufen, bei denen die Anforderungen an eine funktionsfähige, bedarfsgerechte und finanziell tragbare technische Infrastruktur für eine sektorenübergreifende Information und Kommunikation zwischen Behandelnden, Patientinnen und Patienten und sonstigen Einrichtungen ermittelt und zugleich darauf basierende technische Softwarelösungen entwickelt und getestet werden. Die Ursachen für diese Dynamik sind vielfältig: Politisch möchte man z.B. der drohenden medizinischen Unterversorgung im ländlichen Raum durch die Nutzung der mit der digitalen Technik verbundenen Chancen entgegenwirken. Die Kostenträger sehen in dem Einsatz telematischer Anwendungen bei der Gesundheitsversorgung ein hohes Potential zur Effizienz- und Qualitätssteigerung und damit zur Kostenreduzierung. Und viele Software-Unternehmen haben schließlich den Gesundheitsbereich als lukrativen Zukunftsmarkt entdeckt, an dem sie sich gerne beteiligen.

Unter Telematik versteht man die Technik, die die Bereiche Telekommunikation und Informatik verknüpft. Telematik ist also das Mittel der Informationsverknüpfung von mindestens zwei Informationssystemen mit Hilfe eines Telekommunikationssystems sowie einer speziellen Datenverarbeitung. Die Telemedizin ist ein Teilbereich der Telematik im Gesundheitswesen und bezeichnet Diagnostik und Therapie unter Überbrückung einer räumlichen oder auch zeitlichen Distanz zwischen Arzt, Therapeut, Apotheker und Patienten oder zwischen zwei sich konsultierenden Ärzten mittels Telekommunikation.
(Quelle: Wikipedia, Stand: 9. Dezember 2015)

Auch in Rheinland-Pfalz setzt die Landesregierung hohe Erwartungen in die Digitalisierung des Gesundheitsbereichs. In ihrer Antwort auf die Große Anfrage zum Thema „Chancen der Digitalisierung und Netzpolitik in Rheinland-Pfalz nutzen“ (LT-Drs. 16/5348) stellte die Staatskanzlei die Bedeutung des Ausbaus der bundesweiten Telematikinfrastruktur sowie der Nutzung telemedizinischer Anwendungen heraus. Das von der Landesregierung aufgelegte Zukunftsprogramm „Gesundheit und Pflege – 2020“ unterstützt in diesem Zusammenhang diverse im Land angesiedelte Forschungsprojekte, bei denen telemedizinische Strukturen in technischer, organisatorischer und medizinischer Hinsicht entwickelt, erprobt oder ausgebaut werden. Der LfDI wurde frühzeitig in die Projektdurchführung eingebunden (vgl. hierzu 24. Tb., Tz. III-5.2.1).

Aus datenschutzrechtlicher Sicht stehen der Nutzung telemedizinischer Anwendungen im Bereich Gesundheit und Pflege grundsätzlich keine Bedenken entgegen, sofern dabei das informationelle Selbstbestimmungsrecht der Betroffenen angemessen berücksichtigt wird. Bereits im letzten Tätigkeitsbericht hatte sich der LfDI ausführlich dazu geäußert, in welcher Weise dies erreicht werden kann. Danach hat der Gesetzgeber die aus den Vorgaben des Datenschutzes resultierenden Anforderungen an den Einsatz telemedizinischer Verfah-

ren rechtzeitig und umfassend festzulegen. Bislang kam es allerdings weder auf Bundes- noch auf Landesebene zu einer entsprechenden Regelung. Gerade das Ende 2015 vom Bundestag verabschiedete E-Health-Gesetz enttäuschte insoweit die Erwartungen. Zwar schuf der Gesetzentwurf, der vorrangig die elektronische Gesundheitskarte (eGK) nach § 291a SGB V betraf, die rechtlichen und technischen Voraussetzungen zur Nutzung der in diesem Zusammenhang errichteten Telematikinfrastruktur für weitere außerhalb der eGK liegende Anwendungen. Der Gesetzgeber versäumte es jedoch, verbindliche datenschutzrechtliche Standards zu formulieren, die von diesen Anwendungen eingehalten werden müssen.

Der umfassende und effektive Schutz personenbezogener Gesundheits- und Sozialdaten ist ein elementares Anliegen der Datenschutzbeauftragten des Bundes und der Länder. Schon jetzt unterliegt eine Verarbeitung derartiger Daten hohen rechtlichen Hürden. Das bisherige Schutzniveau muss auch bei dem Einsatz telematischer Anwendungen gewahrt bleiben. Für eine flächendeckende Nutzung solcher Technologien in der Regelversorgung bedarf es eines klaren rechtlichen Rahmens zur Sicherstellung des Patienten- und Sozialgeheimnisses. Der LfDI hat zu diesem Zweck erste Eckpunkte formuliert, die bei der Festschreibung der datenschutzrechtlichen Rahmenbedingungen berücksichtigt werden sollten. Hierzu gehört in erster Linie der Aspekt „privacy by design“, d.h. die Wahrung der informationellen Selbstbestimmung sollte durch den Einsatz spezieller datenschutzfreundlicher Technologien so weit wie möglich sichergestellt sein. Damit dies erreicht werden kann, müssen vor allem die Hersteller derartiger technischer Lösungen frühzeitig die Anforderungen kennen, die erfüllt sein müssen. Es kommt somit – wie bereits im letzten Tätigkeitsbericht beschrieben – auf ein rasches Handeln des Gesetzgebers an.

Die 88. Gesundheitsministerkonferenz hat auf ihrer Sitzung am 25. Juni 2015 das Thema Telematik als Schwerpunkt behandelt. Dabei wurde beschlossen bis zur nächsten Sitzung im Frühjahr 2016 eine Strategie zum weiteren Aufbau der Telematikinfrastruktur unter Beteiligung der Länder zu erstellen. U.a. soll geklärt werden, wie die Zusammenarbeit unter den Ländern zu Fragen des Datenschutzes und der Standardisierung verbessert werden kann. Die Datenschutzbeauftragten des Bundes und der Länder haben der Gesundheitsministerkonferenz bzw. der von ihr beauftragten Bund-Länder-Arbeitsgruppe frühzeitig angeboten, die in diesem Zusammenhang maßgeblichen datenschutzrechtlichen Anliegen zu benennen und deren Berücksichtigung in dem Strategiepapier zu begleiten.

Die Landesregierung hat dem LfDI gegenüber ihre Bereitschaft erklärt, sich bei den anstehenden Gesprächen über die bundesweite Strategie des Bundes und der Länder zum weiteren Aufbau der Telematikinfrastruktur nachdrücklich für die Berücksichtigung des Datenschutzes einzusetzen. Unabhängig davon befürwortet der LfDI auch weiterhin eine Festschreibung der bei dem Einsatz telematischer Anwendungen gebotenen datenschutzrechtlichen Standards.

5.5 Einrichtung eines klinisch-epidemiologischen Krebsregisters in Rheinland-Pfalz

Im April 2013 ist das Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister in Kraft getreten. Kern des Gesetzes ist die Einführung und Umsetzung einer flächendeckenden, vollständigen und vollzähligen klinischen Krebsregistrierung in Deutschland durch klinische Krebsregister.

Klinische Krebsregister haben das Ziel, die Behandlung von Krebspatientinnen und -patienten zu verbessern. Hierzu müssen detaillierte Angaben über die Erkrankung und die darauf bezogene Therapie gesammelt werden, die dann zu festgelegten Zwecken ausgewertet werden dürfen. Da die Meldungen an die Krebsregister laufend um Informationen zur Behandlung und Angaben zum Krankheitsverlauf aktualisiert werden müssen, benötigen die Krebsregister zudem personenidentifizierende Angaben über die betroffenen Patientinnen und Patienten. Ansatzpunkte für eine Verbesserung der Krebsbehandlung können z.B. Vergleiche konkreter Therapieansätze oder verschiedener Behandelnder sein. Auch die Bereitstellung aktueller therapeutischer Informationen für sämtliche an einer Behandlung beteiligten Einrichtungen kann zur Optimierung beitragen. Die Qualität der Krebsregister hängt nach Aussage der Fachleute entscheidend von der Meldequote ab. Um gute Ergebnisse erreichen zu können, sei zumindest für klinische Krebsregister eine voll-

zählige, vollständige und andauernde Meldung aller Neuerkrankungen, der durchgeführten Therapien und des weiteren Krankheitsverlaufs entscheidend.

Die Aufgaben der bundesweit einzurichtenden klinischen Krebsregister sind in § 65c SGB V statuiert. Danach werden patientenbezogene Informationen zum Auftreten, zur Behandlung und zum Verlauf bösartiger Neubildungen sowie zu Rückfällen kontinuierlich erfasst und strukturiert ausgewertet. Registrierung und Dokumentation erfolgen auf der Basis eines bundesweit einheitlich festgelegten Datensatzes. Auswertungen haben jährlich landesbezogen zu erfolgen. Auswertungsergebnisse werden auch den Leistungserbringern zur Verfügung gestellt. Nach dem Willen des Gesetzgebers sollen die klinischen Krebsregister zudem die interdisziplinäre, direkt patientenbezogene Zusammenarbeit bei der Krebsbehandlung fördern, die Aufgaben der Versorgungsforschung und der epidemiologischen Krebsregistrierung unterstützen, die Kooperation mit den Zentren für die Onkologie ermöglichen sowie zur Herstellung der Versorgungstransparenz beitragen.

Der Bundesgesetzgeber hat es den Ländern überlassen, die für die Einrichtung und den Betrieb der Register notwendigen Bestimmungen einschließlich der datenschutzrechtlichen Regelungen in eigener Zuständigkeit zu treffen. Rheinland-Pfalz war eines der Länder, die recht frühzeitig die Umsetzung der Vorgaben aus § 65c SGB V angingen. Das bereits im Land bestehende epidemiologische Krebsregister sollte nach Vorstellung der Landesregierung um die Aufgaben eines klinischen Registers erweitert werden. Angesichts der hohen datenschutzrechtlichen Relevanz eines derartigen klinisch-epidemiologischen Krebsregisters wurde der LfDI von Beginn an in die fachlichen Planungen des federführenden Ressorts und das sich anschließende Gesetzgebungsverfahren eingebunden. Dies führte im Ergebnis erfreulicherweise zu einer weitgehenden Beachtung datenschutzrechtlicher Belange.

- Organisatorisch werden die Aufgaben des klinisch-epidemiologischen Krebsregisters im Lande künftig von einer gemeinnützigen Gesellschaft mit beschränkter Haftung wahrgenommen, die insoweit als Beliehene agiert. Die damit gefundene Lösung, den Betrieb des Krebsregisters auch weiterhin im öffentlichen Bereich zu belassen, entspricht auch der Empfehlung des LfDI, die Datenverarbeitung in besonders sensiblen Sachbereichen im Zweifel vorrangig öffentlichen Stellen zu übertragen (vgl. auch die gesetzliche Wertung in § 4 Abs. 4 Satz 2 LDSG).
- Die im bisherigen epidemiologischen Krebsregister erfolgte Aufteilung in einen Vertrauensbereich und einen Registerbereich wird auch künftig beibehalten. Allerdings fällt die strikte räumliche Trennung der beiden Bereiche trotz der deutlich umfangreicheren Datenverarbeitung aus arbeitsökonomischen Gründen in Zukunft weg. Die Bereiche werden nicht mehr in zwei getrennten Gebäuden, sondern in einer baulichen Einheit angesiedelt werden. Aus datenschutzrechtlicher Sicht ist dies zwar zu bedauern, da damit die gebotene Abschottung der beiden Bereiche nach außen nicht mehr erkennbar bleibt. Angesichts der nun in § 2 Abs. 3 Satz 4 LKRG aufgenommenen klaren gesetzlichen Vorgabe, die Datenbestände des Vertrauensbereichs und des Registerbereichs durch „besondere technische und organisatorische Maßnahmen“ voneinander zu trennen und vor unbefugter Verarbeitung zu schützen, hat der LfDI aber die Unterbringung der Bereiche in einem Gebäude hingenommen.
- Anders als bei den meisten anderen Aspekten im Gesetzgebungsverfahren konnte der LfDI die nun in das Gesetz aufgenommene Gestaltung des Widerspruchsrechts der Patientinnen und Patienten leider nicht beeinflussen. Nach dem Willen des Gesetzgebers wird den betroffenen Krebspatientinnen und –patienten lediglich das Recht eingeräumt, der dauerhaften Speicherung ihrer Identitätsdaten im Krebsregister zu widersprechen. Eine patientenbezogene Übermittlung ihrer Krankheitsdaten an das Krebsregister können sie durch den Widerspruch dagegen nicht verhindern. Ein eingelegter Widerspruch hat vielmehr lediglich zur Folge, dass die Identitätsdaten nach der Bildung einer Kontrollnummer für die Krankheits- bzw. Behandlungsdaten im Vertrauensbereich des Registers gelöscht werden. Eine Zuordnung der im Registerbereich vorhandenen Informationen zu einzelnen Patientinnen oder Patienten ist danach nicht mehr möglich. Diese nach den bisherigen datenschutzrechtlichen Erfahrungen zumindest ungewöhnliche Ausgestaltung eines Widerspruchsrechts soll aus Sicht der Landesregierung die Vollzähligkeit der Meldungen und damit

die Funktionsfähigkeit des Krebsregisters sicherstellen. Angesichts der besonderen Situation der von einer Krebserkrankung betroffenen Menschen hätte sich der LfDI erhofft, dass der rheinland-pfälzische Gesetzgeber der Patientenautonomie stärkeres Gewicht eingeräumt hat. Konkrete Anhaltspunkte dafür, dass die Vollzähligkeit der Meldungen an die Register dadurch tatsächlich gefährdet sein könnte, waren nicht ersichtlich.

- Die technischen Anforderungen an die neuen Übermittlungswege zwischen den verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern wurden von der Datenschutzkonferenz in einer Entschließung vom 14. November 2014 „Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern“ ausführlich beschrieben (vgl. http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=088-089_krebsreg). Angesichts der besonderen Schutzbedürftigkeit der in den Registern gespeicherten Informationen bedarf es geeigneter Schutzmaßnahmen, um sowohl Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme sicherzustellen. Der LfDI wird zusammen mit dem im Aufbau befindlichen rheinland-pfälzischen klinisch-epidemiologischen Krebsregister die Umsetzung dieser Anforderungen konstruktiv begleiten.

5.6 Fernwartung im Krankenhaus

Informationstechnik ist im Krankenhaus zu einem unverzichtbaren Hilfsmittel ärztlicher Behandlung geworden. Labor-, Diagnose- und Krankenhausinformationssysteme sind die Grundlage für effiziente Behandlungsentscheidungen. Die dabei verarbeiteten Daten sind von hoher Sensibilität und durch das Arztgeheimnis geschützt. Für jegliche Offenbarung bedarf es einer Befugnis in Form einer gesetzlichen Erlaubnis oder der Einwilligung der Patientinnen und Patienten. Bei einer Fernwartung besteht aus Datenschutzsicht das hauptsächliche Risiko, dass Patientendaten unbefugt offenbart oder zur Kenntnis genommen werden oder den geschützten Bereich des Krankenhauses verlassen.

Die Krankenhäuser sind sich der Sensibilität von Patientendaten und der notwendigen Vertraulichkeit durchaus bewusst. Häufig werden IT-Dienstleister jedoch fälschlicherweise als ärztliche Berufsgehilfen eingeordnet. Hier fehlt es dann oft an einer tragfähigen Grundlage für die Offenbarung von Patientendaten; eine Fernwartung ist dann nur eingeschränkt zulässig. Hier wäre eine gesetzliche Regelung, die Wartungsdienstleister an das Arztgeheimnis bindet, wünschenswert. Oftmals entsprechen Wartungsverträge auch nicht den gesetzlichen Anforderungen.

Problematisch ist weiterhin die undifferenzierte Betrachtung von Wartungszugriffen. Eine Unterscheidung zwischen der Wartung im Rahmen des technischen Betriebs ohne Zugriff auf personenbezogene Daten, Arbeiten mit Zugriff auf personenbezogene, jedoch nicht patientenbezogene Daten und Arbeiten, die den Zugriff auf Patientendaten erfordern, erfolgt meist nicht. Bei der Gestaltung von Fernwartungsverträgen sind folgende Punkte zu beachten

- Zunächst müssen die gesetzlichen Anforderungen aus § 11 BDSG abgebildet sein, wie die Festlegung von Sicherheitsmaßnahmen, die Durchführung von Kontrollen oder Regelungen zum Umgang mit den bei einer Wartung betroffenen Daten.
- Anforderungen an Wartungsprozesse sind in der Orientierungshilfe „Krankenhausinformationssysteme“ der Datenschutzbehörden (vgl. Teil 2, Kapitel 8) festgelegt. Hierzu zählt, dass das Krankenhaus sicherstellt, dass Wartungszugriffe nur mit Einverständnis des Krankenhauses und nach einem Benachrichtigungs- bzw. Freischaltverfahren erfolgen können. Fernwartungsarbeiten müssen weiterhin über verschlüsselte Verbindungen durchgeführt werden.
- Schließlich müssen Zeitpunkt, Dauer, Art des Zugriffs und jeweiliger Benutzerinnen und Benutzer protokolliert werden. Anforderungen an die Auswertung der Protokolle und die Dauer der Speicherung beschreibt die Orientierungshilfe in Teil 2, Kapitel 7.

Orientierungshilfe „Krankenhausinformationssysteme“ der unabhängigen Datenschutzbehörden des Bundes und der Länder
http://www.datenschutz.rlp.de/downloads/oh/dsb_info_kis.pdf

6. Soziales

6.1 Datenschutz bei gesetzlichen Krankenversicherungen

Die Datenverarbeitung im Bereich der gesetzlichen Krankenversicherungen gehörte auch im vergangenen Berichtszeitraum zu einem Schwerpunkt der Beratungstätigkeit des LfDI. Abgesehen von zahlreichen Eingaben, die die Geschäftsstelle des LfDI regelmäßig erreichen, ist dies vor allem der regen Tätigkeit des Gesetzgebers und des Einfallsreichtums der Krankenkassen geschuldet.

6.1.1 Schulquiz und Mitgliederwerbung

Durch eine Eingabe wurde der LfDI auf das Schulquiz einer gesetzlichen Krankenkasse aufmerksam, das im September 2013 bei achten, neunten und zehnten Klassen allgemeinbildender Schulen in Rheinland-Pfalz durchgeführt wurde. Eine Teilnahme an dem Quiz war nur im Rahmen des Klassenverbandes und nach vorheriger Anmeldung bei der Krankenkasse möglich. Im Vorfeld wurden deshalb alle Klassenleitungen schriftlich über das Schulquiz informiert und zur Abgabe einer Anmeldung aufgefordert. In dem Anschreiben wurde als Zielsetzung des Quiz ausschließlich die Sensibilisierung der Schülerinnen und Schüler für wichtige Gesundheitsthemen benannt. Zudem wurden die pro Region ausgelobten Geld- und Sachpreise beschrieben. Aus dem Schreiben war nicht ersichtlich, dass Kundenberaterinnen und -berater der Krankenkasse das Quiz durchführen.

Die Durchführung des Quiz in den Schulen folgte einem vorbereiteten Schema: Jede Schülerin und jeder Schüler einer teilnehmenden Klasse erhielt Fragebögen mit Sachfragen zu den Bereichen Bewegung, Ernährung und Gesundheit und ein vorgefertigtes Antwortblatt, das neben dem Namen auch Erreichbarkeitsangaben der Schülerinnen und Schüler abfragte. Zur Gewinnbenachrichtigung war es nach dem auf dem Vordruck enthaltenen Hinweis zwingend, die Kontaktdaten anzugeben. Unter der Überschrift „Datenverwendung“ enthielt das Blatt zudem eine kleingedruckte Erklärung, die sinngemäß eine weitere Verarbeitung der mit dem Schulquiz erhobenen Teilnehmerdaten durch die Krankenkasse zu Informations- und Beratungszwecken zuließ. Das Schulquiz wurde im Internet durch einen eigenen Online-Auftritt begleitet, in dem u.a. auch Informationen zum Datenschutz und der beabsichtigten Nutzung der Teilnehmerdaten durch die Krankenkasse zu Werbezwecken bereitgehalten wurden. Auf die Internetseite wurde weder in dem Anschreiben zur Ankündigung des Gewinnspiels noch in dem Antwortblatt hingewiesen.

Die Teilnehmerdaten wurden von der Krankenkasse, sofern die Betroffenen 15 Jahre und älter waren, unter dem Merkmal „Interessent“ automatisiert gespeichert. Auf der Basis dieser Angaben sollten den Schülerinnen und Schülern einige Monate vor deren erwartetem Schulabschluss konkrete Hilfs- oder Beratungsangebote gemacht werden. Zumindest teilweise gab die Krankenkasse die Daten an ein von ihr beauftragtes Callcenter weiter, das bei den betroffenen Schülerinnen und Schülern das Interesse an einem Bewerbertraining abfragte.

Aus Sicht des LfDI waren weder die mit dem Schulquiz verbundene Erhebung der Schülerangaben noch deren weitere Verarbeitung durch die Krankenkasse von den zugrunde zu legenden datenschutzrechtlichen Vorgaben gedeckt.

Die Erhebung konnte insbesondere nicht auf die Regelungen der § 284 Abs. 4 Satz 5 SGB V; § 67a Abs. 1 SGB X gestützt werden, da die Kenntnis der Teilnehmerdaten nicht zur Aufgabenerfüllung der Krankenkasse erforderlich war. Im konkreten Fall diente das Schulquiz einerseits der Sensibilisierung der Schülerschaft für wichtige Gesundheitsthemen, andererseits der Eröffnung individueller Hilfs- und Beratungsmöglichkeiten für bislang noch nicht bei der Krankenkasse Versicherte. Für keinen dieser Zwecke war die Kenntnis der Adressangaben der Schülerinnen und Schüler erforderlich. Vielmehr wären die verfolgten Zwecke auch erreicht worden, wenn man im Rahmen eines Besuchs in der Klasse allgemein über die o.g. Themen und Angebote informiert hätte. Die Betroffenen hätten danach selbst entscheiden können, ob sie an einer weiteren individuellen Betreuung durch die Krankenkasse interessiert wären und zu diesem Zweck ihre Identität preisgeben wollen.

Zudem fehlte es an einer wirksamen Einwilligung in das Vorgehen der Krankenkasse. Nach § 67b Abs. 2

SGB X, der über § 284 Abs. 4 Satz 5 SGB V im konkreten Fall heranzuziehen war, ist der Betroffene auf den Zweck der vorgesehenen Erhebung sowie auf die Folgen einer Verweigerung hinzuweisen. Eine Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht und sie im äußeren Erscheinungsbild von gleichzeitig abzugebenden Erklärungen hervorgehoben wird. Diesen Anforderungen wurde jedoch nicht entsprochen: Weder im Vorfeld noch durch die während des Quiz ausgeteilten Unterlagen wurde die Schülerschaft darauf hingewiesen, dass die Erhebung der erbetenen Angaben dem Zweck einer individuellen Kontaktaufnahme durch die Krankenkasse und damit letztendlich der Mitgliedergewinnung diente. Im Gegenteil, es wurde der irreführende Eindruck erweckt, ohne Mitteilung der erbetenen Daten wäre eine Gewinnbenachrichtigung gefährdet.

Auch die weitere Verarbeitung der bereits ohne Rechtsgrundlage erhobenen Schülerdaten war unzulässig. Die Krankenkasse ist der datenschutzrechtlichen Bewertung des LfDI gefolgt und hat sämtliche im Zusammenhang mit dem Schulquiz gewonnenen Teilnehmerdaten umgehend gelöscht. Zugleich sagte die Krankenkasse zu, bei vergleichbaren Vorhaben den LfDI frühzeitig zu beteiligen.

Für künftige Gewinnspiele der Krankenkassen in Schulen ist aus Sicht des LfDI folgende Vorgehensweise zu empfehlen:

1. Abstimmung mit Schulaufsicht
   Sofern ein im Schulbereich vorgesehenes Gewinnspiel der Krankenkassen neben der gesundheitlichen Aufklärung der Adressatinnen und Adressaten auch der Mitgliederwerbung dient, sollte das Vorgehen vorab allgemein mit der zuständigen rheinland-pfälzischen Schulaufsicht abgestimmt werden. Soweit dabei keine grundsätzlichen Bedenken erhoben werden, sollte zumindest geklärt werden, wer schulintern die Beteiligung einzelner Klassen festlegt und inwieweit dies für alle Schülerinnen und Schüler verbindlich sein kann.

2. Informationen zum Vorhaben und der dabei beabsichtigten Datenverarbeitung
   Im Rahmen des Vorhabens sollten alle Beteiligten – also gleichermaßen Lehrerschaft, Erziehungsberechtigte und Schülerschaft – ausführlich und verständlich über die Aktion und die in diesem Zusammenhang beabsichtigte Verarbeitung personenbezogener Daten informiert werden. Dabei sollte sichergestellt sein, dass die Informationen den Adressatenkreis im Vorfeld auch tatsächlich erreichen. Sofern zudem zur Gewinnermittlung ein externer Dienstleister eingebunden sein sollte, wäre auch dies gegenüber den Betroffenen transparent zu machen.

3. Freiwilligkeit der Teilnahme
   Sowohl in dem die Aktion begleitenden Informationsmaterial als auch vor Durchführung der Veranstaltung in der Klasse sollte ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen werden. Denn aufgrund des schulischen Umfeldes kann sehr schnell der Eindruck entstehen, dass im Falle der Beteiligung einer Schulklasse auch alle Schülerinnen und Schüler individuell verpflichtet seien, an dem Gewinnspiel teilzunehmen.

4. Getrennte Erklärungen zur Teilnahme an dem Gewinnspiel und zur Anforderung von Informationen der Krankenkasse
   Aufgrund der unterschiedlichen Zweckbestimmungen sollten die Betroffenen auf voneinander getrennten Texten ihre Teilnahme an dem Gewinnspiel bzw. ihr Interesse an den von der Krankenkasse bereit gestellten Serviceangeboten erklären können.

6.1.2 Neue Beratungsaufgaben der Krankenkasse

Mit dem am 23. Juli 2015 in Kraft getretenen GKV-Versorgungsstärkungsgesetz hat der Gesetzgeber die gesetzlichen Voraussetzungen für eine individuelle Hilfestellung und Beratung arbeitsunfähiger Versicherter durch die Krankenkassen geschaffen. Nach der neu eingefügten Regelung des § 44 Abs. 4 SGB V besteht ein Rechtsanspruch auf Beratung und Unterstützung zu den von der Kasse zur Wiederherstellung der Arbeitsfähigkeit bereit gestellten Leistungen und unterstützenden Angeboten. Voraussetzung ist sowohl eine vorherige schriftliche Unterrichtung über die von der Krankenkasse angebotenen Maßnahmen als auch eine schriftliche Einwilligung der Versicherten in deren Inanspruchnahme. Gleiches gilt auch für die dabei von der Krankenkasse beabsichtigte Datenverarbeitung.

Der LfDI hat sich bereits frühzeitig zu dem bundesweit zwischen den Allgemeinen Ortskrankenkassen abgestimmten und von der AOK Rheinland-Pfalz/Saarland vorgelegten Vordruck geäußert und durchaus datenschutzrechtliches Verbesserungspotential erkannt. So werden die Versicherten in dem Papier zwar über die ihnen zustehenden Beratungs- und Unterstützungsansprüche sowie die möglicherweise hierbei in Betracht kommende Datenverarbeitung aufgeklärt. Allerdings können sie nicht selbst festlegen, ob und in welchem Umfang die Krankenkasse schon im Vorfeld der Beratung Daten über sie von Dritten wie z.B. Ärztinnen und Ärzten oder stationären Einrichtungen erheben darf. Zudem werden die Versicherten in dem Vordruck nicht darauf hingewiesen, was mit den sie betreffenden Daten bei der Krankenlasse passiert, sobald die Aufgaben nach § 44 Abs. 4 SGB V erfüllt sind. Die von der Krankenkasse beabsichtigte Speicherdauer der Daten von sechs Jahren nach Fallabschluss ist nach Einschätzung des LfDI deutlich zu lange. Unterlagen, die nur zum Zwecke der Beratung beigezogen oder von den Versicherten vorgelegt wurden, sollten vielmehr unverzüglich gelöscht oder den Versicherten zurückgegeben werden, sobald sie für die Aufgabenerfüllung der Krankenkasse nicht mehr erforderlich sind.

Die AOK Rheinland-Pfalz/Saarland hat zwar Verständnis für die Anregungen des LfDI geäußert, sah sich aber bislang an einer Überarbeitung des nicht von ihr entwickelten Vordrucks gehindert. Zudem hielt die Krankenkasse die seitens des LfDI vorgeschlagenen Anpassungen teilweise für nicht praktikabel. Der LfDI hofft, trotz der sich abzeichnenden Differenzen doch noch eine datenschutzverträgliche Vorgehensweise vereinbaren zu können.

Im Kreise der Datenschutzbeauftragten des Bundes und der Länder sind die von dem Gesetzgeber den Krankenkassen zugewiesenen Beratungs- und Unterstützungsaufgaben überwiegend kritisch beurteilt worden (vgl. hierzu 25. Tb. der BfDI, Tz. 13.7.1 sowie Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014 „Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!“ http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=088-089_krankengeld). Hauptpunkt der Kritik ist eine drohende Anhäufung medizinischer Angaben über die Versicherten bei den Krankenkassen, die letztendlich zu einer Verwischung der gesetzlich verankerten Aufgabentrennung zwischen ihnen und dem Medizinischen Dienst der Krankenversicherungen führen könne. Der LfDI teilt diese Einschätzungen nur teilweise. Gleichwohl plädierte er im Interesse einer einvernehmlichen datenschutzrechtlichen Begleitung der neuen Beratungsaufgaben durch die Datenschutzbeauftragten des Bundes und der Länder dafür, zu Beginn des Jahres 2016 bundesweit abgestimmte und koordinierte Prüfungen durchzuführen, die klären sollen, ob die im Vorfeld geäußerten Befürchtungen auch tatsächlich eingetreten sind.

Der LfDI konnte sich im Februar 2016 bei einer Krankenkasse ein konkretes Bild von der Wahrnehmung der Beratungsaufgaben im Bereich des Krankengeldfallmanagements machen. Dabei bestätigte sich einerseits die Vermutung, dass in den Akten versichertenbezogene medizinische Unterlagen wie z.B. Arztberichte oder medizinische Gutachten in nennenswertem Umfang vorgehalten werden, ohne dass deren Erforderlichkeit belegt ist. Andererseits waren keine Anhaltspunkte für die zunächst befürchtete Kompetenzüberschreitung der Krankenkasse im Verhältnis zum Medizinischen Dienst der Krankenversicherungen ersichtlich. Vielmehr zeigten die Besuche, dass die Beratungen für die Versicherten ein wichtiges und unverzichtbares Instrument bei der Bewältigung ihrer Arbeitsunfähigkeit und der daraus drohenden sozialversicherungsrechtlichen Folgen sind. Die Ergebnisse der Prüfungen werden zeitnah zusammen mit der Krankenkasse ausgewertet und das weitere Vorgehen abgestimmt.

6.1.3 Auf der Ziellinie: das Verfahren oscare

Schon seit geraumer Zeit begleiten die staatlichen Datenschutzbeauftragten auf Einladung des Bundesverbandes der AOK das vorrangig für die Allgemeinen Ortskrankenkassen entwickelte Datenverarbeitungsverfahren „oscare“. In vielen Feldern führte die enge Zusammenarbeit zwischen der zu diesem Zweck gebildeten Arbeitsgruppe der Datenschutzbeauftragten und dem oscare-Management zu einer datenschutzrechtlichen Optimierung des Verfahrens (vgl. 22. Tb., Tz. 8.4). Ungelöst blieb bislang jedoch die Frage einer Protokollierung lesender Zugriffe.

Nach den mittlerweile vorliegenden Informationen des AOK-Bundesverbandes wird zum Jahresbeginn 2016 die Protokollierung lesender Zugriffe im Verfahren oscare möglich sein. Das hierzu entwickelte Instrument sollte nach Erprobung und Abschluss notwendiger Anpassungsarbeiten allen oscare-Kunden in den von ihnen betriebenen Produktivsystemen spätestens zum Jahresende 2015 bereitgestellt worden sein. Das bislang im Verfahren oscare noch bestehende Protokollierungsdefizit wäre somit herstellerseitig behoben. Es steht nun in der Verantwortung der einzelnen oscare-Betreiber, den Umfang der bei ihrem Einsatz des Verfahrens vorzunehmenden Protokollierung festzulegen.

Damit findet die jahrelange Begleitung der Software-Entwicklung durch die staatlichen Datenschutzbeauftragten ein im Ergebnis positives Ende. Der sicherlich für das ocare-Management zum Teil mühsame und aufwändige Prozess hat sich aus Sicht des Datenschutzes jedoch gelohnt: denn das Verfahren verfügt über die zu einem datenschutzgerechten Betrieb notwendigen Funktionalitäten.

6.1.4 „Wer bin ich?“ – Defizite bei telefonischen Adressänderungen von Krankenversicherten

Am 24. Juni 2015 war in einer bundesweit ausgestrahlten Nachrichtensendung ein Beitrag zu sehen, nach dem bei der elektronischen Gesundheitskarte eklatante Sicherheitslücken vorhanden seien, die sowohl die Ausstellung gefälschter Karten als auch den Zugriff Unbefugter auf Behandlungsdaten von Versicherten ermöglichen würden. Dem Bericht lag die Recherche eines angeblichen IT-Spezialisten bei einer der Aufsicht des LfDI unterliegenden gesetzlichen Krankenkasse zugrunde. Danach hatte er bei der Krankenkasse unter Vorgabe der Identität eines mit ihm kooperierenden Versicherten telefonisch eine Adressänderung mitgeteilt. Tatsächlich handelte es sich bei der von ihm angegebenen Adresse jedoch nicht um die Anschrift des Versicherten, sondern um die der Firma, deren Geschäftsführer der IT-Spezialist war. Zugleich bat er im Namen des Versicherten um Zusendung einer neuen Gesundheitskarte an die geänderte Anschrift. Nach erfolgter Adressänderung und Zusendung der Karte hatte sich der IT-Spezialist im Namen des Versicherten im Online-Portal des Bundesverbandes der betroffenen Krankenkasse registrieren lassen und sich auf diesem Wege Zugang zu dessen elektronischer Patientenquittung verschafft.

Der LfDI nahm sich unmittelbar nach Ausstrahlung der Sendung der Angelegenheit an. Dabei wurde der zugrunde liegende Sachverhalt aufgeklärt und auf möglicherweise vorhandene datenschutzrechtliche Defizite untersucht. Es kam zu folgende Erkenntnissen:

Entgegen der ersten Meldungen im Fernsehbeitrag standen weder die Änderung der Adressdaten noch die unter falscher Identität vorgenommene Registrierung des Online-Zugangs in einem spezifischen Bezug zu dem Instrument der elektronischen Gesundheitskarte. Die Behauptung, dass über die elektronische Gesundheitskarte zum Zeitpunkt der Recherche medizinische Behandlungsdaten der Versicherten abgerufen werden konnten, war unzutreffend. Vielmehr handelte es sich bei den im Fernsehbeitrag gezeigten medizinischen Informationen um die online den Versicherten zur Verfügung gestellte Patientenquittung im Sinne von § 305 SGB V, die keine Funktionalität der elektronischen Gesundheitskarte darstellt. Deren in dem Beitrag präsentierte Verfügbarkeit basierte auf Unzulänglichkeiten im Zusammenhang mit der Änderung von Adressdaten der Versicherten, war aber keinesfalls geeignet, eine Aussage über die Datensicherheit der elektronischen Gesundheitskarte als solche zu treffen.

Verbesserungsbedürftig waren in der Tat die bislang ergriffenen Maßnahmen zur Identifizierung und Authentifizierung eines Versicherten im Falle einer Adressänderung. Denn bei allen denkbaren Formen der Kontaktaufnahme mit der Krankenkasse (per Telefon, E-Mail oder Brief) fehlte es an einem hinreichend verlässlichen Nachweis, dass Anrufende bzw. Absendende auch tatsächlich diejenigen sind, die sie vorgeben zu sein. Auf Anregung des LfDI ergänzte die betroffene Krankenkasse umgehend das Verfahren im Falle einer telefonisch mitgeteilten Adressänderung. Künftig werden die Anrufer gebeten, die auf ihrer Versichertenkarte befindliche Kontrollnummer zu nennen. Damit soll hinreichend verlässlich sichergestellt werden, dass die Anrufenden tatsächlich die zur Adressänderung befugten Versicherten sind. Aus Sicht des LfDI ist die Umstellung

des Verfahrens geeignet, die bislang bestehenden Defizite deutlich zu minimieren. Angesichts der möglicherweise auch bei anderen Krankenkassen vorhandenen Schwachstellen regte der LfDI an, den GKV-Spitzenverband auf die Thematik aufmerksam zu machen.

Im Zusammenhang mit der Registrierung zum Online-Portal der Krankenkasse stellt der LfDI im Ergebnis keine weiteren Defizite bei der Feststellung der Identität und Authentizität der Anmeldenden fest. Allerdings sah der Registrierungsprozess bislang nicht vor, den Einzelfall auf mögliche vorherige Adressänderungen zu überprüfen und sie zumindest dann, wenn diese in zeitlicher Nähe zur Online-Registrierung lagen, separat zu überprüfen. Dies soll sich nach Ankündigung der betroffenen Krankenkasse bzw. des für das Online-Portal verantwortlichen Bundesverbandes jedoch künftig ändern.

6.1.5 Ende des Umschlagverfahrens

Sofern im Zusammenhang mit der Gewährung von Krankenversicherungsleistungen medizinische Zusammenhänge fachlich überprüft werden müssen, ist dies gesetzlich dem Medizinischen Dienst der Krankenversicherung (MDK) vorbehalten. Damit der MDK tätig werden kann, wird er durch eine Krankenkasse ausdrücklich beauftragt (vgl. §§ 275 ff. SGB V). Die zur ärztlichen Begutachtung erforderlichen medizinischen Unterlagen haben die Leistungserbringer dem MDK auf Anforderung zur Verfügung zu stellen.

In der Vergangenheit forderten die Krankenkassen die ärztlichen Einrichtungen auf, die zur Begutachtung durch den MDK im konkreten Fall benötigten Behandlungsunterlagen vorzulegen. Dabei wurde es bislang aus datenschutzrechtlicher Sicht akzeptiert, wenn die Leistungserbringer die Dokumente in einem verschlossenen und ausdrücklich an den MDK adressierten Umschlag der Krankenkasse zusendeten und diese zusicherte, derartige Briefe ungeöffnet den Beschäftigten des MDK zu übergeben. Dieses als „Umschlagverfahren“ bekannte Vorgehen wurde im Jahre 1999 durch den damaligen Landesdatenschutzbeauftragten, Herrn Prof. Dr. Rudolf, mit den von ihm beaufsichtigten Krankenkassen vereinbart.

Das mittlerweile bundesweit etablierte Verfahren stand schon seit einiger Zeit in der Kritik der BfDI (vgl. 20. Tb. der BfDI, Tz. 17.1.5). Nach ihren Erfahrungen öffneten die ihrer Aufsicht unterliegenden Krankenkassen häufig die ausschließlich an den MDK adressierten Umschläge. Dies habe dazu geführt, dass medizinische Unterlagen ohne jegliche rechtliche Befugnis von den Krankenkassen zur Kenntnis genommen werden konnten. Weitere von der BfDI durchgeführte Prüfungen hätten diesen Eindruck bestätigt. Aufgrund dessen kündigte die BfDI im Herbst 2014 an, ab Mitte 2015 das Umschlagverfahren in ihrem Zuständigkeitsbereich nicht mehr zu tolerieren und Zuwiderhandlungen formell zu beanstanden.

In Rheinland-Pfalz lagen bislang keine Anhaltspunkte für eine Verletzung des vereinbarten Verfahrens vor. Insbesondere erhielt der LfDI in der Vergangenheit keine Hinweise des MDK, die auf vergleichbare Defizite, wie sie offenkundig von der BfDI festgestellt wurden, hindeuteten. Es bestand daher zunächst aus datenschutzrechtlicher Sicht in Rheinland-Pfalz kein Anlass, das in der Vergangenheit bewährte Verfahren zu verändern. Dennoch befürwortete der LfDI im Interesse der betroffenen Leistungserbringer ein bundesweit abgestimmtes Vorgehen der Datenschutzbeauftragten.

Aus Sicht des Arbeitskreises Gesundheit und Soziales der Datenschutzkonferenz ist der von der Bundesregierung im Rahmen des Entwurfs eines Krankenhaus-Strukturgesetzes vorgelegte Vorschlag zur Änderung des § 276 Abs. 2 Satz 2 SGB V geeignet, das Anliegen der BfDI aufzugreifen und künftig ausschließlich eine unmittelbare Übersendung der Unterlagen durch die Leistungserbringer an den MDK sicherzustellen. Sollte sich der Gesetzgeber für eine derartige Änderung entscheiden, wäre auch der LfDI bereit, dies zum Anlass zu nehmen und in seinem Zuständigkeitsbereich das Umschlagverfahren zu beenden. Der Gesetzentwurf wurde im November 2015 vom Deutschen Bundestag verabschiedet und ist zu Beginn des Jahres 2016 in Kraft getreten.

6.2 Ein Dauerbrenner: Die Anforderung und Speicherung von Nachweisen bei der Erbringung von Sozialleistungen

Auch nach Jahren datenschutzrechtlicher Begleitung und Aufklärung der im Lande tätigen Sozialverwaltungen gehören Eingaben, die die Anforderung und Speicherung von Nachweisen bei der Erbringung von Sozialleistungen betreffen, immer noch zu einem Dauerbrenner in der Beratungstätigkeit des LfDI. Verantwortlich hierfür ist die gegensätzliche Interessenlage der an der Gewährung von Sozialleistungen beteiligten Leistungsträger und der Antragstellenden. Auf der einen Seite sind die Sozialverwaltungen verpflichtet, nur bei tatsächlich bestehender Hilfebedürftigkeit öffentliche Mittel zu bewilligen. Um dem nachkommen zu können, bedarf es naturgemäß der Vorlage von Nachweisen, aus der die Bedürftigkeit hervorgeht. Auf der anderen Seite schützt das gesetzlich verbriefte Sozialgeheimnis die Hilfesuchenden vor allzu viel behördlicher Neugier.

Dass es in diesem Zusammenhang immer wieder zu nicht vermeidbaren Kollisionen kommt, verwundert nicht. Es liegt auch auf der Hand, dass es vereinzelt zu einer datenschutzrechtlich angreifbaren Abwägung der unterschiedlichen Interessen zulasten der Antragstellenden und damit zu einer Grundrechtsverletzung kommen kann. Überrascht ist der LfDI jedoch von dem Ausmaß der Hartnäckigkeit, den manche Sozialverwaltungen an den Tag legen, wenn es um die Nichtbeachtung klarer datenschutzrechtlicher Vorgaben und der in diesem Zusammenhang ergangenen höchstrichterlichen Rechtsprechung geht. Gerade dort, wo der LfDI bereits in der Vergangenheit den Sozialbehörden klare Schranken für ihre Ermittlungstätigkeit aufgezeigt hatte (vgl. 18. Tb., Tz. 11.6.3; 19. Tb., 11.2; 20. Tb., Tz. 11.1.2; 21. Tb., Tz. 11.1.3 und Tz. 11.6; 22. Tb., Tz. 8.1.1 und 8.1.2), sollte man zu Recht erwarten können, dass sich die behördliche Praxis auch daran orientiert.

Offenkundig handelt es sich hierbei jedoch nicht nur um ein auf Rheinland-Pfalz beschränktes Phänomen. In einer Pressemitteilung des Bayerischen Landesdatenschutzbeauftragten vom 24. November 2015 (https://www.datenschutz-bayern.de/) berichtet dieser von einer bei insgesamt 120 bayerischen Sozialbehörden durchgeführten Datenschutzkontrolle. Sein bitteres Fazit: In zahlreichen Behörden werden Vorgaben des Sozialdatenschutzes missachtet. Nicht vorenthalten werden soll die aus den Prüfungen resultierende Erkenntnis, nach der die Sozialbehörden im Lande bei der Einhaltung datenschutzrechtlicher Vorgaben sehr unterschiedlich vorgehen. Dies entspricht auch den Erfahrungen, die der LfDI in Rheinland-Pfalz macht.

6.2.1 Vorlage und Speicherung von Kontoauszügen

Eine der Aufsichtszuständigkeit des LfDI unterliegende Optionskommune hatte ihn im Berichtszeitraum auf die Entscheidung des Bayerischen Landessozialgerichts vom 21. Mai 2014 (Az. L 7 AS 347/14 B ER) hingewiesen. In diesem Beschluss stellte das Gericht fest, dass die Aufbewahrung der zur Einsicht von dem Leistungsbezieher vorgelegten Kontoauszüge in der Verwaltungsakte eine rechtmäßige Speicherung von Daten nach § 67c SGB X sei. Die Aufbewahrung der Kontoauszüge sei erforderlich, um die Hilfebedürftigkeit des Antragstellers zu überprüfen. Eine kurze Einsichtnahme reiche hierbei nicht aus. Dies gelte unabhängig davon, ob die Kontoauszüge Informationen über anrechenbares Einkommen enhalten oder nicht. Nach Auffassung des Landessozialgerichts stellen Kontoauszüge eine wesentliche Entscheidungsgrundlage für die Gewährung von Leistungen nach dem Sozialgesetzbuch II dar, die auch für mögliche Folgeverfahren aufbewahrt werden müssten. Vor diesem Hintergrund sei eine regelmäßige Aufbewahrungsdauer der Verfahrensakten – und damit auch der Kontoauszüge – von zehn Jahren nach Schließung der Akte bzw. des Vorgangs nicht zu beanstanden. Die Optionskommune sah sich an diese Rechtsprechung gebunden und kündigte an, künftig alle vorgelegten Auszüge zu kopieren und langfristig in der Verfahrensakte vorzuhalten.

Die Entscheidung des Landessozialgerichts Bayern kollidiert mit der bislang vom LfDI in diesem Zusammenhang vertretenen Rechtsauffassung (vgl. 22. Tb., Tz. 8.1.2). Hiernach fehlt es regelmäßig an einer Befugnis zur dauerhaften Speicherung vorgelegter Kontoauszüge, soweit sich aus den Unterlagen keine Abweichungen zu den bisherigen Antragsangaben ergeben. In diesen Fällen sah es der LfDI als ausreichend an, die Vorlage der Nachweise

in der Akte zu vermerken und die eingereichten Auszüge zurückzugeben oder zu vernichten.

An dieser Auffassung hält der LfDI auch nach Würdigung der für die Entscheidung des Landessozialgerichts Bayern maßgeblichen Erwägungen im Wesentlichen fest:

- Die rechtlichen Rahmenbedingungen für eine Anforderung von Kontoauszügen im Zusammenhang mit der Gewährung von Leistungen der Grundsicherung für Arbeitsuchende sind höchstrichterlich mit der Entscheidung des Bundessozialgerichts vom 19. September 2008 (Az. B 14 AS 45/07 R) geklärt. Hiernach stellt die Vorlage von Kontoauszügen sozialrechtlich eine Mitwirkungsobliegenheit der Antragstellenden nach § 60 Abs. 1 Nr. 3 SGB I dar, die zur Feststellung der Hilfebedürftigkeit erforderlich sei. Im Regelfall sei die Anforderung von Kontoauszügen der letzten drei Monate bei Beachtung der von dem Bundessozialgericht benannten Einschränkungen mit den Vorgaben zum Sozialdatenschutz vereinbar.
- Diese höchstrichterliche Rechtsprechung ist auch für die Frage der datenschutzrechtlichen Zulässigkeit der Speicherung vorgelegter Kontoauszüge maßgeblich. In der Regel dürfen solche Auszüge dauerhaft nur dann gespeichert werden, wenn sie leistungsrelevant sind, d.h. wenn die darin enthaltenen Angaben Anhaltspunkte für eine geänderte Bewertung der Hilfebedürftigkeit enthalten oder im Einzelfall die Hilfebedürftigkeit nur im Rahmen umfänglicher und differenzierter Berechnungen festgestellt werden kann. Fehlt den Kontoauszügen dagegen die Leistungsrelevanz, müssen Kopien, die eventuell bei der Vorlage angefertigt wurden, spätestens nach vier Wochen vernichtet werden.

Der Landrat der betroffenen Optionskommune konnte zunächst nicht von dieser Bewertung überzeugt werden, obwohl neben den Datenschutzbeauftragten des Bundes und der meisten Länder auch das rheinland-pfälzische Sozialministerium die Rechtsauffassung des LfDI ausdrücklich teilt.

6.2.2 Anforderung von Sparbüchern durch das Sozialamt

In einem dem LfDI vorliegenden Sachverhalt hatte ein Sozialamt im Zusammenhang mit der Gewährung von Leistungen der Hilfe zur Pflege nach den §§ 61 ff. SGB XII von dem Antragsteller die Vorlage vollständiger Kopien aller Sparbücher der letzten zehn Jahre verlangt. Die Betroffenen wurden ausdrücklich darauf hingewiesen, dass die Anforderung auch die in diesem Zeitraum aufgelösten Sparbücher betreffe. Das Sozialamt hielt dies zumindest im Bereich der Hilfe zur Pflege für erforderlich, da nach den bisherigen Erfahrungen oft noch vor der Beantragung staatlicher Hilfe vorhandenes Vermögen an Dritte wie z.B. nahestehende Angehörige verschenkt werde, ohne dies im Antrag kenntlich zu machen.

Die Argumentation des Sozialamts war aus Sicht des LfDI durchaus nachvollziehbar. Zivilrechtlich besteht bei Verarmung der Schenkenden ein Rückforderungsanspruch gegenüber den Beschenkten, der vor der Gewährung von Sozialleistungen geltend gemacht werden muss. Denn der Anspruch auf Sozialhilfe ist gegenüber dem Rückforderungsanspruch nachrangig. Ob ein derartiger Anspruch besteht, kann nur dann festgestellt werden, wenn der Leistungsträger über Angaben zu früheren Vermögensübertragungen verfügt und dies auch überprüfbar ist. Allerdings hatte der LfDI unter dem Gesichtspunkt der Verhältnismäßigkeit der Datenerhebung datenschutzrechtliche Bedenken gegen den von der Sozialverwaltung festgelegten Zeitraums von zehn Jahren. Dieser stand in deutlichem Widerspruch zu dem vom Bundessozialgericht in der Entscheidung vom 19 September 2008 (vgl. oben) für vertretbar erachteten Vorgehen bei der Vorlage von Kontoauszügen.

Das Sozialamt entwickelte daraufhin ein gestuftes Verfahren, das sowohl mit den leistungsrechtlichen als auch den datenschutzrechtlichen Vorgaben vereinbar ist. Im Ergebnis werden die Antragstellenden zunächst um Vorlage und Nachweis aller Transaktionen auf Sparbüchern, die in einem Zeitraum von drei Jahren vor der Heimaufnahme auf den Namen der Hilfebedürftigen ausgestellt waren, gebeten. Nur bei Auffälligkeiten wird der Sachverhalt weiter aufgeklärt und ggf. auch Nachweise für weiter zurückliegende Zeiträume angefordert. Kommunale Datenschutzbeauftragte können sich über das Datenschutzforum des LfDI hierzu näher informieren.

6.2.3 Einholung sog. Bankvollmachten

Immer wieder fordern Sozialverwaltungen pauschal die Antragstellenden zur Abgabe von sog. Bankvollmachten auf. Dies ist deshalb verwunderlich, weil bereits im Jahre 1995 ein derart undifferenziertes Vorgehen vom Hessischen Verwaltungsgerichtshof als unzulässig abgelehnt wurde (vgl. hierzu 18. Tb., Tz. 11.6.3). Zudem steht den Grundsicherungs- und Sozialhilfeträgern mittlerweile nach § 93 Abs. 8 AO die Befugnis zu, über das Bundeszentralamt für Steuern bestimmte zur Feststellung der Hilfebedürftigkeit von Antragstellenden relevante Kontodateninformationen bei den Kreditinstituten abzurufen. Es ist daher datenschutzrechtlich nicht hinnehmbar, wenn die Sozialverwaltungen vor dem Hintergrund der ihnen gesetzlich zugewiesenen Ermittlungsmöglichkeiten rein vorsorglich alle Antragstellenden routinemäßig zur Erteilung von Bankauskunftsermächtigungen auffordern.

Der LfDI wird sich vor dem Hintergrund der bisherigen Erfahrungen verstärkt an die Sozialverwaltungen im Lande wenden und mit ihnen gemeinsam nach Lösungswegen suchen, damit die vorhandenen unterschiedlichen Interessenlagen bei der Gewährung von Sozialleistungen nicht nur rechtstheoretisch, sondern auch in der behördlichen Praxis bestmöglich miteinander vereinbart werden können. Die Kommunalverwaltungen sind dazu aufgerufen, mit den bei ihnen vorhandenen Kompetenzen praktikable und rechtskonforme Verfahrensweisen zu entwickeln.

6.3 Bericht der Landesregierung zur Umsetzung des Landeskinderschutzgesetzes

Das 2008 in Kraft getretene Landesgesetz zum Schutz von Kindeswohl und Kindergesundheit sieht eine regelmäßige Berichterstattung der Landesregierung zur Umsetzung, zu den Auswirkungen sowie zum Weiterentwicklungsbedarf der in diesem Gesetz enthaltenen Maßnahmen gegenüber dem rheinland-pfälzischen Landtag vor (vgl. 23. Tb., Tz. II-5.1.1). Nach dem ersten Bericht im Jahre 2011 hat die Landesregierung Anfang 2015 zum zweiten Mal in diesem Zusammenhang Stellung genommen. Der LfDI wurde entsprechend der gesetzlichen Vorgaben beteiligt.

Hintergrund
Das in dem Gesetz verankerte aufwändige Einladungs- und Erinnerungsverfahren zu den Früherkennungsuntersuchungen für Kinder wurde 2009 durch den rheinland-pfälzischen Verfassungsgerichtshof überprüft. Hierbei standen insbesondere die gesetzlich vorgesehenen umfassenden Datenaustausche zwischen Kinderärztinnen und -ärzten, Einladungsstelle sowie Gesundheits- und Jugendämtern im Fokus. Im Ergebnis stellte das Gericht in seiner Entscheidung vom 28. Mai 2009 (Az. VGH B 45/08) die verfassungsrechtliche Vereinbarkeit der überprüften Datenverarbeitungen unter den Vorbehalt des Ergebnisses der von der Landesregierung vorzunehmenden Evaluation des Gesetzes. Ausdrücklich wurden die gegenüber dem Verfassungsgerichtshof von allen Beteiligten eingeräumten nicht unerheblichen Defizite im Gesetzesvollzug – gemeint war die hohe Zahl sog. falsch-positiver Fälle – in der Entscheidung nur übergangsweise hingenommen, soweit sie als Anlaufschwierigkeiten bei der Einführung eines mehrstufigen Verfahrens auftreten. Bei den falsch-positiven Fällen werden die Gesundheits- bzw. Jugendämter über Kinder und deren Sorgeberechtigte unterrichtet, die angeblich nicht an den anstehenden Früherkennungsuntersuchungen teilgenommen haben, obwohl tatsächlich eine Untersuchung stattgefunden hatte.

Dem Anfang 2015 dem Landtag gegenüber vorgelegten Bericht der Landesregierung ist die Stellungnahme des LfDI unkommentiert als Anlage beigefügt. Im Fokus der Äußerungen des LfDI stand weiterhin die sehr hohe Zahl falsch-positiver Fälle. Ausweislich der in dem Bericht enthaltenen statistischen Auswertungen betrug deren Anteil selbst im Jahre 2013 noch über 51 Prozent. Dies bedeutet, dass selbst fünf Jahre nach Inkrafttreten des Gesetzes noch in mehr als der Hälfte der als auffällig angesehenen Fälle die betroffenen Kinder entgegen der behördlichen Vermutung sehr wohl kinderärztlich untersucht wurden. Die Einschaltung der Gesundheitsämter war daher in diesen Fällen weder zum Schutz der Kindergesundheit noch zur Stärkung des Kindeswohls erforderlich. Datenschutzrechtlich wirft das die Frage auf, ob ein derartiges Verfahren, das dauerhaft zu Eingriffen in das informationelle Selbstbestimmungsrecht führt, die zur Erreichung des Gesetzeszwecks gar nicht erforderlich sind, akzeptiert werden kann. Der Verfassungsgerichtshof hat dies in seiner Entscheidung aus dem Jahre 2009

zumindest in Zweifel gezogen (vgl. auch 23. Tb., Tz. II-5.1.1). Der LfDI hat deshalb die Landesregierung aufgefordert, die verfassungsrechtliche Vereinbarkeit des Verfahrens darzulegen. Dies ist bislang bedauerlicherweise nicht geschehen.

Zugleich bat der LfDI die Landesregierung, den Ursachen der falsch-positiven Meldungen künftig entschlossener entgegenzuwirken. Auf der Basis einer aussagekräftigen empirischen Analyse sollten die bislang auf regionaler Ebene mit unterschiedlichem Erfolg ergriffenen Maßnahmen zur Verbesserung der Qualität der Meldungen ausgewertet werden. Auch der Austausch mit den Ländern, bei denen vergleichbare Defizite auftreten, sollte intensiviert werden.

Schon jetzt ist aber erkennbar, dass einer der Hauptgründe für das Auftreten falsch-positiver Fälle im Bereich der ärztlichen Behandlerinnen und Behandler liegt. Teilweise versäumen sie, Untersuchungsbestätigungen an die Zentrale Stelle zu übermitteln, teilweise unterlassen sie derartige Meldungen ganz bewusst. Der LfDI bat aus diesem Grund die Landesregierung ausdrücklich, zeitnah geeignete Vorschläge zur deutlichen Verbesserung des Meldeverhaltens der Ärztinnen und Ärzte vorzulegen und Verstöße gegen die Meldepflicht zu sanktionieren. Auch hier steht eine Rückmeldung der Landesregierung aus.

Im Übrigen begrüßte der LfDI in seiner Stellungnahme die im Berichtszeitraum eingetretenen Korrekturen des Landeskinderschutzgesetzes. Hierzu gehören die Reduzierung des der Zentralen Stelle von den Meldebehörden zu übermittelnden Meldedatensatzes sowie die den Gesundheitsämtern zugestandene eigene Entscheidungs- und Übermittlungsbefugnis über die Einschaltung der Jugendämter, falls eine oder mehrere Früherkennungsuntersuchungen nicht wahrgenommen wurden. Leider traten diese Gesetzesänderungen erst im November 2014 in Kraft, obwohl ein insoweit bestehender Handlungsbedarf seitens der Landesregierung bereits in ihrem ersten Bericht gegenüber dem Landtag im Jahre 2011 erkannt wurde (vgl. 23. Tb., Tz. II-5.1.1).

Der LfDI wird auch künftig das von der Landesregierung verfolgte Ziel, Kinder und Jugendliche in ihrer gesundheitlichen und geistigen Entwicklung besonders zu fördern, umfassend unterstützen. Allerdings muss auch hierbei der verfassungsrechtliche Rahmen staatlicher Maßnahmen gewahrt bleiben. Es ist dauerhaft nicht hinzunehmen, wenn trotz eindeutiger Vorgaben des Verfassungsgerichtshofs das Einladungs- und Erinnerungsverfahren weiterhin in mehr als der Hälfte der aufgegriffenen Fälle die Weitergabe personenbezogener Daten zulässt, obwohl dies zur Erreichung des Gesetzeszwecks tatsächlich nicht erforderlich ist.

6.4 Protokollierung im VdK-Verfahren ARV Viva WEB

Im Zusammenhang mit anstehenden Vorstandswahlen beim Sozialverband VdK Rheinland-Pfalz e.V. wurde anonym eine CD mit internen Daten in Umlauf gebracht.

Im Rahmen der Untersuchungen zur unbefugten Datenweitergabe beim Sozialverband VdK Rheinland-Pfalz e.V. durch den LfDI hat sich gezeigt, dass die vorhandene Protokollierung im Verfahren zur Mitgliederverwaltung „ARV VivaWeb“ ungeeignet ist, unbefugte Datenzugriffe aufzuklären. Aus den Protokolldaten waren lediglich Zeitpunkt, Benutzerkennung einer An- bzw. Abmeldung am Verfahren sowie fehlgeschlagene Anmeldeversuche erkennbar. Die Protokolldaten ließen hingegen nicht erkennen, welche Nutzerinnen und Nutzer auf welche Dokumente Zugriff genommen haben bzw. welche Funktionsaufrufe erfolgten.

Aus der Auswertung der Datenzugriffe durch den LfDI ließen sich damit zwar Indizien, jedoch keine belastbaren Hinweise auf die Urheberin oder den Urheber der Daten-CD gewinnen.

Der LfDI hat das Ergebnis der Protokollauswertung an den Sozialverband VdK Rheinland-Pfalz e.V. weitergegeben, damit dieser seine eigenen Aufklärungsbemühungen fortsetzen konnte. Des Weiteren wurden die Erkenntnisse zur Prüfung, ob eine Wiederaufnahme des seinerzeitigen Ermittlungsverfahrens geboten ist, an die Staatsanwaltschaft Mainz abgegeben.

Der Zweck einer Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener

Daten insoweit transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Aufgrund der aus Sicht des LfDI bestehenden Defizite bei der Protokollierung wurden dem Sozialverband VdK Rheinland-Pfalz e.V. folgende Verbesserungen empfohlen:

6.4.1 Protokollierung schreibender und lesender Zugriffe

Eine datenschutzkonforme Protokollierung erfordert die Erfassung sowohl schreibender als auch lesender Zugriffe.

Nach Nr. 5 der Anlage zu § 9 BDSG ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten eingegeben, verändert oder entfernt worden sind. Dies erfordert die Erfassung folgender Angaben:

- Benutzerkennung
- Zeitpunkt der Dateneingabe/-änderung
- Kennung des betroffenen Datensatzes/ Datenfeldes
- Transaktionskennung (Dateneingabe/Datenänderung/Datenlöschung)

Die Löschung von Daten sollte lediglich insoweit erfasst werden, als für einzelne Datenfelder der Zeitpunkt der Löschung und der jeweilige Benutzer, für Datensätze die jeweilige Fallnummer oder vergleichbare Identifikationsmerkmale festgehalten werden.

Nach Nr. 3 der Anlage zu § 9 BDSG ist zu gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen oder kopiert werden können. In diesem Zusammenhang sowie auch mit Blick auf die vergleichbare Anforderung aus Nr. 4 der Anlage ist als vorbeugende Maßnahme eine Protokollierung lesender Zugriffe mit folgenden Angaben erforderlich.

- Zeitpunkt eines Zugriffs,
- Kennung der jeweiligen Benutzerinnen oder Benutzer, ggf. Kennung der jeweiligen Arbeitsstation,
- aufgerufene Transaktion (Anzeige-/Abfragefunktion, Reportname, Maskenbezeichnung),
- verwendete Such- bzw. Abfragekriterien (z.B. Mitgliedsnummer, Name, Geburtsdatum, Wohnort, Fallnummer etc.),
- Ergebnis der Abfrage (z.B. Zahl der Trefferfälle, Fallnummern, Kennung der angezeigten Bildschirmmaske),
- etwaige Folgeaktionen bzw. Navigationsschritte (z.B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport).

Im Gegensatz zur Protokollierung schreibender Zugriffe, bei der in der Regel der Zustand vor und nach der jeweiligen Änderung erfasst wird, ist bei lesenden Zugriffen die Speicherung des Inhalts der betroffenen Datensätze entbehrlich. Dies gilt insbesondere dann, wenn bei Bedarf der Inhalt eines Datensatzes zum Zeitpunkt des Zugriffs über eine vorhandene Protokollierung der Datenspeicherung und -änderung festgestellt werden kann.

6.4.2 Vollständigkeit der Protokollierung

Die Nutzung der Protokolldaten für Revisions- und Beweiszwecke erfordert, dass sie vollständig sind. Eine lediglich stichprobenweise Protokollierung entspricht dem nicht. Die Protokolldaten dürfen weiterhin nicht nachträglich verändert werden können und dürfen nur den zur Nutzung Berechtigten zugänglich sein.

6.4.3 Auswertbarkeit der Protokolldaten

Es müssen geeignete Mechanismen zur Verfügung stehen, um die Protokolldaten nach Benutzerkennungen, Arbeitsstationen, Funktionen/Transaktionen, Versichertennummern/Fallnummern, Zeiträumen oder Suchkriterien auswerten zu können (s.o.). Struktur und Format der Protokolldaten müssen es ermöglichen, bei Bedarf auch flexible Auswertungen vorzunehmen. Die Protokolldaten müssen daher in einem durch gängige Analysewerkzeuge oder Datenbankfunktionen auswertbaren Format vorliegen bzw. in ein solches überführt werden können (z.B.

CSV-Format mit geeigneten Trennzeichen, je Protokolleintrag eine Zeile).

6.4.4 Aufbewahrungsdauer

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist die Erforderlichkeit zur Aufgabenerfüllung einschließlich der Erfordernisse einer ordnungsgemäßen Dokumentation. Als Anhaltspunkte dienen die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und die Notwendigkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle aufklären zu können. Im Allgemeinen ist danach eine Aufbewahrungsdauer von zwölf Monaten ausreichend.

6.4.5 Zweckbindung

Protokolldaten unterliegen einer strikten Zweckbindung nach § 31 BDSG. Sie dürfen nicht für eine allgemeine Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z. B. zur Strafverfolgung, zu.

Orientierungshilfe „Protokollierung“ der unabhängigen Datenschutzbehörden des Bundes und der Länder

http://www.datenschutz.rlp.de/downloads/oh/ak_oh_protokollierung.pdf

7. Schuldatenschutz und Wissenschaft

7.1 Schuldatenschutz

7.1.1 Veröffentlichung von Fotos auf der Homepage von Schulen oder Kindertagesstätten

Immer wieder fragen Kindertagesstätten oder Schulen beim LfDI an, ob und unter welchen Voraussetzungen Fotos oder Videos von Kindern, Lehrkräften oder Erzieherinnen und Erziehern auf der eigenen Homepage veröffentlicht werden dürfen. Bei der Beantwortung dieser Frage sind neben spezialgesetzlichen Regelungen insbesondere die Bestimmungen des Kunsturhebergesetzes zu beachten. Hiernach ist die Veröffentlichung von Fotos grundsätzlich nur mit Einwilligung der abgebildeten Personen zulässig. Bei Minderjährigen kommt es insoweit auf die Einwilligungsfähigkeit an. Die Einwilligungsfähigkeit im datenschutzrechtlichen Sinne ist nicht abhängig vom Erreichen der Volljährigkeit. Die Schülerinnen und Schüler sind vielmehr dann einwilligungsfähig, wenn sie die Bedeutung und Tragweite der Einwilligung und ihrer rechtlichen Folgen erfassen können und ihren Willen hiernach zu bestimmen vermögen. Einer Einwilligung bedarf es nicht, wenn es sich um eine Veranstaltung der Kindertagesstätte oder Schule handelt, bei der die Dokumentation des Ereignisses und nicht die abgebildeten Personen im Vordergrund stehen. Das Einwilligungserfordernis gilt auch für Gruppen- oder Klassenfotos, wenn die abgebildeten Personen als solche erkennbar sind und den zentralen Bestandteil des Fotos darstellen. Die häufig vertretene Auffassung, wonach bei Gruppenbildern ein Einwilligungserfordernis nicht bestünde, findet im Gesetz keine Stütze.

Bereits das Fertigen von Fotos in der Kindertagesstätte oder in der Schule (z.B. für Portfolios oder zur Erstellung eines Klassensitzplans) stellt einen Eingriff in das allgemeine Persönlichkeitsrecht in der Form des Rechts am eigenen Bild dar, so dass auch insoweit eine Einwilligung der Betroffenen einzuholen ist (vgl. 24. Tb., Tz. III-6.1.5). Mit dem Einholen der Einwilligungserklärung sollte darüber unterrichtet werden, zu welchem Zweck die Fotos aufgenommen, wo und wie lange sie gespeichert und ob externe Dritte (z.B. ein Online-Fotolabor) eingeschaltet werden.

Der LfDI hat aufgrund zahlreicher Anfragen folgenden Mustertext einer Einwilligungserklärung für die Veröffentlichung von Fotos bzw. Videos auf einer Schulhomepage zur Verfügung gestellt:

Sehr geehrte Eltern,
im Rahmen der schulischen Aktivitäten (Schulprojekte, Veranstaltungen, usw.) an unserer Schule werden Fotos und manchmal auch Videos der beteiligten Kinder gemacht. Beispielsweise werden anlässlich der Einschulung Einzel- und Gruppenaufnahmen durch professionelle Fotografen gefertigt. Um die Tätigkeiten der Schule auch nach außen hin zu kommunizieren, sollen gelegentlich auch Fotos in Medien, wie Tageszeitungen und der Homepage der Schule veröffentlicht werden. Immer wieder kommen auch Fernseh- und Rundfunkanstalten auf die Schule zu und möchten aus aktuellem Anlass Film- und Tonaufnahmen machen.

Mit diesem Schreiben möchten wir eine grundsätzliche Klärung herbeiführen, ob Sie mit den Anfertigen und Veröffentlichen von Fotos/Videos Ihres Kindes einverstanden sind. Bitte füllen Sie nachfolgende Erklärungen aus; Ihrem Kind entstehen keinerlei Nachteile, wenn Sie mit der Veröffentlichung von Fotos/Video Ihres Kindes insgesamt oder teilweise nicht einverstanden sind. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Name des Kindes _____ Klasse _____

Name der Erziehungsberechtigten _____

Ich bin damit einverstanden, dass Einzel- und Gruppenaufnahmen meines Kindes durch Fotografen gefertigt werden
Ja ☐ Nein ☐

Ich bin damit einverstanden, dass Fotos meines Kindes in Zeitungsberichten veröffentlicht werden
Ja ☐ Nein ☐

Ich bin damit einverstanden, dass von meinem Kind Film- und Tonaufnahmen durch Pressevertreter gemacht werden dürfen:
Ja ☐ Nein ☐

Ich bin damit einverstanden, dass Fotos/Videos meines Kindes im Internet auf der Homepage der Schule veröffentlicht werden:
Ja ☐ Nein ☐.

(weitere Fälle bitte gegebenenfalls ergänzen)

Datum _____

Unterschrift Erziehungsberechtigter _____

7.2 Wissenschaft

7.2.1 Datenschutzrechtliche Prüfung wissenschaftlicher Forschungsvorhaben

Die Zahl der im Zusammenhang mit § 67 Abs. 6 des SchulG zur Prüfung eingereichten Vorhaben ist nochmals deutlich angestiegen.

Wurden dem LfDI in den Jahren 2008/2009 noch nur gut 100 Vorhaben vorgelegt, waren es im aktuellen Berichtszeitraum 2014/2015 annähernd 300 an der Zahl! Wie bereits berichtet, führt dies zu Einschnitten in anderen Tätigkeitsfeldern (vgl. 24. Tb., Tz. III-6.2). Überhaupt ist die Prüfung in diesem Umfang u.a. nur noch deswegen zu handhaben, weil die Studierenden, Wissenschaftlerinnen und Wissenschaftler und Forschungsinstitute kooperieren und die datenschutzrechtlichen Anmerkungen grundsätzlich aufgreifen.

Dies lässt sich trotz fehlender Vorort-Prüfungen auch daran festmachen, dass nur ganz ausnahmsweise einmal auf eine Eingabe z.B. eines Elternteiles hin ein Forschungsvorhaben daraufhin zu prüfen war, ob bei der Durchführung gegen datenschutzrechtliche Vorgaben verstoßen wurde.

Jedenfalls sollte in Zeiten der zunehmenden Digitalisierung von öffentlichen Stellen z.B. mehr Zeit von den vorhandenen Personalressourcen zur datenschutzrechtlichen Begleitung der Einführung weiterer zeit- und ortsunabhängiger Verwaltungsdienste (eGovernment) eingesetzt werden können.

Leider konnte die mit der Aufsichts- und Dienstleistungsdirektion Trier als Schulbehörde und dem Wissenschaftsministerium abgestimmte Verfahrensänderung, die den LfDI in diesem Zusammenhang entlasten soll, noch immer nicht in die Praxis umgesetzt werden. Dies ist aber nach Absprache mit dem Ministerium für das Schuljahr 2016/2017 zugesagt.

7.2.2 Zunehmende Themenvielfalt der Anfragen aus dem Hochschulbereich

Beschränkten sich die Eingaben und Anfragen bisher praktisch ausschließlich auf das Thema „Nachweis der Prüfungsunfähigkeit und Anforderungen an ein ärztliches Attest“ (vgl. 23. Tb., Tz. II-6.2.2), waren im Berichtszeitraum vielfältige Fragestellungen aus dem Bereich des allgemeinen Datenschutzrechts zu beantworten, was den Schluss nahelegt, dass man sich auch in diesem Umfeld zunehmend mit dem Thema Datenschutz auseinandersetzt.

So warf das Präsidium eines Studierendenparlaments die Frage auf, ob die Studierendenschaft einen Datenschutzbeauftragten bestellen muss oder ob für die Bearbeitung von Anfragen mit datenschutzrechtlichem Bezug aus dem Bereich der Studierendenschaft die oder der behördliche Datenschutzbeauftragte der Universität zuständig ist. Hierzu ist zunächst festzuhalten, dass die Studierendenschaft eine rechtsfähige Körperschaft des öffentlichen Rechts ist (§ 108 Abs. 2 HochSchG). Somit ist gemäß § 2 Abs. 1 S. 1 LDSG das Landesdatenschutzgesetz auf das Handeln der Studierendenschaft anwendbar. Als öffentliche Stelle hätten Studierendenschaften also bei Vorliegen der Voraussetzungen nach § 11 Abs. 1 S. 1 LDSG behördliche Datenschutzbeauftragte zu bestellen. Gemäß § 11 Abs. 1 S. 4 LDSG ist es aber auch nicht ausgeschlossen, dass die oder der behördliche Datenschutzbeauftragte der Universität diese Aufgabe in Personalunion sowohl für den allgemeinen Verwaltungsbereich der Universität wie auch für die Studierendenschaft übernimmt.

Ein Allgemeiner Studierendenausschuss (AStA) als die hochschulweite Interessenvertretung der Studierenden problematisierte, ob zur Prüfung eines Härtefallantrages durch das Prüfungsamt die Vorlage eines Totenscheines gefordert werden kann. Die Antragstellenden müssen die von ihnen geltend gemachten Gründe für die Wiederholung eines Prüfungstermins oder für den Rücktritt nach Beginn

einer Prüfung regelmäßig gegenüber dem Prüfungsamt glaubhaft machen. Im Einzelfall kann daher die Vorlage des Totenscheines verstorbener Angehöriger zur Aufgabenerledigung des Prüfungsamtes erforderlich sein. Gegebenenfalls wäre die Vorlage einer beglaubigten Kopie, auf der außer dem Namen der Verstorbenen und dem Sterbetag alle anderen Angaben geschwärzt sind, zur Glaubhaftmachung ausreichend.

Ein AStA thematisierte, dass eine Beratungsstelle zum Zweck des Nachweises durchgeführter Beratungen für die Abrechnung mit einer anderen Stelle den Namen und die Matrikelnummer der die Leistungen in Anspruch nehmenden Studierenden sowie den Termin auf der Grundlage einer Einwilligung erhebt und übermittelt. Hier konnte der LfDI gemeinsam mit dem behördlichen Datenschutzbeauftragten eine pseudonymisierte Vorgehensweise abstimmen, die allen Seiten gerecht wird.

7.2.3 Sonstiges

Im Datenschutzbericht 2012/2013 wurde über das Anliegen der Leitungen verschiedener namhafter Forschungsinstitute informiert, eine Verfahrensabrede zur datenschutzrechtlichen Prüfung bundeslandübergreifender Schulleistungsuntersuchungen (z.B. PISA) zu treffen, mit der eine Erleichterung und Entbürokratisierung von Abläufen sowohl in den Aufsichtsbehörden als auch in den Forschungsinstituten einhergehen soll (vgl. 24. Tb., Tz. III-6.2.2).

Dieses Anliegen wurde im Dezember 2015 in der Arbeitsgruppe „Datenschutz und Schule“ der Datenschutzkonferenz beraten und die Einrichtung einer Unterarbeitsgruppe beschlossen, in deren Arbeit sich der LfDI einbringen wird.

Die Unterarbeitsgruppe soll sich mit einem zukünftigen Verfahren zur Prüfung solcher länderübergreifender Untersuchungen beschäftigen. Als weitere Aufgaben kommen die Entwicklung eines Grundkonzepts sowie von Positionen zu grundlegenden Fragen, die sich bei der Durchführung eines Forschungsvorhabens stellen, in Betracht.

Nach den Universitäten Mainz und Trier werden weitere rheinland-pfälzische Hochschulen vorhandene Anwendungen durch integrierte Campusmanagementsysteme ablösen, die aus den Modulen Studierendenverwaltung, Prüfungsverwaltung und Studienmanagement bestehen.

Dem geäußerten Beratungsbedarf, z.B. im Hinblick auf die Umsetzung eines geeigneten Rollen- und Berechtigungskonzepts oder Konzepten für die Protokollierung von Zugriffen oder zur Löschung nicht mehr zur Aufgabenerfüllung erforderlicher Daten, wird der LfDI entsprechend seinem gesetzlichen Auftrag nachkommen.

8. Bildung und Erziehung

8.1 Youngdata

Im November 2013 wurde vom LfDI das Internetangebot Youngdata freigeschaltet, das sich mit Datenschutzinformationen gezielt an Kinder und Jugendliche richtet (vgl. 24. Tb., Tz. II-3.1). Es beinhaltet Datenschutztipps bei der Nutzung von Facebook, WhatsApp, YouTube, Spielekonsolen, Smartphones und anderen Anwendungen, klärt über die Gefahren von Cybermobbing auf und bietet Hintergrundinformationen zum Datenschutz im Allgemeinen. Ein eigener Newsbereich und konkrete Handlungsempfehlungen („Tipps“) sollen dazu beitragen, sich möglichst datenschutzbewusst im Internet zu bewegen. Um die bisweilen etwas sperrigen Datenschutzthemen zielgruppengerecht zu transportieren, bemüht sich Youngdata um eine jugendgerechte Sprache und ist mit zahlreichen Karikaturen, Videos und Fotos angereichert.

Die Datenschutzkonferenz hatte bereits vier Monate nach dem Start von Youngdata beschlossen, diese als gemeinsame Internetseite aller Datenschutzbeauftragten für Jugendliche weiter zu betreiben. Anlässlich des „Safer Internet Day“ am 10. Februar 2015 wurde unter Beteiligung der BfDI, Frau Andrea Voßhoff, und einigen Länderkollegen dieses gemeinsame Projekt der Öffentlichkeit im Rahmen einer Pressekonferenz vorgestellt. Seit Februar 2015 wird Youngdata daher als gemeinsames Portal der Datenschutzbeauftragten des Bundes und der Länder betrieben.

Mit der Übernahme als gemeinsame Seite aller Datenschutzbeauftragten haben sich auch die Verantwortlichkeiten geändert: Die Pflege der Hauptmenüpunkte erfolgt im Wege einer Arbeitsteilung durch einzelne Datenschutzbeauftragte. Unter dem Menüpunkt „Was gibt’s in deiner Nähe?“ hat jedes Land die Möglichkeit, eigene Bildungsprojekte vorzustellen. Die Geschäftsführung liegt jedoch nach wie vor beim LfDI. Die Kosten für den Betrieb der Seite werden auf alle Länder und den Bund verteilt.

Youngdata versteht sich damit als Beitrag der Datenschutzbeauftragten des Bundes und der Länder zur digitalen Bildung.

Im Berichtszeitraum hat auch der Datenschutzbeauftragte des Kantons Zürich Interesse an einer Kooperation bekundet. Um eine noch größere Verbreitung von wichtigen Informationen zum digitalen Datenschutz und der Informationsfreiheit zu erreichen, ist es aus Sicht des LfDI erstrebenswert, stetig weitere Kooperationspartner hinzu zu gewinnen.

Seit ihrem Bestehen wurde Youngdata kontinuierlich weiterentwickelt:

- 2014 wurde ein in Zusammenarbeit mit dem Fachbereich Informatik und Mikrosystemtechnik der Fachhochschule Kaiserslautern erstelltes Quiz online gestellt, in dem Interessierte ihr Wissen zu allgemeinen und speziellen Datenschutzfragen testen können.
- Außerdem wurde die Seite um Lernszenarien für den Unterricht ergänzt. Diese E-Learning-Szenarien befähigen Lehrkräfte auch ohne aufwändige Eigenfortbildung z.B. in einer Vertretungsstunde eine Unterrichtseinheit zum Datenschutz im Internet für die Mittel- und Oberstufe durchführen.
- Da zunehmend Datenschutzfragen im Zusammenhang mit dem Fertigen und Verbreiten von Handyfotos und –videos entstehen, enthält der Untermenüpunkt „Datenschutz-Tipps“ jetzt einen neuen Bereich zum Thema „Datenschutz bei Selfies“.
- Zum zweijährigen Bestehen der Plattform wurde eine neue Rubrik „Digitale Selbstverteidigung“ eingeführt. Die notwendigen Vorarbeiten hierfür wurden von einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder unter Federführung des LfDI geleistet. Der neue Menüpunkt stellt dar, welche Möglichkeiten Jugendliche haben, durch eigenes Verhalten digitale Datenspuren zu vermeiden und Kontrolle über ihre Daten zu behalten. Hierzu werden vorhandene Angebote gebündelt und zu verschiedenen Themenbereichen entsprechende Informationen zielgruppengerecht aufbereitet. Ein zusammen mit dem Offenen Kanal Mainz eigens hierfür produziertes Video soll verdeutlichen, dass im Internet veröffentlichte Informationen leicht zweckentfremdet werden können.
- Auf technischer Seite wurde eine Optimierung für mobile Endgeräte vorgenommen („responsive design“).

- Mit Blick auf die sog. „Cookie-Richtlinie“ (Richtlinie 2002/58/EG in der Fassung durch Richtlinie 2009/136/EG) wurde ein Banner am oberen Seitenrand integriert, das die Besucherinnen und Besucher gut sichtbar auf die Verwendung von Cookies hinweist und auf den betreffenden Teil der Datenschutzerklärung verweist.
- Weiterhin wurde eine JavaScript-Weiche installiert, die eine verbesserte Darstellung der Seite für Besucherinnen und Besucher ohne aktiviertes JavaScript gewährleistet. Zusätzlich wird am oberen Seitenrand ein Infobanner angezeigt, das über etwaige Beeinträchtigungen (z.B. die eingebetteten Videos) informiert.
- Eine gemeinsam mit der Hochschule Kaiserlautern entwickelte „CheckApp“ wird angeboten werden, mit der das eigene Wissen und Verhalten in puncto Datenschutz überprüft werden kann.
- Die im 24. Tätigkeitsbericht beschriebene Zwei-Klick-Lösung für Videos in Form einer eigens entwickelten TYPO3-Erweiterung steht nun inklusive Dokumentation für die Öffentlichkeit zum Download zur Verfügung (vgl. 24. Tb., Tz. III-1.3). Nähere Informationen unter: http://www.datenschutz.rlp.de/de/zweiklick.php

Was die Zugriffszahlen angeht, konnten in den ersten sechs Monaten nach dem Start von Youngdata ca. 40.000 Seitenaufrufe festgestellt werden. Innerhalb des ersten Jahres steigerte sich die Zahl der Besucherinnen und Besucher auf etwa 70.000. Nachdem Youngdata in die Verantwortung aller Datenschutzbeauftragten überführt wurde, haben sich die täglichen Besuche von ursprünglich ca. 130 auf ca. 175 gesteigert. Durchschnittlich wird die Seite derzeit ca. 3.000 Mal im Monat aufgerufen. Der Anteil der mobilen Geräte beträgt dabei 25 Prozent. Zwischenzeitlich wurde die Plattform mehr als 100.000 Mal besucht. Dabei handelt es sich um geschätzte Mindestzahlen, da die zum Einsatz kommende Software nicht alle Seitenbesuche erfasst.

Youngdata ist aber auch notwendiger Bestandteil des Schülerworkshop-Projektes. Denn mithilfe dieser Internetseite können Schülerinnen und Schüler zu datenschutzrelevanten Themen bei der Internetnutzung selbstständig recherchieren und sich die Ergebnisse noch während des Workshops gegenseitig präsentieren.

Aber auch an die Lehrkräfte wurde gedacht: Die Medienpädagogen beim LfDI haben eigene E-Learning-Szenarien entwickelt, die es Lehrkräften auch ohne aufwendige Eigenfortbildung ermöglichen, z.B. in einer Vertretungsstunde eine Unterrichtseinheit zur Thematik „Datenschutz und Internet“ anzubieten.

8.2 Medienpädagogische Arbeit

Die Vernetzung und inhaltliche Abstimmung mit dem für die Lehrerfortbildung zuständigen Pädagogischen Landesinstitut ist wichtiger Bestandteil der Bildungsaktivitäten des LfDI. In mehreren Gesprächen unter Beteiligung des Bildungsministeriums wurden die Angliederung von Lehrinhalten mit Datenschutzbezug an die Medienscoutausbildung, weitere Möglichkeiten der Fortbildung für Lehrkräfte und die inhaltliche Abgrenzung der Schülerworkshops des LfDI gegenüber anderen Landesangeboten thematisiert.

Aufgrund der engen Kooperation mit medien+ bildung.com – einer gemeinnützigen GmbH der Landeszentrale für Medien und Kommunikation (LMK) – ist seit dem Jahr 2010 eine medienpädagogische Fachkraft zum LfDI abgeordnet. Derzeit teilen sich die Stelle ein Medienpädagoge und ein Medienwissenschaftler. Ohne diese fachspezifische und tatkräftige Unterstützung wären die vielfältigen Bildungsaktivitäten (vgl. Tz. III-8) des LfDI nicht möglich gewesen.

Die medienpädagogischen Fachkräfte hatten maßgeblichen Anteil an der Gestaltung und Pflege der Jugendseite Youngdata (vgl. Tz. III-8.1). Dies gilt sowohl für das Design der Seite, die technische Umsetzung unter Nutzung der Software Typo3 sowie das Erstellen von inhaltlichen Beiträgen. Hervorzuheben sind die eigens produzierten Videoclips, die auf Youngdata zu sehen sind.

Die fachspezifischen Kenntnisse seiner Mitarbeiter in Sachen Mediengestaltung und grafisches Layout nutzte der LfDI auch im Rahmen seiner Öffentlichkeitsarbeit, etwa bei der Gestaltung von Flyern, Plakaten, Rollups und Broschüren.

8.3 Medienkomp@ss

Das Projekt „Medienkomp@ss“ wurde im Berichtszeitraum weiter entwickelt. Über 350 Schulen nutzen zwischenzeitlich den Medienkompass im Bereich der Primar- und Orientierungsstufe. Für den LfDI besteht die Möglichkeit, künftig Schulungsmaterialien zu erarbeiten, die zusammen mit dem bereits vorhandenen Unterrichtsmaterialien auf dem sog. OMEGA-Server gespeichert werden. Lehrkräfte können sodann über die Medienkompass-Seite des Bildungsministeriums (http://medienkompass.bildung-rp.de/) gezielt nach Unterrichtsmaterial zu bestimmten (Datenschutz-)Themen auf dem OMEGA-Server suchen (z.B. Persönlichkeitsrecht, Virenschutz). Da das hinterlegte Material auf dem Server in Teilen frei verfügbar ist, kann es auch außerhalb des Medienkompasses für die digitale Grundbildung von Schülerinnen und Schülern verwendet werden.

Neu hinzugekommen ist die Verknüpfung des Medienkompasses mit dem Schülerworkshop-Projekt (vgl. Tz. III-8.5): Schülerinnen und Schüler, die einen Workshop erfolgreich absolviert haben, können dies als erworbene Kompetenz im Medienkompass eintragen lassen.

8.4 Sonstige Bildungsaktivitäten

Als Vorsitzender des Arbeitskreises Datenschutz und Bildung suchte der LfDI bereits 2010 den Kontakt zur Kultusministerkonferenz. Der Vorsitzende der Gemischten Kommission und ein Mitglied des Schulausschusses haben im Arbeitskreis wiederholt referiert. Der LfDI folgte den sich anschließenden regelmäßigen Einladungen der KMK und hielt letztmals am 18. Mai 2015 vor der Gemischten Kommission der KMK einen Vortrag mit dem Titel „Digitale Grundbildung und Medienkompetenz“. Nicht zuletzt diesem bewährten Gedankenaustausch zwischen Arbeitskreis und KMK ist es zu verdanken, dass es im März 2012 zu dem heute viel zitierten Beschluss der KMK „Medienbildung in der Schule“ kam. Unter dem AK-Vorsitz des LfDI Thüringen wurde die Zusammenarbeit weiter fortgeführt.

Fast dreißig programmierbegeisterte und kreative Jugendliche im Alter zwischen 13 und 18 Jahren haben vom 13. bis zum 16. Mai 2015 am Rabanus-Maurus-Gymnasium in Mainz im Rahmen des vom LfDI erstmals ausgerichteten Coding Camps eigene Smartphone-Apps entwickelt. Unterstützt wurden die Schülerinnen und Schüler dabei von Informatikstudierende der Fachhochschule Bingen, der Hochschule Mainz und Mitgliedern des Chaos Computer Clubs Mainz/ Wiesbaden, die als Mentorinnen und Mentoren fungierten und wo nötig mit technischem Know-how weiterhalfen. Ihre Apps präsentierten die Jugendlichen am letzten Tag des Camps, im 22. Stock des Bonifaziusturms A im Rahmen der Veranstaltungsreihe des LfDI zu Kunst und Datenschutz mit dem Titel „#watch22 – Ausstellung/Datenschutz/Kunst/Kultur/“. Eine Jury zeichnete aus den insgesamt elf Projekten die pfiffigsten aus. In zwei Kategorien warben die Teilnehmerinnen und Teilnehmer um die Gunst der Juroren: In der Kategorie „Open Data App“ konkurrierten fünf Teams um den Preis für die beste App, die auf offenen Geodaten basierte. In der Kategorie „Freestyle App“ wetteiferten sechs Projekte, unter anderem eine Chat-Applikation, eine Stundenplan-App und eine Vokabeltrainer-App um den ersten Preis.

Anlässlich des „Safer Internet Day“ 2015 fanden in Erfurt gleich zwei Ereignisse statt, an denen der LfDI maßgeblich beteiligt war: Zum einen wurde im Rahmen einer Pressekonferenz die bislang vom LfDI Rheinland-Pfalz gehostete Jugendseite Youngdata in die Hände aller Datenschutzbeauftragten des Bundes und der Länder übergeben. Zum anderen hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit zu einer Veranstaltung „Medienkunde als eigenes Schulfach – Neuland in Sicht?“ eingeladen. An der ganztägigen Veranstaltung nahmen über 150 Lehrkräfte teil. Der LfDI hielt einen der Hauptvorträge und war bei der anschließenden Diskussion auch auf dem Podium vertreten.

Als Kooperationspartner des medientriXX-Projekts des Südwestwundfunks beteiligte sich der LfDI mit insgesamt neun Schülerworkshops in Grundschulen der vierten Klasse zu Datenschutzthemen. Bei der jährlich stattfindenden iMedia – einer Fortbildungsveranstaltung für Lehrkräfte in Mainz – präsentierte der LfDI in mehreren Informationsveranstaltungen die Jugendseite Youngdata einschließlich der zum Einsatz kommenden E-Learning-Module.

Anlässlich des 13. Bundeskongresses der Bundeszentrale für politische Bildung in Duisburg veranstaltete der LfDI einen Workshop mit dem Titel „Kleine Dinge und große Spuren – Wie das Internet der Dinge und Big Data unsere Gesellschaft verändern“. Für die pädagogische Vermittlung wurde die Methode „Fishbowl“ gewählt, was eine aktive Einbeziehung der Teilnehmer ermöglichte.

Im Rahmen des TAIEX-Programms der Europäischen Union (vgl. 24. Tb., Tz. II-2.11) war der LfDI erneut – diesmal in Montenegro – vertreten: Die montenegrischen Datenschutzbeauftragten wurden über die Bildungsprojekte des LfDI informiert.

Seit dem Jahr 2014 hat der LfDI Kontakt zur Anne-Frank-Stiftung in Frankfurt. Die Stiftung betreibt nachhaltige Projekte zum Thema „Menschenrechtsbildung“, z.B. Schülerworkshops mit einem Referententeam und eine Wanderausstellung in Form eines „mobilen Lernlabors“ mit dem Titel „Mensch, Du hast Rechte“. In mehreren Besprechungen wurden Kooperationsmöglichkeiten ausgelotet. Ziel war es, die institutionell unterschiedlichen Bildungsmodelle zu vergleichen und Ansätze der Informationsvermittlung und Sensibilisierung von Jugendlichen für Grund- und Menschenrechte zu erörtern.

Zusammen mit dem Medienkompetenznetzwerk Mainz-Rheinhessen und der Johannes Gutenberg-Universität erweitere der LfDI im Berichtszeitraum seine Aktivitäten zur Medienkompetenzvermittlung für Seniorinnen und Senioren. Neben einer inhaltlich redaktionellen Mitarbeit bei der Neuauflage des „Silversurfer“-Modulhandbuchs zum Datenschutz, erstellten der LfDI und der Landesbeauftragte für den Datenschutz Baden-Württemberg für die Homepage www.silver-tipps.de Beiträge und steuerten zu den monatlich wechselnden Themenschwerpunkten Artikel mit Datenschutzaspekten bei.

8.5 Schülerworkshops

Einen Arbeitsschwerpunkt der medienpädagogischen Arbeit bildete das Schülerworkshop-Projekt des LfDI. Hier erarbeiteten die Kräfte pädagogische Konzepte und E-learning-Szenarien für den Bereich der Grundschulen und weiterführenden Schulen. Bei der Auswahl und Ausbildung neuer Honorarkräfte und deren Weiterbildung waren sie ebenfalls maßgeblich beteiligt.

Weiterhin übernahmen die Fachkräfte im Berichtszeitraum zahlreiche Multiplikatorenschulungen, informierten auf Studientagen und Elternabenden und übten Vortragstätigkeiten im Bereich der Universitäten und Hochschulen aus.

Hervorzuheben ist schließlich die Betreuung von FSJ-Kräften durch die Medienspezialisten der Behörde. Im September 2014 wurde beim LfDI erstmals eine FSJ-Stelle Politik eingerichtet. Die FSJ-Kräfte wurden im Rahmen ihrer einjährigen Beschäftigung beim LfDI in die allgemeine Verwaltungsarbeit eingearbeitet, erhielten Softwareschulungen im Bereich Mediengestaltung, einschließlich der Produktion von Kurzfilmen. Inhaltlich wurden die FSJ-Kräfte in rechtlichen und technischen Fragen zum Datenschutz bei der Internetnutzung ausgebildet und arbeiteten zusammen mit den medienpädagogischen Kräften im Bereich der Organisation des Schülerworkshop-Projekts mit.

8.6 Wissenschaftspreis des LfDI

Im Jahr 2014 wurde zum fünften Mal gemeinsam mit dem Ministerium für Bildung, Wissenschaft, Weiterbildung und Kultur der Datenschutzpreis des LfDI für herausragende wissenschaftliche Arbeiten im Bereich des Datenschutzes vergeben. Der Preis ging an eine Studentin der Johannes Gutenberg-Universität Mainz und wurde für die Bachelorarbeit „Google – The World Brain. Was passiert, wenn die ganze Welt zum Index wird“ verliehen. Im Mittelpunkt der Arbeit stehen die Google-Suchmaschine und die Ambivalenz der von Google angebotenen sonstigen Dienste sowie deren individuelle und gesellschaftliche Konsequenzen.

Unter dem Titel „Aufklärung im Interesse der Freiheit“ veröffentlichte der LfDI im Rahmen der Preisverleihung eine Erklärung, mit der die Verdienste des Whistleblowers Edward Snowden gewürdigt wurden. Ihm ist es zu verdanken, dass in Staat und Gesellschaft eine breite und intensive Diskussion über notwendige Strategien gegen eine alltägliche und globale Überwachung in Gang gekommen ist. Dies hat das Datenschutzbewusstsein geschärft und die digitale Welt verändert.

Im Jahr 2015 wurde aufgrund der Veranstaltungsreihe #watch22 (vgl. Tz. II-3) der Preis nicht ausgeschrieben.

Verleihung des Wissenschaftspreises 2014
http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2014091601
Erklärung des LfDI – „Aufklärung im Interesse der Freiheit – Zu den Verdiensten Edward Snowdens“
http://www.datenschutz.rlp.de/de/wissenschaftspreis/bisherige_arbeiten/2014_Erklaerung_zu_Snowden.pdf

9. Kommunales, Meldewesen und Statistik

9.1 Kommunales

9.1.1 eGovernment im kommunalen Alltag

Unter e(lectronic)-Government im engeren Sinne wird allgemein die Abwicklung von Prozessen über elektronische Medien im Zusammenhang mit Regieren und Verwalten unter Verwendung von Informations- und Kommunikationstechniken verstanden. Es geht sowohl um Prozesse zwischen öffentlichen Stellen untereinander als auch gerade um solche zwischen öffentlichen Stellen und den Bürgerinnen und Bürgern bzw. Unternehmen.

Das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz) wurde bereits im Datenschutzbericht 2012/2013 angesprochen (vgl. 24. Tb., Tz. I-3.3.2). Das Gesetz dient dem unterstützenswerten Ziel, die elektronische Kommunikation mit der Verwaltung zu erleichtern und Bund, Ländern und Kommunen zu ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten (e-Government im weiteren Sinne).

Im Folgenden sollen mit einem Ausschnitt von Anwendungsbeispielen aus dem kommunalen Alltag die bereits vorhandene Vielfalt aufgezeigt und die damit ggf. verbundenen datenschutzrechtlichen Probleme, die teilweise auch im Hinblick auf das E-Government-Gesetz thematisiert wurden, angerissen werden.

Abhängig vom Grad der Beteiligung der Bürgerinnen und Bürger werden e-Government-Anwendungen folgendermaßen unterschieden:

- e-Information als (bloße) Bereitstellung von Inhalten für einen unbestimmten Nutzerkreis
- e-Kommunikation mit dem Schwerpunkt auf dem Austausch von Informationen durch Kommunikationsprozesse
- e-Transaktion als wechselseitiger Kontakt zwischen Verwaltung und Bürgerinnen und Bürger und der Erbringung der gewünschten Dienstleistung auf elektronischem Weg

Unter e-Information fallen:

- Zulässig ist ein sog. Live-Stream von Gremiensitzungen, der nach einer Änderung der Gemeinde- bzw. Landkreisordnung (vgl. Tz. I-3.2) auf der Grundlage der Hauptsatzung möglich ist.
- Als „Bürgerinformationssystem“ wird der Service bezeichnet, aus einem Ratsinformationssystem (vgl. Tz. III-14.1) der Öffentlichkeit Informationen bzw. Dokumente zur Verfügung zu stellen, die im Rahmen der Gremienarbeit anfallen. Grundsätzlich geht es hier um die Beantwortung der Frage, inwieweit deren Veröffentlichung im Internet datenschutzrechtlich zulässig ist. Denn bei der Veröffentlichung auch personenbezogener Ratsinformationen im Internet handelt es sich um eine Datenübermittlung an nicht-öffentliche Stellen (§ 16 LDSG) und eine Datenübermittlung ins Ausland (§ 17 LDSG), da auf den öffentlichen Teil des Ratsinformationssystems weltweit von einem unbestimmten Personenkreis zugegriffen werden kann.

Das Kommunalverfassungsrecht sieht aber regelmäßig nur eine lokal begrenzte Öffentlichkeit vor. Sein Ziel ist es, den Bürgerinnen und Bürgern der jeweiligen Kommune zum Zweck der demokratischen Kontrolle und Teilhabe Einblick in die Tätigkeit kommunaler Vertretungskörperschaften zu gewähren.

Die Inhalte für ein Bürgerinformationssystem müssen daher einer Abwägung zwischen öffentlichem Informationsinteresse und Schutz der personenbezogenen Daten unterzogen werden. Im Hinblick auf die Dauer der Bereitstellung von Dokumenten ist der Wegfall des Informationsinteresses bzw. des -gehaltes für die Öffentlichkeit zu berücksichtigen.

Konkret geht es hier z.B. um die Tagesordnung und die Niederschrift einer Ratssitzung, Einwendungen gegen den Entwurf eines Bebauungsplanes, den Beschluss eines Wahlausschusses zur Wählbarkeit einer Bewerberin oder eines Bewerbers oder Karten eines Dorferneuerungskonzepts.

Unter e-Kommunikation fällt:

- Mit dem Service „Videodolmetschen“ ist ein deutschlandweiter Dolmetscherpool gemeint, mit

dem gerade die Kommunen im Bereich Asylwesen und Migration unterstützt werden sollen.
Als Videokonferenzsystem werden über gesicherte Internetverbindungen auf bereits vorhandener Hardware in der Behörde Dolmetscherinnen und Dolmetscher für Beratungsgespräche u.a. mit z.B. Asylbewerberinnen und -bewerbern zugeschaltet.
Im Hinblick auf die vorgestellte IT-Infrastruktur und unter der Voraussetzung, dass außerhalb der jeweils nutzenden Stelle weder Aufzeichnungen erfolgen noch Gesprächsinhalte gespeichert werden, bestehen keine datenschutzrechtlichen Bedenken.

Unter e-Transaktion fallen:

- Die „Onleihe“ ist ein Service zur Ausleihe von e-Medien, der für die Nutzerinnen und Nutzer von öffentlich zugänglichen Bibliotheken erbracht wird. Damit wird das traditionelle Angebot der Bibliotheken ergänzt. Öffentlichen Bibliotheken wird es dadurch ermöglicht, eine von der Bibliothek getroffene Auswahl digitalisierter Medien zum virtuellen Ausleihen zur Verfügung zu stellen.
  Die Nutzung der elektronischen Ausleihe erfordert eine Registrierung und die Freischaltung des Zugangs durch die Bibliothek, wofür Stammdaten von der Bibliothek an Dienstleister übermittelt werden müssen.
  Da die Inanspruchnahme dieses zusätzlichen Angebotes auf der Grundlage der informierten Einwilligung der Bibliotheksnutzerinnen und -nutzer erfolgt und personenbezogenes Nutzerverhalten nicht protokolliert wird, bestehen keine datenschutzrechtlichen Bedenken.
- Für alle Kommunen steht ein temporäres Bürger- bzw. Servicekonto als Webservice zur Verfügung. Dieses Bürger- bzw. Servicekonto dient mit einer zentralen Identifizierungskomponente der Abwicklung von Online-Verwaltungsdienstleistungen. Nachdem dieser Dienst zur elektronischen Identifizierung aus dem Chip des (neuen) Personalausweises (eID-Funktion) einer Bürgerin oder eines Bürgers notwendige Daten ausgelesen hat, können über angebundene Fachverfahren der jeweiligen Kommune Verwaltungsdienstleistungen online abgewickelt werden.
  Für ein Bürger- bzw. Servicekonto muss der IT-Dienstleister eine Genehmigung, das sog. Berechtigungszertifikat (§ 21 Abs. 1 PAuswG), beim Bundesverwaltungsamt beantragen. Diesbezüglich ist datenschutzrechtlich zu beachten, dass auf der Grundlage eines Zertifikates über ein Bürger- bzw. Servicekonto nicht mehrere Verwaltungsdienstleistungen abgewickelt werden, für die zur Identifizierung des Antragstellers unterschiedliche Datenprofile ausgelesen werden.
  Online können im Melde- und Personenstandswesen verschiedene Verwaltungsdienstleistungen sowie die Kfz-Abmeldung abgewickelt werden. Sofern dafür eine Gebühr anfällt, kann diese mittels e-Payment bezahlt werden.
  Ein temporäres Bürger- bzw. Servicekonto sieht vor, dass nach Abschluss der Nutzung einer Verwaltungsdienstleistung und Übergabe der Identitätsdaten an das betreffende Verwaltungsfachverfahren die Identitätsdaten im Bürgerkonto wieder gelöscht werden.
  Der Strategie für eID und andere Vertrauensdienste im e-Government (eID-Strategie) des IT-Planungsrates ist zu entnehmen, dass es perspektivisch möglich sein soll, sich behörden- und verwaltungsebenen übergreifend für die Abwicklung von Verwaltungsdienstleistungen identifizieren zu können. Damit wäre es z.B. möglich, eine Geburtsurkunde beim Standesamt des Geburtsortes mit einem Bürgerkonto des Wohnortes, der oft nicht identisch mit dem Geburtsort ist, zu beantragen.

9.1.2 Zusammenarbeit mit privaten Inkassounternehmen

Immer wieder befassen Kommunalverwaltungen den LfDI mit dem Vorhaben, ein privates Inkassounternehmen in den kommunalen Forderungseinzug einzubinden. Dabei wird z.B. im Rahmen einer Studie des Fachverbandes der Kommunalkassenverwalter e.V. die Aussage getroffen, dass eine solche Zusammenarbeit als Optimierungsstrategie für das kommunale Forderungsmanagement keine praktische Relevanz habe.

Nach der Einschätzung des LfDI bestehen keine materiell-rechtlichen Bedenken, ein privates Inkassounternehmen im Wege der Verwaltungshilfe in den kommunalen Forderungseinzug einzubinden.

Beispiele für eine Hilfstätigkeit, die von einem Inkassounternehmen als Auftragnehmer im Wege der Verwaltungshilfe ausgeübt werden kann, sind die Fertigung von Mahnschreiben oder die Nutzung von Vollstreckungsauskünften als weisungsgebundene Tätigkeit des Auftragnehmers, der die in der firmeneigenen Vollstreckungsauskunft enthaltenen Informationen der Kommune als Auftraggeberin bereitstellen soll. Auch die Adressermittlung kann im Rahmen einer Auftragsdatenverarbeitung (§ 4 LDSG) erfolgen.

Typische Fälle der Auftragsdatenverarbeitung sind – ganz allgemein gesagt – die Auslagerung

- einzelner Phasen der Datenverarbeitung oder
- technisch vorhersehbarer Unterstützungsleistungen

auf eine andere Stelle.

Anders verhält es sich bei Tätigkeiten, die nur im Wege einer Aufgabenübertragung übernommen werden können. Da dies aus fachrechtlicher Sicht schon nicht möglich ist, sofern die öffentlich-rechtlichen oder privat-rechtlichen Forderungen dem Geltungsbereich des Landesverwaltungsvollstreckungsgesetzes unterfallen, wurden insoweit vom LfDI datenschutzrechtliche Bedenken geäußert.

Im Gegensatz zur Verwaltungshilfe ist Merkmal einer Aufgabenübertragung ein Ermessens- und Gestaltungsspielraum bei der Erledigung der vereinbarten Tätigkeit, mit anderen Worten, der Auftragnehmer kann eigene Entscheidungen in Bezug auf die Daten bzw. Datenverarbeitung treffen. Als Aufgabenübertragung gilt auch jede Tätigkeit, die (außerdem) mit einer unmittelbaren Außenwirkung des Auftragnehmers verbunden ist.

Das (Telefon-)Inkasso bzw. die Beitreibung privatrechtlicher und öffentlich-rechtlicher Forderungen würde aber einen solchen Ermessens- und Gestaltungsspielraum bzw. eine Außenwirkung erforderlich machen. Von einem Spielraum ist auszugehen, weil der Auftragnehmer selbständig an die Betroffenen herantreten müsste und somit eine Kontrolle durch die Kommune als Auftraggeberin im Prinzip nicht mehr vollumfänglich möglich wäre. Die Beitreibung solcher Forderungen würde über eine bloße Hilfstätigkeit hinausgehen und wäre nach der hier vertretenen Rechtsauffassung mit datenschutzrechtlichen Vorgaben nicht vereinbar.

Auch die Vermittlung von Ratenzahlungsvereinbarungen und Vergleichen oder die Prüfung eines berechtigten Interesses bzw. die Abwägung zwischen streitigen Interessen könnte aus den o.g. Gründen nicht im Rahmen eines Vertrages im Sinne von § 4 LDSG von einem Auftragnehmer erledigt werden.

Letztendlich ging es in jedem vorgetragenen Einzelfall um die Abgrenzung zwischen grundsätzlich möglicher Zusammenarbeit bei Hilfstätigkeiten und unzulässiger Aufgabenübertragung.

9.2 Meldewesen

9.2.1 Neue Bestimmungen im Melderecht

Im Zuge der Föderalismusreform wurde das Meldewesen im Jahr 2006 in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Hiervon hat der Bund am 28. Juni 2012 mit dem Gesetz zur Fortentwicklung des Meldewesens Gebrauch gemacht und in Art. 1 MeldFortG das Bundesmeldegesetz beschlossen, welches am 1. November 2015 in Kraft getreten ist. Das Melderechtsrahmengesetz sowie die bisherigen Meldegesetze der Länder einschließlich der hierauf basierenden landesrechtlichen Verordnungen sind damit außer Kraft getreten (vgl. 23. Tb., Tz. II-7.2.1).

Die Bemühungen der Datenschutzbeauftragten des Bundes und der Länder, datenschutzrechtliche Verbesserungen des neuen Melderechts zu erreichen, waren nur zum Teil erfolgreich (vgl. hierzu auch die Entschließung der Datenschutzkonferenz vom 22. August 2012 „Melderecht datenschutzkonform gestalten!“):

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels dürfen nur erteilt werden, wenn die Betroffenen in die Übermittlung für diesen Zweck eingewilligt haben. Die Anfragende müssen den Zweck angeben und das Vorliegen einer Einwilligung nachweisen, es sei denn, der Meldebehörde liegt die Einwilligung bereits vor.

- Melderegisterauskünfte zu gewerblichen Zwecken unterliegen einer ausdrücklichen Zweckbindung. Empfänger dürfen die erhaltenen Daten nur für die Zwecke verwenden, zu deren Erfüllung sie übermittelt wurden. Das neue Wiederverwendungsverbot für Daten, die zum Zwecke der geschäftsmäßigen Anschriftenermittlung für Dritte erhoben werden, soll vor einer unkontrollierten Weitergabe von Daten durch den Adresshandel schützen und den Aufbau von „Schattenmelderegistern“ verhindern.
- Leider nicht aufgegriffen wurde hingegen die datenschutzrechtliche Forderung, den Meldepflichtigen ein generelles Widerspruchsrecht in Bezug auf sonstige einfache Melderegisterauskünfte einzuräumen, sofern die Auskunftssuchenden kein rechtliches Interesse glaubhaft gemacht haben.
- Auch die Forderung, erweiterte Melderegisterauskünfte – z.B. über Geburts- und Sterbedaten, Angaben über den Familienstand und über den Ehegatten und Lebenspartnerin oder -partner sowie die oder den gesetzlichen Vertreter – vom Vorliegen eines rechtlichen Interesses abhängig zu machen, wurde nicht umgesetzt.
- Bei den Melderegisterauskünften in besonderen Fällen (z.B. Auskünfte an Presse oder Rundfunk über Alters- und Ehejubiläen und an Adressbuchverlage) wurde die zentrale datenschutzrechtliche Forderung, diese Weitergaben von der Einwilligung der Betroffenen abhängig zu machen, vom Gesetzgeber erneut nicht aufgegriffen (vgl. Tz. III-9.2.2). Es bleibt bedauerlicherweise bei den bisherigen Widerspruchsregelungen.
- Die Widerspruchsmöglichkeit gegen die Erteilung einfacher Melderegisterauskünfte über das Internet wurde gestrichen.
- Für die Betroffenen besteht weiterhin kein umfassender Auskunftsanspruch bei Melderegisterauskünften an Einzelpersonen auf herkömmlichem Weg.
- Die Hotelmeldepflicht für inländische Gäste, deren Abschaffung von den Datenschutzbeauftragten über Jahre hinweg immer wieder gefordert worden war, bleibt bestehen.
- Trotz datenschutzrechtlicher Kritik wurde die Vermieterbescheinigung bei der An- und Abmeldung von Mieterinnen und Mietern wieder eingeführt.

Das Bundesmeldegesetz weist den Ländern in einigen Bereichen eigene Regelungskompetenzen zu. Dies gilt insbesondere für regelmäßige und automatisierte Datenabrufe. Nachdem mit der Meldedaten-Übermittlungsverordnung sowie der Informationssystemabrufverordnung maßgebliche landesrechtliche Regelungen außer Kraft getreten sind, bedurfte es neuer rechtlicher Grundlagen auf Landesebene, um die bisherige Wahrnehmung melderechtlicher Aufgaben beizubehalten. Diese wurden mit dem Landesgesetz zur Ausführung des Bundesmeldegesetzes, das am 1. November 2015 in Kraft getreten ist, geschaffen (Artikel 1 des Landesgesetz zur Neuregelung des Melde-, Pass- und Ausweiswesens vom 21. Oktober 2015, GVBl. S. 365 ff.).

Eine regelmäßige Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgesellschaften darf nach den neuen Bestimmungen des Melderechts nur erfolgen, wenn sichergestellt ist, dass die Religionsgesellschaften ausreichende Maßnahmen zum Datenschutz getroffen haben (§ 42 Abs. 5 Satz 1 BMG). Gemäß § 42 Abs. 5 Satz 2 BMG hat die Feststellung hierüber eine durch Landesrecht zu bestimmende Behörde zu treffen. Dies ist in Rheinland-Pfalz das für das Melderecht zuständige Ministerium im Einvernehmen mit dem LfDI (vgl. § 6 AGBMG). Damit wird dem LfDI insoweit erstmals die Aufgabe zugewiesen, sich mit dem Datenschutz bei öffentlich-rechtlichen Religionsgesellschaften zu befassen. Da die Kirchen über eigene kirchliche Datenschutzbeauftragte verfügen und eigene kirchliche Datenschutzbestimmungen erlassen haben, ist es dem LfDI aufgrund fehlender Zuständigkeit grundsätzlich versagt, die Datenverarbeitung von Stellen zu prüfen, die sich in kirchlicher Trägerschaft befinden. Insofern handelt es sich bei der Feststellung nach § 42 BMG und der damit verbundenen Einbeziehung des LfDI um ein Novum. Im Berichtszeitraum fanden unter Federführung des Ministeriums des Innern, für Sport und Infrastruktur erste Gespräche mit den öffentlich-rechtlichen Religionsgesellschaften statt, um auszuloten, wie den gesetzlichen Anforderungen am besten entsprochen werden kann.

9.2.2 Veröffentlichungen von Jubiläumsdaten

Bei Pflichtangaben, wie dies im Bereich des Meldewesens der Fall ist, ist in Bezug auf die weitere Verwendung der erhobenen Informationen durch staatliche Stellen ein strenger Maßstab anzulegen. Dies

gilt umso mehr, wenn die Weitergabe der erhobenen Daten im Wege einer Veröffentlichung im Raum steht.

Aus datenschutzrechtlicher Sicht ist insoweit zu differenzieren, ob es sich auf Seiten des Übermittlungsempfängers um einen überschaubaren Personenkreis handelt oder ob die Veröffentlichung über das Internet erfolgt und somit weltweit abrufbar ist. Diese Differenzierung spielt auch in anderen Bereichen außerhalb des Meldewesens eine Rolle. Sie hängt damit zusammen, dass bei der Veröffentlichung im Internet ein deutlich höherer Verbreitungsgrad der Informationen erreicht wird und personenbezogene Daten dauerhaft und weltweit verfügbar gemacht werden. Mit Hilfe von Suchmaschinen ist eine Auffindbarkeit auch in archivierten Datenbeständen möglich, so dass sämtliche zu einer bestimmten Person vorhandenen Angaben gesammelt und – losgelöst vom ursprünglichen Informationszweck – zur Erstellung eines Persönlichkeitsprofils genutzt werden können.

Die dem LfDI vorliegenden zahlreichen Beschwerden gegen die Weitergabe von Jubiläumsdaten durch Meldeämter zeigen, dass viele Betroffene über ihr bestehendes Widerspruchsrecht trotz der öffentlichen Bekanntmachungen nicht unterrichtet sind.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher seit langem gefordert, die Weitergabe von Jubiläumsdaten durch Meldeämter von der Einwilligung der Betroffenen abhängig zu machen. Die Datenschutzkonferenz hat in einer Entschließung „Melderecht datenschutzkonform gestalten!“ vom 22. August 2012 hierzu ausgeführt:

> „…Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.“

Bedauerlicherweise hat der Bundesgesetzgeber diese Forderung im neuen Bundesmeldegesetz nicht berücksichtigt (vgl. Tz. III-9.2.1). Die jetzige Regelung in § 50 Abs. 2 BMG sieht vor, dass die Meldebehörde im Rahmen des ihr zustehenden Ermessens der Presse oder dem Rundfunk auf Verlangen Auskunft über Alters- oder Ehejubiläen von Einwohnerinnen und Einwohnern erteilen darf, sofern die Betroffenen einer Datenweitergabe nicht widersprochen haben.

Der LfDI hatte insoweit die Empfehlung ausgesprochen, dass Meldeämter im Rahmen ihrer Ermessensausübung von einer Veröffentlichung von Meldedaten im Internetangebot von Kommunen Abstand nehmen (vgl. 22. Tb., Tz. 10.2.1). Ebenso wurde vom LfDI eine Forderung der kriminalpolizeilichen Präventionsarbeit aufgegriffen und empfohlen, bei der Veröffentlichung in Printmedien auf die Bekanntgabe der Anschrift der Jubilarinnen und Jubilare zu verzichten. Diese Empfehlungen wurden vom Ministerium des Innern, für Sport und Infrastruktur mit Rundschreiben vom 22. April 2015 zusammengefasst.

9.3 Durchführung von Wahlen

Mit Anfragen, Beschwerden oder auch Entwürfen für Gesetzesänderungen muss sich der LfDI naturgemäß nur im engeren zeitlichen Zusammenhang mit Parlaments- und Kommunalwahlen befassen.

Vor jeder Wahl wird dabei die Melderegisterauskunft für Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen problematisiert. Diese erhalten, z.B. zum Versand von Erstwählerbriefen, über die Registerauskunft Vor-, Nachname, Anschrift sowie eine Alterskategorie zu den Bürgerinnen und Bürgern.

Bisher war immer gemäß § 35 Abs. 1 MG darauf zu verweisen, dass die o.g. Personengruppen im Zusammenhang mit Parlaments-, Kommunal- und Ausländerbeiratswahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über entsprechende Kontaktdaten erhalten.

Diese Auskunft ist in das Bundesmeldegesetz, das zum 1. November 2015 in Kraft getreten ist, übernommen worden (§ 50 Abs. 1 BMG).

Die Person oder Stelle, der diese Daten übermittelt wird, darf diese aber nur für den Zweck verwenden, zu dessen Erfüllung sie übermittelt wurden. Weiterhin sind die Daten spätestens einen Monat nach der Wahl zu löschen oder zu vernichten. Außerdem

räumt das Gesetz den Bürgerinnen und Bürgern das Recht ein, der Weitergabe ihrer Daten zu Wahlzwecken zu widersprechen.

Während des Berichtszeitraumes wurden dem LfDI noch weitere Sachverhalte zur Bewertung vorgelegt:

- Der Wahlausschuss einer Gemeinde hatte die Wählbarkeit eines Bewerbers für ein Amt zu prüfen. Konkret ging es dabei um die Frage, ob sich der Lebensmittelpunkt des Bewerbers in der Gemeinde befindet. Das Ergebnis der Prüfung hat der Wahlleiter der Gemeinde unter Nennung des Namens des Bewerbers im Internet veröffentlicht und im Rahmen seiner Mitteilung auch konkrete persönliche Lebensumstände mitgeteilt.
  Das Kommunalwahlgesetz bzw. die Kommunalwahlordnung sehen nur eine Bekanntmachung der Entscheidung des Wahlausschusses über die Zulässigkeit eines Wahlvorschlages und somit des Ergebnisses vor. Der Wahlleiter gibt die Entscheidung des Wahlausschusses im Anschluss an die Beschlussfassung bekannt (§ 29 Abs. 5 Satz 1 KWO) und macht die zugelassenen Wahlvorschläge mit den in § 25 Abs. 1 Satz 2 KWO bezeichneten Angaben öffentlich bekannt (§§ 30 Abs. 1 Satz 1, 70 KWO).
  Eine Information über die geprüften problematischen Gesichtspunkte ist nicht vorgesehen. Der Hinweis auf konkrete persönliche Lebensumstände sowie das Wohnumfeld des Wahlbewerbers war zur rechtmäßigen Erfüllung der in der Zuständigkeit des Wahlleiters liegenden Aufgaben nicht erforderlich und somit rechtswidrig.
  Die Veröffentlichung des Prüfungsergebnisses mit dem oben geschilderten Inhalt wurde daher gem. § 25 Abs. 1 Nr. 2 LDSG beanstandet.
- Weiterhin wurde problematisiert, ob es mit dem Grundsatz der geheimen Wahl zu vereinbaren ist, wenn bei Mehrheitswahl der Stimmzettel handschriftlich ausgefüllt wird. Gerade in kleineren Gemeinden könne es nicht ausgeschlossen werden, dass Wahlberechtigte von einem Mitglied des Wahlvorstandes aufgrund der Handschrift identifiziert werden.
  Nach einem Urteil des Oberverwaltungsgericht Rheinland-Pfalz (Az. 7 A 75/78) ist es jedoch keine Verletzung des Grundsatzes der geheimen Wahl, wenn die Stimmzettel handschriftlich (durch Aufschreiben des Namens des Gewählten) auszufüllen sind. Das Wesen der geheimen und freien Wahl bestehe darin, dass Wählerinnen und Wähler von Dritten unbeobachtet und ohne irgendeine Beeinflussung von außen bei der eigentlichen und entscheidenden Abstimmungshandlung, d.h. innerhalb der Wahlkabine, ihren Willen frei bekunden können.
- Im Zusammenhang mit der letzten Kommunalwahl wurde auch die Veröffentlichung von Wahlvorschlägen im Internet – zusätzlich zur Bekanntmachung in den Printmedien – aufgegriffen, da somit Daten wie das Geburtsdatum, Anschrift und Beruf mitgeteilt werden.
  Grundsätzlich ist die öffentliche Bekanntmachung von Wahlvorschlägen mit den in § 19 Abs. 1 KWG genannten Daten einer Bewerberin oder eines Bewerbers im von der Gemeinde festgelegten Veröffentlichungsorgan (Amtsblatt, Tageszeitung) aus Gründen der Transparenz zulässig (§ 30 Abs. 1 Satz 1 KWO).
  Aufgrund dieser Vorschriften dürfen die Wahlvorschläge der Öffentlichkeit aber nur insoweit zugänglich gemacht werden, als das für die ordnungsgemäße Durchführung der Wahl notwendig ist. Die öffentliche Bekanntgabe der Wahlvorschläge dient der Information der Wahlberechtigten und der Parteien und der jeweiligen kommunalen Gebietskörperschaft. Sie ist daher in örtlichem und zeitlichem Zusammenhang mit der jeweiligen Wahl zu sehen.
  Dabei ist aus datenschutzrechtlicher Sicht zu beachten, dass der Verbreitungsgrad von Informationen im Medium Internet einen deutlich höheren Umfang erreicht als dies bei einer Veröffentlichung in einem Amtsblatt, einer Broschüre oder einer regionalen Tageszeitung der Fall ist. Damit wird das informationelle Selbstbestimmungsrecht nicht unerheblich betroffen, weshalb es hier eines besonderen Augenmerks auf den Grundsatz der Datensparsamkeit bedarf.
  Diesen Erwägungen wurde für Landtagswahlen bereits insofern Rechnung getragen, als in der Landeswahlordnung folgende datenschutzfreundlichen Beschränkungen des Umfanges von Veröffentlichungen im Internet geregelt wurden:
  - Angabe lediglich des Geburtsjahres anstelle des Geburtstages;
  - Angabe lediglich des Wohnortes anstelle der Anschrift;

- Konkreter Zeitpunkt für die Löschung von Internetveröffentlichungen.

Da kein Anhaltspunkt dafür ersichtlich ist, warum die KWO in dieser Hinsicht nicht mit der Landeswahlordnung harmonisiert werden sollte, hat der LfDI um eine diesbezügliche Änderung der Kommunalwahlordnung gebeten. Der Landeswahlleiter hat diese Bitte insofern schon berücksichtigt, als in dem aktuellen Rundschreiben zur gleichzeitigen Durchführung von Kommunal-/Direktwahlen mit der Landtagswahl am 13. März 2016 entsprechende Hinweise zu den Internetveröffentlichungen bei Kommunalwahlen gegeben wurden.

9.4 Statistik

Im Datenschutzbericht 2010/2011 (vgl. 23. Tb., Tz. II-7.3) wurde über die „heiße Phase“ der ersten Volkszählung für die Bundesrepublik Deutschland seit 1981 (Ostdeutschland) bzw. 1987 (Westdeutschland) berichtet. Im Datenschutzbericht 2012/2013 (vgl. 24. Tb., Tz. III-7.3) wurde mit dem Hinweis auf die „Eckpunkte für eine datenschutzgerechte Volkszählung“ der BfDI bereits ein erster Ausblick auf den nächsten Zensus 2021 gegeben.

Zuletzt war im Hinblick auf laufende Verwaltungsgerichtsverfahren zur Klärung der Einwohnerzahlen einzelner Kommunen in verschiedenen Bundesländern von der Fortführung der Löschung der vorhandenen Hilfsmerkmale aus der abgeschlossenen Zensuserhebung seitens des dortigen Statistischen Landesamtes abgesehen worden, obwohl gemäß § 19 Abs. 1 Satz 3 Zensusgesetz 2011 die Hilfsmerkmale spätestens bis zum Stichtag, dem 9. Mai 2015, zu löschen waren.

In Rheinland-Pfalz konnten dagegen alle Datenbestände mit Hilfsmerkmalen fristgerecht gelöscht werden. Die auf methodische Fehler gestützte einzige Klage einer rheinland-pfälzischen Kommune wurde nicht weiter betrieben. In Rheinland-Pfalz waren aber auch nur sehr geringe Abweichungen zwischen den Ergebnissen der Fortschreibung auf Basis der Volkszählung 1987 und des Zensus 2011 festzustellen. Dies wird auf die in den Bundesländern unterschiedlichen Melderegistersysteme und deren jeweilige Datenqualität zurückgeführt.

Eine einheitliche Rechtsauffassung zu den im Zusammenhang mit der Pflicht zur Löschung der Hilfsmerkmale bei entgegenstehenden gerichtlichen Entscheidungen aufgeworfenen Fragen konnte allerdings nicht erzielt werden.

Während der Jahrestagung 2015 des Statistischen Landesausschusses wurde folgender Fahrplan für den Zensus 2021 vorgestellt:

- Grundsatzentscheidung der Innenministerkonferenz zum Rahmenwerk bis Ende 2015
- Vorbereitungsgesetz (Aufbau Anschriftenregister) bis Ende 2016
- Durchführungsgesetz bis Frühjahr 2019
- Länder-Ausführungsgesetze bis Ende 2019
- Aufbau Anschriftenregister 2021 ab Frühjahr 2017

Weiterhin wurde in diesem Rahmen darüber informiert, dass eine Evaluierung organisatorischer und rechtlicher Regelungen bis Anfang 2016 abgeschlossen sein soll. Mit deren Ergebnis werden sich die Datenschutzaufsichtsbehörden intensiv befassen müssen.

10. Justiz

10.1 Datenschutzrechtliche Aspekte bei der Herausgabe von Urteilsabschriften

Von verschiedenen Seiten wurde der LfDI um eine Einschätzung zu Reichweite und Grenzen des verfassungsrechtlich verbürgten Anspruchs auf Herausgabe von Urteilsabschriften gebeten. Die Anfragen beim LfDI betrafen Anträge von Medienvertreterinnen und -vertretern auf Herausgabe strafgerichtlicher Verurteilungen.

Ausgangspunkt der Überlegungen zur Überlassung von Urteilsabschriften ist dabei die maßstabsbildende Entscheidung des Bundesverwaltungsgerichts vom 26. Februar 1997 (Az. 6 C 3/96). Das Gericht hat darin eine verfassungsunmittelbare „Rechtspflicht der Gerichtsverwaltung zur Publikation veröffentlichungswürdiger Gerichtsentscheidungen“ hergeleitet. Hierzu zählten alle Entscheidungen, „an deren Veröffentlichung die Öffentlichkeit ein Interesse hat oder haben kann“. Das Bundesverfassungsgericht hat diese Rechtsprechung mit seinem Beschluss vom 14. September 2015 (Az. 1 BvR 857/15) bestätigt und damit noch einmal die verfassungsrechtliche Bedeutung des Zugangs zu Urteilsabschriften betont.

Der LfDI vertritt insoweit die Auffassung, dass sich der mit der aufgezeigten verfassungsunmittelbaren Verpflichtung zur Veröffentlichung von Urteilsabschriften korrespondierende individuelle Überlassungsanspruch grundsätzlich nach den einfachgesetzlichen Informationszugangsansprüchen des Presserechts bzw. des jeweiligen Prozessrechts (z.B. § 6 LMG, § 475 StPO) richtet.

Dabei gilt, dass Anfragen der Presse regelmäßig dazu führen, dass eine Entscheidung als veröffentlichungswürdig im Sinne der Rechtsprechung des Bundesverwaltungsgerichts anzusehen ist. Maßgeblich ist hierbei, dass die Presse selbst darüber entscheidet, welche Informationen sie für relevant erachtet.

Soweit die maßgeblichen Informationszugangsbestimmungen (nur) einen Auskunftsanspruch gewähren und die Form der Auskunft in das Ermessen der Behörde gestellt ist, kommt es nach Auffassung des LfDI in der Regel zu einer Ermessensreduktion auf Null dahingehend, dass der verfassungsrechtlichen Pflicht zur Herausgabe einer Entscheidung nur mit deren Überlassung und nicht mit einer Auskunftserteilung über ihren Inhalt entsprochen werden kann.

Da eine wirksame Anonymisierung von Urteilsabschriften regelmäßig scheitert, ist im Rahmen der einfachgesetzlichen Übermittlungsgrundlagen stets eine mitunter komplizierte Abwägungsentscheidung zu treffen, ob und in welchem Umfang ein Urteil zugänglich gemacht werden kann. Es geht insoweit um einen angemessenen Ausgleich zwischen den Persönlichkeitsrechten und dem informationellen Selbstbestimmungsrecht der Betroffenen einerseits und der Pressefreiheit bzw. der eingangs dargestellten rechtsstaatlichen Transparenzverpflichtung der Gerichte andererseits. Dabei sind die verfassungsrechtlichen Rechtspositionen im Einzelfall unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes und des Verwendungszusammenhangs der Daten gegeneinander abzuwägen.

Folgenden Aspekten kann nach Auffassung des LfDI besonderes Gewicht zukommen:

- Je näher die Daten zum unantastbaren Persönlichkeitskern stehen und je geringer ihr Sozialbezug daher ist, desto intensiver ist der Schutz gegenüber staatlichen Eingriffen. Gesundheitsdaten z.B. genießen vor diesem Hintergrund einen besonderen Schutz (vgl. Verwaltungsgerichtshof Baden-Württemberg, Beschluss vom 23. Juli 2010, Az. 1 S 501/10). Dabei ist freilich bei strafgerichtlichen Urteilen zu berücksichtigen, dass ein Kernbereichsbezug fehlen kann, wenn es sich um Angaben handelt, die auf die Straftat bezogen sind (vgl. Beschluss des Bundesverfassungsgerichts vom 14. September 2015, Az. 1 BvR 857/15);
- inwieweit personenbezogene Daten von Opfern und Zeugen betroffen sind;
- ob bzw. in welchem Maß das Resozialisierungsinteresse (vgl. hierzu bereits BVerfGE 35, 202) durch die Herausgabe der Urteilsabschrift beeinträchtigt werden;
- welche Bedeutung die Straftat hat und in welchem Maß die Rechtsordnung und individuelle Rechtsgüter durch sie verletzt worden sind;

- die zeitgeschichtliche Bedeutung eines Urteils;
- inwieweit in dem Urteil (rechts-)grundsätzliche Fragen aufgeworfen werden.

Der LfDI erkennt insoweit an, dass das Gewicht der verfassungsrechtlich begründeten besonderen Transparenzverpflichtung der Justiz regelmäßig dazu führt, dass auf einen entsprechenden Antrag hin Urteilsabschriften an Pressevertreterinnen und -vertreter herauszugeben sind.

Dem informationellen Selbstbestimmungsrecht der Betroffenen ist dann aber dadurch Rechnung zu tragen, dass (ggf. umfangreiche) inhaltliche Schwärzungen im Urteilstext vorgenommen werden. Eingriffe in das informationelle Selbstbestimmungsrecht der Einzelnen sind auf das Erforderliche zu begrenzen. Das bedeute konkret, dass z.B. Feststellungen zur Person der Verurteilten in der Regel nicht zu übermitteln sind.

10.2 Strafprozessuale Ermittlungsbefugnisse und Datenschutz

Der LfDI hat sich im Berichtszeitraum zu verschiedenen strafprozessualen Ermittlungsmaßnahmen datenschutzrechtlich geäußert. Er hat sich dabei für eine Verbesserung der Normenklarheit sowie für eine Stärkung der Transparenz für datenschutzrechtlich Betroffene eingesetzt.

In einer Stellungnahme gegenüber dem Ministerium der Justiz und für Verbraucherschutz hat der LfDI ausgeführt, dass nach seiner Einschätzung jedenfalls die seinerzeitigen technischen Möglichkeiten eine rechtkonforme Durchführung der sog. Quellen-TKÜ (vgl. 24. Tb., Tz. III-4.1.8) nicht ermöglichen. Er hat ferner zum Ausdruck gebracht, dass er hierfür eine ausdrückliche Rechtsgrundlage für erforderlich erachtet.

Gleiches gilt für den Einsatz sog. stiller SMS, die nach ihrem Versand durch die Ermittlungsbehörden beim SMS-Empfänger zwar nicht angezeigt werden und auch kein Empfangssignal auslösen, die aber gleichwohl Verbindungsdaten generieren, die ausgewertet werden sollen. Die Grundsätze der Normenklarheit und –bestimmtheit lassen nach Auffassung des LfDI eine ausdrückliche Rechtsgrundlage als jedenfalls wünschenswert erscheinen. Gleichzeitig hat er aber das ermittlungstaktische Bedürfnis für stille SMS anerkannt und wird deren Einsatz nicht beanstanden, soweit dieser im Rahmen der strengen Voraussetzungen einer Telekommunikationsüberwachung nach §§ 100a, 100b StPO erfolgt.

In Bezug auf die Funkzellenabfrage (vgl. hierzu § 100g Abs. 3 n.F. StPO) hat der LfDI unter Hinweis auf den Beschluss der Datenschutzkonferenz vom 27. Juli 2011 „Funkzellenabfrage muss eingeschränkt werden!“ besonders auf die Beachtung des Verhältnismäßigkeitsgrundsatzes hingewiesen.

Da nicht individualisierte Funkzellenabfragen zu massenhaften Datenerhebungen führen, hat der LfDI weiterhin angeregt, jenseits des § 101 Abs. 4 StPO, der die individuelle Benachrichtigung der datenschutzrechtlich Betroffenen regelt, hiervon aber weitgehende Ausnahmen zulässt, neue Benachrichtigungsinstrumente in Betracht zu ziehen. Zu denken ist z.B. an eine Information der Öffentlichkeit im Rahmen der staatsanwaltschaftlichen Pressearbeit. Überdies sollte der Einsatz des in Berlin bereits diskutierten SMS-Benachrichtigungssystem geprüft werden, bei dem Bürgerinnen und Bürger durch eine SMS an eine behördliche Stelle den Wunsch dokumentieren können, per SMS über eine Erhebung ihrer Daten im Rahmen einer Funkzellenabfrage informiert zu werden (vgl. hierzu Drs. des Abgeordnetenhauses Berlin 17/2404).

Die im Berichtszeitraum angekündigte Änderung der Richtlinien für das Strafverfahren und das Bußgeldverfahren betrifft die Öffentlichkeitsfahndung im Internet und in sozialen Netzwerken. Der LfDI bewertet diese Änderungen unter Hinweis auf den Beschluss der Datenschutzkonferenz vom 27. März 2014 „Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich“ kritisch und regt nach wie vor an, für diesen Problemkreis eine spezialgesetzliche Regelung zu schaffen.

Der LfDI hat sich ferner intensiv mit dem Thema IP-Tracking auseinandergesetzt. Es handelt sich dabei um ein strafprozessuales Ermittlungsinstrument, mit dem Internetnutzerinnen und -nutzer über ihre IP-Adresse identifiziert werden sollen. Es bestehen verschiedene Formen des IP-Trackings. Beim sog. Dokumenten- und E-Mail-Tracking werden z.B. in einer E-Mail oder einem bestimmten Dokument sog.

„webbugs“, das heißt kleine unsichtbare Zählpixel, eingebaut, die beim Öffnen einer E-Mail oder eines Dokuments nachgeladen werden. Bei diesem Vorgang wird dann die IP-Adresse mitgeteilt.

In Rechtsprechung, Literatur und Praxis ist umstritten, auf welcher Rechtsgrundlage die genannten Varianten des Dokumenten- und E-Mail-Trackings gestützt werden können. Während die rheinland-pfälzischen Sicherheitsbehörden den Einsatz des IP-Trackings unter § 100h StPO subsumieren, erachtet der LfDI in Übereinstimmung mit einem Beschluss des Ermittlungsrichters beim Bundesgerichtshof (vgl. hierzu BGH (Ermittlungsrichter), Beschluss vom 23. September 2014, Az. 1 BGs 210/14) § 100g StPO für einschlägig. Zwar ist es zutreffend, dass es beim IP-Tracking regelmäßig nicht zu einem Eingriff in Art. 10 GG (Fernmeldegeheimnis) kommt, weil die Ermittlungsbehörden selbst Kommunikationspartner werden und den Kommunikationsvorgang damit nicht von außen überwachen; § 100g StPO knüpft nach seinem Wortlaut aber lediglich an die bei einem Telekommunikationsvorgang anfallenden Verkehrsdaten an und verknüpft diese mit einer erhöhten Eingriffsschwelle.

Die Beachtung dieser im Vergleich zu § 100h erhöhten Voraussetzungen des § 100g StPO (z.B. Richtervorbehalt) überzeugt aus Sicht des LfDI auch wertungsmäßig. Unter Berücksichtigung der Heimlichkeit des Vorgangs – verknüpft mit einer Täuschung der Betroffenen – handelt es sich nämlich um einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht, der in seiner Intensität mit dem von § 100g StPO erfassten Regelfall vergleichbar ist. So liegt zwar formal kein Eingriff in Art. 10 GG vor, die Betroffenen selbst allerdings gehen nicht davon aus, dass sie mit einer Ermittlungsbehörde kommunizieren und glauben ihr Verhalten daher durch das Fernmeldegeheimnis geschützt. Sie bedürfen daher des Schutzes nach § 100g StPO.

10.3 Datenschutzrechtliche Kontrollzuständigkeit des LfDI im Gerichtsvollzieherwesen

Durch das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung erhielten Gerichtsvollzieherinnen und Gerichtsvollzieher mit Wirkung zum 1. Januar 2013 die Möglichkeit, nach Maßgabe von § 802l Abs. 1 Nr. 2 ZPO beim Bundeszentralamt für Steuern Kontenabfragen über Schuldnerinnen und Schuldner durchzuführen. Presseberichten zufolge hat sich die Anzahl der Kontenabfragen seit 2012 jährlich jeweils fast verdoppelt. Für das Jahr 2014 registrierte das Bundeszentralamt für Steuern z.B. 230.000 erledigte Kontenabrufe.

Vor diesem Hintergrund hat der LfDI die Prüfung von Kontenabfragen durch rheinland-pfälzische Gerichtsvollzieherinnen und Gerichtsvollzieher angekündigt. Hiergegen wurden allerdings zunächst Zuständigkeitsbedenken geltend gemacht. Eingewandt wurde insbesondere, die Tätigkeit von Gerichtsvollzieherinnen und Gerichtsvollziehern sei nach § 24 Abs. 2 LDSG einer externen Datenschutzkontrolle entzogen, weil das Zwangsvollstreckungsverfahren materiell der Rechtsprechung zuzurechnen sei.

Der LfDI begrüßt insoweit, dass das Ministerium der Justiz und für Verbraucherschutz Rheinland-Pfalz die geltend gemachten Bedenken nicht teilt und mit den Kontrollen Ende 2015 begonnen werden konnte. Nach § 24 Abs. 1 Satz 1 LDSG überprüft der LfDI die Einhaltung der Bestimmungen des Landesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz bei den in § 2 Abs. 1 LDSG bezeichneten öffentlichen Stellen. Hierzu gehören ausdrücklich auch die Organe der Rechtspflege. Die Bestimmung des § 802l Abs. 1 Nr. 2 ZPO ist ferner eine spezialgesetzlich normierte Datenerhebungsbefugnis und damit „andere Vorschrift über den Datenschutz“ nach § 24 Abs. 1 Satz 1 LDSG.

Die Ausnahmevorschrift des § 24 Abs. 2 LDSG ist bei Gerichtsvollzieherinnen und Gerichtsvollziehern nicht einschlägig. Danach unterliegen die Gerichte und der Rechnungshof einer Kontrolle des LfDI nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Fraglich ist nach Auffassung des LfDI bereits, ob Gerichtsvollzieherinnen und Gerichtsvollzieher tatbestandlich unter den Begriff „Gericht“ subsumiert werden können (vgl. hierzu Beschluss des Oberlandesgerichts München vom 5. Februar 2013, Az. 9 VA 17/12). Jedenfalls aber handelt es sich bei der in Rede stehenden Kontenabfrage um eine Verwaltungsaufgabe.

Der Sinn und Zweck des § 24 Abs. 2 LDSG besteht in der Absicherung der richterlichen Unabhängigkeit

(Art. 97 Abs. 1 GG). Der Tätigkeit der Gerichtsvollzieherinnen und Gerichtsvollzieher im Rahmen eines Vollstreckungsverfahrens fehlt allerdings ein Bezug zur in Art. 97 GG geschützten richterlichen Unabhängigkeit und sie wird damit auch nicht von § 24 Abs. 2 LDSG erfasst.

Erste Ergebnisse der begonnen Prüfung zeigen, dass die geprüften Gerichtsvollzieherinnen und Gerichtsvollzieher für die sich stellenden Datenschutzfragen sensibilisiert sind. Eine abschließende Bewertung der Prüfung war zum Ende des Berichtszeitraums allerdings noch nicht möglich.

10.4 Zusammenarbeit von Polizei und Gerichtsvollziehern im Vorfeld von Vollstreckungsmaßnahmen

Veranlasst durch die Tötung eines Gerichtsvollziehers bei der Vollstreckung eines Räumungstitels in Baden-Württemberg kamen Forderungen nach einer engeren Zusammenarbeit zwischen Polizei und Gerichtsvollzieherinnen und Gerichtsvollziehern im Rahmen der Zwangsvollstreckung auf. Insbesondere um die Gewaltbereitschaft und das Aggressionspotenzial einer Schuldnerin oder eines Schuldners abschätzen zu können, wurde gefordert, für Gerichtsvollzieherinnen und Gerichtsvollzieher sog. Sicherheitsabfragen bei den zuständigen Polizeibehörden zu ermöglichen.

Das durch das Ministerium der Justiz und für Verbraucherschutz an den LfDI herangetragene Anliegen hat der LfDI dem Grunde nach unterstützt. Da die Abfragen aber mit einem Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Schuldnerinnen und Schuldner verbunden sind, erachtet der LfDI im Sinne einer ausreichenden Normenklarheit und –bestimmtheit eine spezialgesetzliche Regelung im Rahmen der Zivilprozessordnung als jedenfalls wünschenswert.

Dem Erlass einer Verwaltungsvorschrift zur Regelung der Sicherheitsabfragen ist der LfDI aber nicht entgegengetreten. Eine Datenerhebungsbefugnis lässt sich bei einem im Vollstreckungsverfahren zu erwartenden Widerstand durch die Schuldnerin oder den Schuldner auf der Grundlage von § 12 Abs. 1, 4 Nr. 1 LDSG i.V.m. § 758 Abs. 3 ZPO begründen. Aus Sicht des LfDI war es aber wichtig, dass auf dieser Grundlage nur eine Abfrage in begründeten Einzelfällen zulässig ist und die Polizei den Gerichtsvollzieherinnen und Gerichtsvollziehern nur eine Gefahrenprognose mitteilt. Dem wird die Verwaltungsvorschrift „Zusammenarbeit zwischen den Gerichtsvollzieherinnen und Gerichtsvollziehern und der Polizei“, wie sie mit Wirkung zum 1. Oktober 2014 in Kraft getreten ist, gerecht.

10.5 Gemeinsames Vollstreckungsportal der Länder

In dem Gemeinsamen Vollstreckungsportal der Länder werden die bundesweiten Daten aus den Schuldnerverzeichnissen nach §§ 882b ff. ZPO zum kostenpflichtigen Abruf bereitgestellt. Im Rahmen der Umsetzung dieser aus dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung mit Wirkung zum 1. Januar 2013 bestehenden Verpflichtung hat der LfDI im Berichtszeitraum zu verschiedenen Einzelfragen Stellung genommen. So hat er sich unter Hinweis auf die Entschließung der Datenschutzkonferenz vom 7. Februar 2012 „Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke“ für die Erhöhung der Treffergenauigkeit bei Abfragen sowie das Einsichtsrecht des Betroffenen nach § 882f Satz 1 Nr. 6 ZPO ausgesprochen.

10.6 Datenverarbeitungen beim Sozialdienst der Justiz

Im Rahmen eines Anhörungsverfahrens zum Thema „Anforderungen an eine moderne und effiziente Gestaltung von Bewährungshilfe, Gerichtshilfe, Führungsaufsicht, insbesondere im Hinblick auf das Übergangsmanagement“ beim Rechtsausschuss des Landtages Rheinland-Pfalz hat der LfDI einzelne Datenverarbeitungsszenarien des Sozialdienstes der Justiz (Bewährungshilfe, Gerichtshilfe, Führungsaufsicht) näher beleuchtet. Schwerpunkt der Anhörung bildete der Datenaustausch zwischen den sozialen Diensten und den Einrichtungen des Justizvollzugs.

In seiner Stellungnahme, die als Vorlage 16/4948 unter dem Link http://www.landtag.rlp.de/landtag/vorlagen/4948-V-16.pdf abgerufen werden kann, hat der LfDI zunächst dargelegt, dass Datenverar-

beitungsbestimmungen für den Sozialdienst der Justiz in unterschiedlichen Spezialgesetzen abgebildet werden. So finden sich z.B. für die Bewährungshilfe Regelungen in § 56d StGB und für die Führungsaufsicht in § 68a StGB. Darüber hinaus kennt die Strafprozessordnung mit den § 483 ff. StPO Datenverarbeitungsbestimmungen (strafprozessuale Dateiregeln), die sich ausdrücklich auf die sozialen Dienste beziehen.

Vor diesen Hintergrund hat der LfDI festgehalten, dass bereits der derzeitige Rechtsrahmen bei einem komplexen Ineinandergreifen verschiedener Regelungssysteme eine Vielzahl von Datenübermittlungen ermöglicht. Er hat sich aber dennoch, insbesondere zur Verbesserung der Rechts- und Handlungssicherheit für die Beschäftigten des Sozialdienstes der Justiz, für eine einheitliche Gesamtkodifikation der Datenverarbeitungen durch den Sozialdienst der Justiz ausgesprochen. Dies auch deshalb, weil Beschäftigte der sozialen Dienste regelmäßig als Berufsgeheimnisträger einzustufen sind und sich bei der Offenbarung dienstlich erlangter Informationen ggf. strafbar machen (§ 203 StGB).

Wegen der bereits bestehenden bundesrechtlichen Datenverarbeitungsbestimmungen hat er sich für eine bundeseinheitliche Regelung ausgesprochen. Da eine solche – angesichts bereits vorliegender, allerdings nicht weiterverfolgter Gesetzesentwürfe (vgl. z.B. BT-Drs. 18/2012) – nicht zu erwarten war, wurde auch eine Regelung durch den Landesgesetzgeber angeregt. Durchgreifende kompetenzrechtliche Probleme bestehen nach Auffassung des LfDI insoweit nicht, da die Regelungen zu den sozialen Diensten zur konkurrierenden Gesetzgebung zählen und der Bundesgesetzgeber erkennbar keine abschließende Datenschutzkodifikation vorgenommen hat.

Entsprechend hat der LfDI den Entwurf eines Landesgesetzes zur Änderung des Landesgesetzes über den Sozialdienst der Justiz begrüßt, das der Landtag am 22. Dezember 2015 beschlossen hat. Danach wird das Gesetz über den Sozialdienst der Justiz um eine Datenschutzbestimmung (§ 5) ergänzt. Diese lautet:

> Für die Verarbeitung personenbezogener Daten im Sinne des § 3 Abs. 1 des Landesdatenschutzgesetzes (LDSG) durch den Sozialdienst der Justiz gelten, soweit nicht Bundesrecht dies ausdrücklich im Einzelnen regelt, die Bestimmungen des Landesdatenschutzgesetzes mit folgenden Maßgaben:
>
> 1. eine Erhebung personenbezogener Daten, einschließlich besonderer Arten im Sinne des § 3 Abs. 9 LDSG, bei Dritten ist auch bei Vorliegen der Voraussetzungen des § 12 Abs. 3 Nr. 2 LDSG zulässig,
> 2. die Übermittlung personenbezogener Daten, einschließlich besonderer Arten im Sinne des § 3 Abs. 9 LDSG, an Stellen des Justiz- und Maßregelvollzugs ist zulässig, wenn die Daten rechtmäßig vom Sozialdienst der Justiz im Rahmen seiner Aufgabenerfüllung erhoben worden sind und ihre Kenntnis für den Vollzug der Freiheitsentziehung oder der nachgehenden Betreuung erforderlich ist.

Mit dieser Bestimmung werden nicht nur Datenübermittlungen zwischen dem Sozialdienst der Justiz und den Stellen des Justiz- und Maßregelvollzugs auf eine ausreichend klare und bestimmte Rechtsgrundlage gestellt, sondern darüber hinaus Klarheit in Bezug auf die maßgeblichen Bestimmungen bei der Datenerhebung durch die sozialen Dienste erzielt. Soweit es hierbei zu einer Abweichung vom Direkterhebungsgrundsatz kommt (§ 5 Nr. 1), ist diese sachlich gerechtfertigt. Die Norm bildet zutreffend ab, dass die Ermittlungsfunktion der Gerichtshilfe und die Überwachungsaufgaben von Bewährungshilfe und Führungsaufsichtsstellen regelmäßig auf Datenerhebungen bei Dritten angewiesen sind.

10.7 Datenübermittlungen auf der Grundlage des NATO-Truppenstatuts an die Rechtsverbindungsstelle der US-amerikanischen Streitkräfte durch rheinland-pfälzische Staatsanwaltschaften

Veranlasst durch eine Eingabe hat sich der LfDI im Berichtszeitraum mit der Frage beschäftigt, inwieweit Verfahrensabgaben rheinland-pfälzischer Staatsanwaltschaften auf der Grundlage des NATO-Truppenstatuts an die Rechtsverbindungsstelle der US-Streitkräfte zulässig sind, wenn sich eine an die hiesige Staatsanwaltschaft adressierte Strafanzeige gegen Mitglieder der amerikanischen Streitkräfte richtet.

Der LfDI hat hierzu zunächst festgestellt, dass aus dem Postulat der engen Zusammenarbeit zwischen bundesdeutschen Stellen und den Stellen eines NATO-Entsendestaates (Art. 3 Abs. 1, 2 ZA-NTS i.V.m. Art. VII Abs. 6 a NTS) – vorliegend also der USA – eine spezialgesetzliche Datenübermittlungsgrundlage abgeleitet werden kann. Die Übermittlung personenbezogener Daten ist daher zulässig, soweit sie zur Erfüllung des Vertragszwecks des NATO-Truppenstatuts erforderlich ist.

Grundsätzlich können aus Sicht des LfDI damit auch die mit einer Verfahrensabgabe einhergehenden Datenübermittlungen auf die Bestimmungen des NATO-Truppenstatuts gestützt werden. Gleichwohl ist wie bei jeder Datenübermittlung stets im Einzelfall zu prüfen, in welchem Umfang sie konkret erforderlich ist. Da eine Datenübermittlung einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen begründet, kann es aus Gründen der Verhältnismäßigkeit geboten sein, diese im Umfang zu begrenzen.

Im konkreten Fall hat sich der LfDI daher für die Schwärzung des Namens des Anzeigeerstatters eingesetzt. Gründe hierfür waren, dass die Anzeige erkennbar politisch motiviert und der Anzeigeerstatter nicht persönlich betroffen war. Ferner verfügte er nicht über besondere Kenntnisse, die ihn z.B. als Zeugen qualifiziert hätten. Zwar konnte insoweit keine Einigkeit mit den Justizbehörden erzielt werden. Der LfDI wird sich aber auch zukünftig – im Hinblick auf den konkreten Fall auch bestärkt durch die Safe Harbor-Entscheidung des Europäischen Gerichtshofs (vgl. Tz. I-1.4, I-1.5) – für eine strenge Beachtung des Erforderlichkeitsgrundsatzes bei der Datenübermittlung im Rahmen von internationalen Verfahrensabgaben einsetzen.

11. Verbraucherschutz

11.1 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts

Am 17. Dezember 2015 hat der Bundestag das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts verabschiedet. Kern dieses Artikelgesetzes bildet aus datenschutzrechtlicher Sicht die Erweiterung des Unterlassungsklagegesetzes. Schon bisher konnten anspruchsberechtigte Stellen (§ 3 UKlaG), wozu z.B. die Verbraucherzentralen und die Industrie- und Handelskammern gehören, Unternehmen auf Unterlassung in Anspruch nehmen, wenn diese Vorschriften zuwidergehandelt haben, die dem Schutz der Verbraucherinnen und Verbraucher dienen.

Mit § 2 Abs. 2 Nr. 11 UKlaG wird künftig klargestellt, dass auch die Regelungen zum Datenschutz Verbraucherschutzbestimmungen im Sinne des Unterlassungsklagegesetzes sein können. Konkret werden durch die Novellierung jene Vorschriften erfasst, „welche die Zulässigkeit regeln

a) der Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer oder
b) der Verarbeitung oder der Nutzung personenbezogener Daten, die über einen Verbraucher erhoben wurden, durch einen Unternehmer,
wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden.“

Neu eingeführt wurde auch ein Beseitigungsanspruch nach den entsprechenden Datenschutzgesetzen (Berichtigung, Sperrung und Löschung), der neben den Unterlassungsanspruch tritt.

Der LfDI hat das Gesetzgebungsvorhaben in einer Stellungnahme ausdrücklich befürwortet. Die Erweiterung des Unterlassungsklagegesetzes ist aus seiner Sicht ein wichtiger Baustein, um das informationelle Selbstbestimmungsrecht von Betroffenen in einer sich rasant digitalisierenden Welt noch effektiver zu schützen. Hinsichtlich der vom Unterlassungsklagegesetz in Bezug genommenen Datenschutzbestimmungen hatte der LfDI gar für einen erweiterten Anwendungsbereich des § 2 Abs. 2 Nr. 11 UKlaG plädiert. So können z.B. auch die Bestimmungen zum technisch-organisatorischen Datenschutz nach seinem Verständnis verbraucherschützenden Charakter haben.

Da die neu geschaffenen Klagemöglichkeiten den Aufgabenbereich der Datenschutzaufsichtsbehörden tangieren, hat sich der LfDI dafür ausgesprochen, diesen die Möglichkeit zu eröffnen, ihre datenschutzrechtliche Expertise im Rahmen der anhängigen Klageverfahren einbringen zu können. Konkret hat er die Beteiligung der Datenschutzaufsichtsbehörden nach dem Vorbild der Beteiligung der Bundesanstalt für Finanzdienstleistungsaufsicht bei Klagen in Versicherungsangelegenheiten (§ 8 Abs. 2 UKlaG) angeregt. Insoweit begrüßt der LfDI die in § 12a UKlaG geregelte Anhörung der zuständigen Datenschutzaufsichtsbehörde durch das angegangene Gericht.

Aus Sicht des LfDI trägt diese Beteiligungsform auch dazu bei, die am Gesetz geübte Kritik, es komme zu einer Rechtswegzersplitterung (nämlich zivilrechtlicher Verfahren im Rahmen der Verbandsklage und verwaltungsgerichtlicher Verfahren bei Klagen gegen Maßnahmen der Aufsichtsbehörden), abzumildern.

11.2 Marktwächter „Digitale Welt“ der Verbraucherzentralen

Der LfDI begrüßt die Einrichtung eines sog. Marktwächters „Digitale Welt“, der als neues Instrument der Verbraucherschutzpolitik bei den Verbraucherzentralen eingerichtet wird. Das sich noch in der Aufbauphase befindliche Projekt dient dem Zweck, die mitunter unübersichtlichen und komplexen Marktstrukturen wie man sie im Bereich der Digitalwirtschaft beobachten kann, systematisch zu analysieren und ggf. bestehende Missstände aufzudecken.

Die verbraucherrelevanten Problemfelder – unter Einbeziehung von Datenschutzfragen – sollen sich

aus den Beratungsfällen und speziellen Marktuntersuchungen der Verbraucherzentralen ergeben. Defizite sollen so bereits frühzeitig erkannt und Verbraucherinnen und Verbraucher effektiv informiert werden. Daneben sollen die gewonnenen Erkenntnisse in den politischen Diskurs eingebracht und den Datenschutzaufsichtsbehörden für ihre Aufsichtstätigkeit zur Verfügung gestellt werden.

Da die Verbraucherzentrale Rheinland-Pfalz im Rahmen des Marktwächters „Digitale Welt“ den Bereich „Digitale Güter“, zu denen z.B. E-Books, MP3s und Apps gehören, verantwortet, war der LfDI im Dezember 2014 Teilnehmer an einem runden Tisch, bei dem die Möglichkeiten einer strukturierten Zusammenarbeit zwischen Datenschutzaufsichtsbehörden und den Verbraucherzentralen erörtert wurden. Der LfDI hat aus diesem Anlass die Einrichtung des Marktwächters ausdrücklich begrüßt. In einer sich rasant digitalisierenden Umwelt werden Fragen des Verbraucherdatenschutzes immer wichtiger. Aus dem Marktwächter „Digitale Welt“ können sich daher wertvolle Erkenntnisse für die Aufsichtsbehörden ergeben.

Institutionell wurde in der Zwischenzeit ein Beirat beim Marktwächter „Digitale Welt“ eingerichtet. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg hat den Beiratsvorsitz für den Marktwächter „Digitale Welt“ übernommen und vertritt darin die Datenschutzaufsichtsbehörden.

11.3 Bargeld in der digitalen Gesellschaft – Anachronismus oder gedruckte Freiheit? Eine Kooperationsveranstaltung des LfDI mit der Verbraucherzentrale Rheinland-Pfalz

In Rheinland-Pfalz besteht seit langer Zeit eine enge Kooperation zwischen der Verbraucherzentrale und dem LfDI. Da das Zusammenwirken von Verbraucher- und Datenschützerinnen und --schützern in einer sich rasant digitalisierenden Welt immer wichtiger wird, kooperieren der LfDI und die Verbraucherzentrale Rheinland-Pfalz auch im Rahmen von gemeinsamen Veranstaltungsprojekten. Die Zukunft des Bargelds in der digitalen Gesellschaft war Gegenstand einer Podiumsdiskussion, welche die Verbraucherzentrale Rheinland-Pfalz und der LfDI im Rahmen des Kunst- und Kulturprojekts #watch22 (vgl. Tz. II-3) ausgerichtet haben.

Zu den Freiheitsthemen der Zukunft wird auch die Frage gehören, welche Rolle das Bargeld in der digitalen Zukunft spielen wird. Zwar steht die Abschaffung des Bargeldes wohl nicht unmittelbar bevor. In Zeiten, in denen Negativzinsen für Sparerinnen und Sparer diskutiert werden, das bargeldlose Zahlen dank des technischen Fortschritts immer einfacher und bequemer wird und eine ernstzunehmende Debatte über eine Obergrenze für das Zahlen mit Bargeld eingesetzt hat, werden aber die entscheidenden Weichen für eine bargeldlose Zukunft gestellt.

Der Datenschutzbezug ist dabei vielleicht nicht auf den ersten Blick ersichtlich. Wenn man sich aber die Folgen einer bargeldlosen Zukunft vor Augen führt, wird schnell deutlich, dass der digitale Zahlungsverkehr geeignet ist, einen Menschen weitgehend gläsern zu machen. Wenn jeder Bezahlvorgang jedenfalls potenziell nachvollziehbar ist, bleibt das nicht ohne Auswirkungen auf die Freiheit eines jeden Einzelnen. Der Anpassungsdruck wird groß, wenn sich unsere Krankenversicherung plötzlich auch für unseren Warenkorb interessiert und ernährungsbedingte Risikozulagen nach dem Gemüseanteil berechnet. Umso wichtiger ist es also, sich auch aus Sicht des Daten- und Verbraucherschutzes mit dem Bargeld zu beschäftigen.

Thematisch wurde die Veranstaltung mit einem Vortrag des früheren Chefredakteurs der Wirtschafts-Woche und Vorsitzenden der Ludwig-Erhard-Stiftung, Roland Tichy, eingeleitet. Tichy sprach sich deutlich gegen die Abschaffung des Bargelds aus und lieferte damit die Thesen für die sich anschließende Podiumsdiskussion. Zusammen mit Roland Tichy diskutierten Wirtschaftsministerin Eveline Lemke, der Head of Client Cluster Visa Europe, Hans Bernhard Beykirch, und Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands, die Vor- und Nachteile einer bargeldlosen Zukunft.

Tenor des Abends war: Das bargeldlose Zahlen ist Ausdruck unserer digitalen Gesellschaft. Aber auch in dieser gelten tradierte Werte. Der LfDI betonte, dass das Selbstbestimmungsrecht der Einzelnen Wahlmöglichkeiten und Alternativen voraussetzt –

auch im Wirtschafts- und Geschäftsleben. Neben der Möglichkeit, sicher elektronisch zu bezahlen, müsse deshalb auch der Bargeldverkehr erhalten bleiben. Die Bürgerinnen und Bürger müssten die Möglichkeit behalten, Dritten Einblicke in ihr Konsumverhalten zu verwehren.

11.4 Vierter Verbraucherdialog Smart Home

In bewährter Zusammenarbeit mit dem Ministerium der Justiz und für Verbraucherschutz Rheinland-Pfalz und der Verbraucherzentrale Rheinland-Pfalz hat sich der LfDI im Rahmen des 4. Verbraucherdialogs dem Thema Smart Home gewidmet. Ziel der Verbraucherdialoge ist es, zusammen mit Expertinnen und Experten aus Wirtschaft, Wissenschaft, Verbänden und Behörden datenschutz- und verbraucherfreundliche Anforderungen an neue digitale Technologien zu formulieren. Diese werden in Empfehlungen zusammengefasst und veröffentlicht, die sich zum einen an Verbraucherinnen und Verbraucher, zum anderen aber auch an Produktanbieter richten.

Mit dem Thema Smart Home war das intelligente Zuhause Gegenstand des im Juni 2015 gestarteten und in mehreren Arbeitssitzungen entfalteten Verbraucherdialogs. Unter dem Oberbegriff „Smart Home“ wurden dabei technische Verfahren, Systeme und Dienste in Wohnräumen, -häusern und der Wohnumgebung betrachtet, die auf vernetzten Geräten und Installationen sowie automatisierbaren Abläufen basieren und zur Erhöhung der Wohn- und Lebensqualität, der Sicherheit sowie zur Steuerung der Energienutzung beitragen sollen.

Aktuelle Angebote am deutschen Markt betreffen z.B. die Vernetzung und Steuerung von Heizungsthermostaten, Jalousien, Beleuchtung, Tür- und Hauskameras oder Rauchmeldern. Solche sog. nachrüstbaren Lösungen, die jedermann – egal ob Mieterinnen und Mieter oder Eigentümerinnen und Eigentümer – zu vergleichsweise moderaten Preisen erwerben und oftmals selbständig in den eigenen vier Wänden installieren kann, standen im Fokus des 4. Verbraucherdialogs.

Aus Sicht des Datenschutzes hat die Themenstellung eine besondere Brisanz. Den fraglos mit den smarten Technologien verbundenen Vorteilen stehen nämlich häufig Nachteile gegenüber, die mit der Preisgabe persönlicher Lebensumstände verbunden sind. Auch wenn auf den ersten Blick vermeintlich nur technische Daten erhoben und verarbeitet werden, eröffnen diese mitunter erstaunlich detaillierte Einblicke in die Privatsphäre einzelner Nutzerinnen und Nutzer. Die schiere Datenmenge macht es häufig leicht, aussagekräftige Nutzerprofile zu erstellen und Lebensgewohnheiten offen zu legen. Heizungswerte geben in diesem Sinne Aufschluss über das Nutzungsverhalten einzelner Räume, und aus dem Stromverbrauch lassen sich gar Rückschlüsse auf das konsumierte Fernsehprogramm ziehen.

Da die Daten die räumliche Privatsphäre und damit einen besonders schützenswerten Rückzugsort betreffen, war es aus Sicht des LfDI wichtig, Leitlinien zur Umsetzung grundlegender datenschutzrechtlicher Prinzipien für Smart Home-Anwendungen zu definieren. Besondere Bedeutung kommt in den Empfehlungen daher den Aspekten der Transparenz, der Datensouveränität, der Datensparsamkeit aber nicht zuletzt auch der Datensicherheit zu.

Weitere Informationen zum Verbraucherdialog, einschließlich der erarbeiteten Empfehlungen finden sich unter: http://www.verbraucherdialog.rlp.de/

11.5 Scoring durch Witschaftsauskunfteien

Der Bundesgerichtshof hatte im Januar 2014 über den Umfang einer von der SCHUFA zu erteilenden Auskunft zum sog. Scoringverfahren entschieden. Dabei kam er zu dem Schluss, dass die SCHUFA als Wirtschaftsauskunftei nur die bei ihr über eine Person gespeicherten Informationen und die Tatsache, welche dieser Daten in die Scorewertberechnung eingeflossen sind, mitteilen muss. Welches Gewicht die einzelnen Informationen haben, um den Sorewert zu beeinflussen, muss die SCHUFA nicht erläutern. Das sei ihr Geschäftsgeheimnis, das der Gesetzgeber mit der Reglung im Bundesdatenschutzgesetz wahren wollte.

Diese Entscheidung löste lebhafte Diskussionen aus. Denn gerade Transparenz ist eine wichtige Säule des Datenschutzes. Nur wer weiß, welche Informationen über ihn gespeichert und wie diese zustande gekommen sind, kann sich gegen Fehler

wehren und sein Grundrecht auf Datenschutz auch wirksam ausüben. Mit der Einführung eines ausdrücklichen Auskunftsanspruchs zum Scoring im Jahr 2010 wurde dieses Grundverständnis auch im Bundesdatenschutzgesetz festgeschrieben. Doch ist durch die höchstrichterliche Entscheidung klar geworden, dass der Gesetzgeber das Ziel eines transparenten Verfahrens noch nicht erreicht hat und nachbessern muss. Angesichts der existentiellen Bedeutung von SCHUFA-Einträgen für viele Bürgerinnen und Bürger hält der LfDI diese Nachbesserung für dringlich geboten.

Doch ist wohl leider davon auszugehen, dass es hier nicht so schnell zu gesetzlichen Anpassungen kommen wird. Denn vor dem Hintergrund der erwarteten europäischen Datenschutz-Grundverordnung wird der nationale Gesetzgeber in Sachen Datenschutz zunächst wohl kaum aktiv werden (vgl. Tz. I-1.3). Dies obwohl eine vom Bundesministerium der Justiz und für Verbraucherschutz und des Bundesministeriums des Innern in Auftrag gegebene Studie zum Thema Scoring zu dem Ergebnis gekommen ist, dass der Rechtsrahmen durchaus verbesserungswürdig ist. So sollten die Auskunfteien in einem Zulassungs- und Registrierungsverfahren ihr Geschäftskonzept und die für das Scoring erhobenen Daten beschreiben. Die Anforderungen an die wissenschaftliche Qualität von Scoringverfahren sollten gesetzlich festgelegt werden. Besonders sensible bzw. potenziell diskriminierende Merkmale sollten beim Scoring nicht verwendet werden dürfen. Für die Frage, ob eine weitere Speicherung der Daten zulässig ist, sollten taggenaue Löschfristen gelten. Die Studie wurde im Dezember 2014 veröffentlicht und ist abrufbar z.B. unter

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/studie-scoring.pdf?__blob=publicationFile.

Auch ein Gesetzentwurf der Fraktion Bündnis 90/Die Grünen zur verbraucherfreundlicheren Gestaltung von Scoring-Verfahren (BT-Drs. 18/4864), in dem u.a. mehr Auskunftsansprüche und das Verbot von Geoscoring gefordert werden, musste sich zum Jahresende 2015 in der parlamentarischen Diskussion entgegen halten lassen, dass zunächst die EU-Datenschutz-Grundverordnung abzuwarten sei.

11.6 Personenidentifizierung per Videotechnik durch die Kreditwirtschaft

Kreditinstitute und Finanzdienstleister sind nach dem Geldwäschegesetz verpflichtet, ihre Kundinnen und Kunden zu identifizieren. Dies erfolgt in der Regel dadurch, dass ein Ausweisdokument, z.B. der Personalausweis vorgelegt wird. Die Kredit- und Finanzinstitute erheben dann die im Geldwäschegesetz vorgesehenen Daten, was grundsätzlich auch durch das Kopieren von bestimmten Teilen des Ausweispapieres erfolgen darf.

Schwieriger wird es, wenn die Kundin bzw. der Kunde und das Institut nicht am gleichen Ort sind. So haben sich bisher insbesondere Online-Banken z.B. des formularbasierten Postidentverfahrens bedient. Bei diesem Verfahren legen Kundinnen und Kunden ihren Ausweis bei einer Postfiliale vor, die dann die erforderlichen Daten erhebt und dem Kredit- oder Finanzinstitut übermittelt.

Seit März 2014 ist es Kredit- und Finanzinstituten nunmehr erlaubt, diese Identifizierung per Videotechnik durchzuführen. Dabei kann die Bankkundin oder der Bankkunde vom heimischen PC mit Kamera aus mittels des neuen Personalausweises den Identifizierungsvorgang durchführen. Im Videochat der Kundinnen und Kunden mit speziell geschulten Beschäftigten eines entsprechenden Dienstleisters halten diese ihren neuen Personalausweis so in die Kamera, dass die Sicherheitsmerkmale durch die andere Seite geprüft werden können. Der prüfende Dienstleister ist verpflichtet, Screenshots des Ausweisdokuments anzufertigen sowie das Gespräch akustisch aufzuzeichnen.

Das Bundesamt für Finanzdienstleistungsaufsicht geht davon aus, dass ein solcher Videochat als Identifizierung unter Anwesenden im Sinne des Geldwäschegesetzes zu qualifizieren sei und hat in einem Rundschreiben vom März 2014 hierzu Näheres bestimmt. Dabei hat es allerdings verabsäumt, Vorgaben zum Datenschutz und zur Datensicherheit zu machen.

Durch das Anfertigen von Screenshots wird eine komplette Kopie des Ausweispapieres angefertigt, was aus datenschutzrechtlicher Sicht nicht den Vorgaben des Geldwäschegesetzes entspricht. Denn

dort werden die notwendig zu erhebenden Identifikationsdaten abschließend aufgezählt. Daraus folgt, dass bei einer Kopie des Ausweises bestimmte Teile abgedeckt werden müssen.

Dieses Verfahren ist für die Kundinnen und Kunden freiwillig, d.h. sie müssen ihre Einwilligung erklären und zwar freiwillig, informiert und dokumentiert.

Wenn das Identifizierungsverfahren abgebrochen wird, z.B. weil die Bildübertragung gestört ist oder die Betroffenen es sich anders überlegt haben, ist unklar, was mit den bereits erhobenen Daten geschieht. Aus datenschutzrechtlicher Sicht ist sicherzustellen, dass die Daten dann komplett gelöscht werden.

Auch die vorgesehenen TAN-Eingabe stößt auf Bedenken hinsichtlich der Datensicherheit, wenn die selben Kommunikationswege für Eingabe und Bestätigung genutzt werden. Zudem ist aus datenschutzrechtlicher Sicht eine Ende-zu-Ende-Verschlüsselung zu fordern.

Datenschutzrechtlich bedenklich wird es auch, wenn die Videochatverbindung über Skype hergestellt wird. Denn dieser Dienst speichert vollständige Kommunikationsinhalte. Wenn diese Daten dann auch noch auf Servern außerhalb Europas abgelegt werden, ist dies gerade vor dem Hintergrund der Safe Harbor-Entscheidung des Europäischen Gerichtshofs besonders kritikwürdig (vgl. Tz. I-1.4, I-1.5).

Mittlerweile hat das Bundesministerium für Finanzen die von den Datenschützern geäußerte Kritik aufgegriffen und in einem Schreiben an die Vertreter der Deutschen Kreditwirtschaft die oben beschriebenen datenschutzrechtlichen Rahmenbedingungen für das Verfahren dargelegt. So ist zu hoffen, dass die Kredit- und Finanzinstituten eingeräumte Möglichkeit der Fernidentifizierung mittels Videotechnik zukünftig datenschutzgerecht umgesetzt wird. Dies wird in der Praxis zu überprüfen sein.

12. Finanzen

12.1 Neues zur Kirchensteuer

Ab dem 1. Januar 2015 soll das System für die Abführung der Kirchensteuer auf die Abgeltungssteuer für Kapitalerträge vereinfacht werden: Musste man bisher gegenüber Banken, Sparkassen und anderen Finanzinstituten unter Angabe seiner Religionszugehörigkeit beantragen, dass die Kirchensteuer ebenso wie die Kapitalertragssteuer direkt an der Quelle abgeführt wird, soll dies nunmehr automatisch erfolgen. Im Vorfeld hierzu fragt das Kredit- bzw. Finanzinstitut beim Bundeszentralamt für Steuern in einem automatisierten Verfahren ab, ob die Kundinnen oder Kunden Angehörige einer Steuer erhebenden Religionsgemeinschaft sind und welcher Kirchensteuersatz angewendet werden muss. Dem Finanzinstitut wird hierzu ein sechsstelliges Kirchensteuerabzugsmerkmal mitgeteilt. Es erfährt also nicht im Klartext, welcher Religionsgemeinschaft seine Kundinnen und Kunden angehören. Zudem ist es verpflichtet, dieses Kirchensteuerabzugsmerkmal vor unberechtigten Zugriffen sowohl intern als auch extern zu schützen. Es darf nur zur Abführung der Kirchensteuer auf Kapitalerträge genutzt werden und zu keinem anderen Zweck (vgl. 23. Tb., Tz. II-9).

Wer nicht möchte, dass sein Kredit- oder Finanzinstitut dieses Kirchensteuerabzugsmerkmal erfährt, kann der Übermittlung beim Bundeszentralamt für Steuern widersprechen. Wer sich einen solchen Sperrvermerk eintragen lässt, muss seinen kirchensteuerlichen Verpflichtungen dann wie bisher auch direkt gegenüber dem Finanzamt nachkommen, das wiederum vom eingetragenen Sperrvermerk durch das Bundeszentralamt für Steuern informiert wird.

Während Bürgerinnen und Bürger bisher selbst aktiv werden mussten, um Daten preiszugeben, hat sich das Prinzip zu Lasten des Datenschutzes umgekehrt. Jetzt muss handeln, wer Datenflüsse verhindern will. Das den Datenschutz stärkende Prinzip der Einwilligung hat der Gesetzgeber ersetzt durch die datenschutzrechtlich deutlich schwächere Widerspruchslösung. Hierzu kommt, dass die Institute zukünftig nicht mehr jährlich über die Widerspruchsmöglichkeit informieren müssen, sondern nur noch einmalig bei Begründung der Geschäftsbeziehung.

12.2 Auskunftsrechte gegenüber der Finanzverwaltung – eine unendliche Geschichte

Während der LfDI zuletzt (vgl. 23. Tb., Tz. II-9) verhalten optimistisch war, dass Betroffene zukünftig voraussetzungslos Auskunft über ihre in der Finanzverwaltung vorhandenen persönlichen Daten erlangen können, hat sich diese Hoffnung im Berichtszeitraum leider zerschlagen. Das gemeinsame Konzept von Bund und Ländern zur Modernisierung des Besteuerungsverfahrens sah zwar die Schaffung bereichsspezifischer Regelungen zum Datenschutz und insbesondere einen Auskunftsanspruch auf Antrag über die im Besteuerungsverfahren gespeicherten personenbezogenen Daten vor (vgl. Diskussionsentwurf „Modernisierung des Besteuerungsverfahrens“, veröffentlicht durch das Bundesministerium der Finanzen am 21. November 2014, abrufbar unter http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/2014-11-21-Modernisierung-des-Besteuerungsverfahrens-Diskussionsentwurf-Anlage.pdf?__blob=publicationFile&v=1). Doch fanden diese geplanten Regelungen keinen Eingang in das „Gesetz zur Modernisierung des Besteuerungsverfahrens“, das derzeit als Referentenentwurf vorliegt. Die geplanten Regelungen waren aus datenschutzrechtlicher Sicht nicht optimal, doch hätten sie die derzeitige Situation wesentlich verbessert. Denn gegenwärtig müssen Betroffene nach Vorgabe des Bundesfinanzministeriums erst ein berechtigtes Interesse an einer Auskunft darlegen, bevor die Finanzverwaltung über die Herausgabe der Daten entscheidet. Diese ministerielle Vorgabe widerspricht der Gesetzeslage, wie sie sich in den Landesdatenschutzgesetzen und auch im Bundesdatenschutzgesetz darstellt (vgl. hierzu ausführlich 22. Tb., Tz. 12.2). Als Begründung für einen Verzicht auf entsprechende Regelungen im Gesetz zur Modernisierung des Besteuerungsverfahrens dient die geplante europäische Datenschutz-Grundverordnung (vgl. Tz. I-1.3). So heißt es ausdrücklich in der Gesetzesbegründung:

> „Obwohl die verstärkte Nutzung der elektronischen Kommunikation und Datenverarbeitung auch Fragen des Datenschutzes berührt und auch für das Besteue-

rungsverfahren moderner Prägung sichergestellt werden muss, dass zu jeder Zeit und in jedem Verfahrensschritt die dem Steuergeheimnis unterliegenden Daten der Steuerpflichtigen geschützt sind, verzichtet dieses Gesetz auf die in den vorbereitenden Beratungen zunächst vorgesehenen, bereichsspezifischen Regelungen zum Datenschutz, insbesondere auf Regelungen zum Auskunftsanspruch des Betroffenen über zu seiner Person gespeicherte Daten und auf Regelungen zu den so genannten sonstigen Betroffenenrechten. Dies war erforderlich, weil die Beratungen auf Ebene der Europäischen Union zur sog. Datenschutz-Grundverordnung (vgl. http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_de.pdf) kurz vor ihrem Abschluss stehen.
Die Datenschutz-Grundverordnung wird auch im öffentlichen Bereich, also auch im Besteuerungsverfahren, unmittelbar gelten. Nach Verkündung der Datenschutz-Grundverordnung wird innerhalb einer mehrjährigen Übergangsphase von den Mitgliedstaaten zu prüfen sein, ob und inwieweit nationales Datenschutzrecht aufzuheben oder zu ändern ist und wie die Gestaltungsspielräume der Mitgliedstaaten – z.B. nach Art. 21 des Verordnungsentwurfs – künftig genutzt werden.“ (Referentenentwurf des Bundesministeriums der Finanzen „Entwurf eines Gesetzes zur Modernisierung des Besteuerungsverfahrens“, Bearbeitungsstand: 26. Mai 2015 13:47 Uhr, S. 56 f., abrufbar unter http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Referentenentwuerfe/2015-08-27-entwurf-eines-Gesetzes-zur-modernisierung-des-besteuerungsverfahrens.html)

So befinden sich Betroffene weiterhin in einer schlechten Ausgangslage, und es bleibt abzuwarten, was die europäische Datenschutz-Grundverordnung bringen wird.

12.3 Rücksendung von Belegen durch das Finanzamt

Ein Steuerpflichtiger hatte sich an den LfDI gewandt, da sein Finanzamt bei der Rücksendung von Belegen kein eigenes Deckblatt mit Adressierung verwendete, sondern einfach einen adressierten Beleg dafür nutzte. So kam es im konkreten Fall dazu, dass die eingereichte Schornsteinfegerrechnung als Vorblatt diente mit der Folge, dass als Absender ebenfalls der Schornsteinfeger zu erkennen war. Bei Unzustellbarkeit wäre dieser Briefumschlag sicherlich sodann an den Schornsteinfeger gesandt worden, da das Finanzamt nicht als Absender erkennbar war. In einem solchen Fall hätte dieser als unberechtigter Dritter Einblick in Steuerunterlagen erhalten.

Das Finanzamt bestätigte, dass ein solches Vorgehen nicht üblich sei und es sich um einen Einzelfall handelte. Aufgrund dieses Vorfalls seien die Beschäftigten nochmals darauf hingewiesen worden, den Belegen stets ein eigenes Vorblatt mit Adressierung und korrekter Absenderangabe vorzuheften. Umso erstaunlicher war es dann, dass der gleiche Fehler gegenüber dem gleichen Steuerpflichtigen zwei Jahre später wieder passierte. Dies führte dazu, dass sich auch das Finanzministerium mit diesem Problem befasste. Mittlerweile wurde das korrekte Verfahren schriftlich verfügt.

Es bleibt abzuwarten, ob dies zukünftig nunmehr endgültig ein datenschutzgerechtes Vorgehen sicherstellt.

13. Verkehr

13.1 Autos in neuer Dimension

Im modernen Auto finden sich neben einem Motor, vier Rädern und einem Lenkrad auch ganz besonders eines, nämlich Daten. Ausgestattet mit moderner Informationstechnik verfügt es über vielfältige Systeme, die den Nutzerinnen und Nutzern das Leben im Auto sicher und angenehm machen sollen. Dazu zählen z.B. Navigation, Notruf (das sog. eCall-System), Werkstattdokumentation und auch Mulitmediaanwendungen.

Diese fortschreitende Technik bietet einerseits vielfältige Vorteile im Bereich Verkehrssicherheit und Komfort. Doch beeinträchtigt sie andererseits auch die Persönlichkeitsrechte der Fahrzeugnutzerinnen und –nutzer in nicht unerheblichem Umfang.

Aus diesem Grund haben sich die Datenschutzaufsichtsbehörden im Berichtszeitraum intensiv mit dieser Problematik befasst und in einer Entschließung die aus ihrer Sicht besonders gravierenden Risiken veröffentlicht (vgl. Entschließung der Datenschutzkonferenz vom 9. Oktober 2014 „Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert“). Sie haben zudem Gespräche mit Vertretern der Automobilindustrie geführt, um für das Thema weiter zu sensibilisieren und sicherzustellen, dass Kfz-Nutzerinnen und –Nutzer von den Vorteilen profitieren, ohne ihr Persönlichkeitsrecht im hohen Maße einzuschränken.

Dabei sind insbesondere folgende Punkte relevant:

- Personenbezogen sind die bei der Nutzung eines Fahrzeugs anfallenden Daten immer dann, wenn sie mit dem Kennzeichen bzw. mit der Fahrzeugidentifikationsnummer verknüpft werden.
- Zulässig ist eines solche Datenverarbeitung dann, wenn sie auf einer informierten Einwilligung der Nutzerinnen und Nutzer beruht. Dazu gehört aber insbesondere, dass die Hersteller über Funktionen und Datenflüsse verständlich aufklären. Bei einzelnen Datenverarbeitungsprozessen kann sich die Rechtsgrundlage auch aus einer gesetzlichen Vorgabe oder einer Sorgfaltspflicht des Herstellers ergeben. Aber auch in diesen Fällen ist Transparenz angebracht.
- Um die verantwortliche Stelle für die Datenverarbeitung festzustellen, muss unterschieden werden: Werden die Daten im Fahrzeug gespeichert, also sozusagen „offline“, werden sie zunächst nur gespeichert. Eine Erhebung findet dann erst statt, wenn z.B. die Werkstatt den Fehlerspeicher ausliest. In diesem Augenblick ist dann die Werkstatt verantwortliche Stelle im Sinne des Datenschutzrechts. Werden die Daten hingegen aus dem Auto heraus übermittelt, in der Regel „online“, werden die Daten durch die Stelle erhoben, an die die Daten übermittelt werden. Dies ist in der Regel der Hersteller. Die Bestimmung der verantwortlichen Stelle ist aber entscheidend, damit Betroffene von ihren Rechten, z.B. dem auf Auskunft, Gebrauch machen können.
- Da die Hoheit über die erhobenen bzw. gespeicherten Daten bei den Nutzerinnen und Nutzern liegt, sollte ihnen ermöglicht werden, einzelne Funktionen der Datenverarbeitung zu erkennen und auch abzuschalten. Hier sind insbesondere die Hersteller gefragt, die entsprechende Technik zur Verfügung zu stellen und darüber aufzuklären.

Gemeinsame 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 Kraftfahrzeuge“:
http://www.datenschutz.rlp/de/aktuell/2016/images/Gemeinsame_Erklaerung_VDA_Datenschutzbehoerden.pdf

Diese Thematik und die damit verbundenen datenschutzrechtlichen Fragen werden die Datenschutzaufsichtsbehörden auch in Zukunft hinreichend beschäftigen.

13.2 Protokollierung von IP-Adressen für die Erkennung und Abwehr von Angriffen Hacker-Angriff auf das Verfahren „Kfz-Wunschkennzeichen“

Im Zusammenhang mit einem Hackerangriff auf das beim Landesbetrieb Daten und Information betriebene IT-Verfahren zur Reservierung von Kfz-Wunschkennzeichen wurde ein strafrechtliches Ermittlungsverfahren eingeleitet. Dieses wurde mit der Begründung eingestellt, dass eine Zuordnung der IP-Adressen zu einer Täterin oder einem Täter von

vornherein ausgeschlossen war, da aus Gründen des Datenschutzes die letzten drei Stellen der IP-Adressen der auf das System zugreifenden Nutzerinnen und Nutzer systemseitig anonymisiert wurden.

Dies erweckt den Eindruck, der Datenschutz stehe notwendigen strafrechtlichen Aufklärungsbemühungen entgegen. Dies trifft nicht zu.

Bei der vollständigen IP-Adresse handelt es sich nach einheitlicher Auffassung der Datenschutzaufsichtsbehörden um ein personenbezogenes Datum. Diese Einschätzung wurde in einem Urteil des Europäischen Gerichtshofs vom 24. November 2011 (Az. C-70/10) bestätigt.

Nach § 13 Abs. 4 Nr. 2 TMG sind die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung zu löschen. Nach § 15 Abs. 1 TMG darf der Dienstanbieter personenbezogene Daten von Nutzerinnen und Nutzern nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. § 15 Abs. 3 TMG erlaubt u.a. die Bildung von Nutzungsprofilen zur bedarfsgerechten Gestaltung von Telemedien und damit die Speicherung individueller Zugriffe, jedoch nur bei Verwendung von Pseudonymen. Bei der vollständigen IP-Adresse handelt es sich nicht um ein solches Pseudonym (vgl. 23. Tb., Tz. II-1.4). Ziel dieser Regelung ist es, die Bildung von Profilen über das persönliche Nutzungsverhalten zu verhindern.

Die Landesregierung hat sich der Auffassung des LfDI, dass es sich bei IP-Adressen um personenbezogene Daten handelt, deren Protokollierung in vollständiger Form (im Rahmen der o.g. Regelungen) rechtswidrig ist, angeschlossen. Der Landesbetrieb Daten und Information ist den Empfehlungen des LfDI gefolgt, indem die IP-Adressen in den Protokolldaten der Internet- und Anwendungsserver frühzeitig zu anonymisieren. Aktuell erfolgt dies automatisiert in einem kurzzeitigen Rhythmus, bei dem das letzte Byte der IP-Adressen in den Protokolldaten gelöscht wird. Die anonymisierten Zugriffsdaten stehen für die nach dem Telemediengesetz zugelassenen Zwecke (z.B. statistische Nutzungsanalyse, Angebotsoptimierung etc.) zur Verfügung.

Die Notwendigkeit, zur Abwehr oder Aufklärung von Angriffen auf die IP-Adressen in ungekürzter Form zugreifen zu können, wurde dabei seitens des LfDI stets anerkannt. Er hat in diesem Zusammenhang einer siebentägigen Speicherung der vollständigen IP-Adresse auf den Firewall- bzw. Angriffserkennungssystemen als technischer Vorkehrung zum Schutz der Datenverarbeitungssysteme gegen Angriffe und zum Erkennen, Eingrenzen oder Beseitigen von Störungen zugestimmt. Die genannte Speicherfrist geht konform mit der Rechtsprechung des Bundesgerichtshofs in dieser Frage.

Da diese Daten anderen Zwecken als den im Telemediengesetz genannten dienen – nämlich der Gewährleistung eines ordnungsgemäßen IT-Betriebs nach § 13 Abs. 6 LDSG – werden sie gemäß der Zweckbindungskontrolle nach § 9 Abs. 2 Nr. 8 LDSG gesondert, d.h. auf der Firewallstruktur des Landesbetriebs Daten und Information gespeichert. Für den genannten Zeitraum stehen damit IP-Adressen ungekürzt zur Verfügung. Der Differenzierung zwischen einer Speicherung der IP-Adressen auf den Anwendungssystemen der Kundinnen und Kunden des Landesbetriebs Daten und Information und auf der Sicherheitsstruktur liegt zugrunde, dass die Protokolldaten auf dem Sicherheitsgateway ausschließlich der Verantwortung des Landesbetriebs Daten und Information unterfallen und einer engen Zweckbindung (§ 13 Abs. 6 LDSG) und Zugriffskontrolle unterliegen. Dies ist bei einer Speicherung auf den Anwendungssystemen grundsätzlich anders. Die dortigen Daten und deren Nutzung unterliegen nicht der Verantwortung des Landesbetriebs Daten und Information und werden primär zu Zwecken der statistischen Auswertung, der Nutzungsanalyse oder der bedarfsgerechten Gestaltung der Angebote und Verfahren erfasst.

Mit der gefundenen Verfahrensweise wurden einerseits datenschutzrechtliche Vorgaben umgesetzt und andererseits notwendige Sicherheitsaspekte bedacht.

Aufgrund der hohen Zahl von Zugriffen am zentralen Internetgateway des Landesnetzes (ca. 70 Milliarden Zugriffe pro Monat) und des mit deren vollständiger Protokollierung verbundenen Aufwands hat der Landesbetrieb Daten und Information zunächst lediglich Zugriffe erfasst und ausgewertet, die auf-

grund vorgegebener Kriterien als verdächtig einzustufen sind. Für die Zugriffe im Rahmen des Angriffs auf das Verfahren „Kfz-Wunschkennzeichen“ war eine solche Auswertung bzw. Einstufung als „verdächtiger Zugriff“ jedoch nicht möglich, da die Kommunikation verschlüsselt war und die Inhalte der Datenpakete somit an der Firewall nicht eingesehen bzw. überprüft werden konnten. Damit wurden diese Zugriffe nicht entsprechend der dargestellten Verfahrensweise erfasst.

Als Konsequenz aus dem Angriff auf das Verfahren „Kfz-Wunschkennzeichen“ hat der Landesbetrieb Daten und Information in Abstimmung mit dem LfDI die Verfahrensweise dahingehend erweitert, dass die Zugriffsdaten nach der Entschlüsselung auf den Endsystemen und vor der Kürzung der IP-Adressen auf einen separaten Protokollserver gespiegelt und dort für sieben Tage gespeichert werden. Damit wird beiden Belangen – der Anonymisierung der IP-Adressen in den Protokolldaten der Web- und Anwendungsserver und einer Speicherung aller für die Abwehr und Analyse von Angriffen erforderlichen Daten – entsprochen. Im Fall eines strafrechtlichen Ermittlungsverfahrens stehen die jeweiligen Zugriffsdaten auch für einen darüber hinausgehenden Zeitraum zur Verfügung.

13.3 Datenschutzrechtliche Fragen rund um die Fahrzeugzulassung

Rund um die Fahrzeugzulassung stellen sich immer wieder datenschutzrechtliche Fragen:

■ Einscannen von Personalausweisen

So wurde zumindest bei einer Zulassungsstelle in Rheinland-Pfalz für dortige Handlungen stets der Personalausweis der Bürgerinnen und Bürger gescannt und digital auf dem Rechner der Beschäftigten abgespeichert. Der LfDI sah keine Rechtsgrundlage für diese Art der Datenerhebung und –speicherung. Denn bei der Zulassung eines Fahrzeuges sind gem. § 6 Abs. 1 Satz 2 Nr. 1 FZV Familienname, Geburtsname, Vorname, evtl. Ordens- oder Künstlername, Geburtsdatum und -ort, Geschlecht und Anschrift des Halters anzugeben. Auf Verlangen sind diese Angaben nachzuweisen. In der Regel reicht für einen Nachweis hier die Vorlage des Personalausweises, so dass sich die Beschäftigten auf der Zulassungsstelle von der Richtigkeit der gemachten Angaben überzeugen können. Diese Vorschrift sieht nicht vor, dass der Personalausweis kopiert, eingescannt und weiterhin gespeichert wird.

Die betroffene Zulassungsstelle hatte ihr Vorgehen damit begründet, dass es ein Service für Bürgerinnen und Bürger sei, wenn ihr Ausweis bereits eingescannt sei. So müsse bei Folgehandlungen nicht mehr der Personalausweis vorgelegt werden, da er bereits archiviert sei. Die Zulassungsstelle hatte aber gleichzeitig bestätigt, dass sie zukünftig vom Einscannen der Ausweise absehen werde. Der Forderung des LfDI, die bereits gespeicherten Kopien zu löschen, sah sich die Zulassungsstelle außerstande nachzukommen, da dies aufgrund der Menge der Daten nicht realisierbar sei.

Eine Löschung hält der LfDI aber unbedingt für erforderlich. Er hat daher das zuständige Ministerium des Innern, für Sport und Infrastruktur gebeten sicherzustellen, dass das bemängelte Verfahren auch in andern Zulassungsstellen keine Anwendung findet und die bereits erhobenen und gespeicherten Personalausweisdaten gelöscht werden.

■ Kfz-Kennzeichen mit Sicherheitscode

Ein Kfz-Halter hatte sich mit der Sorge an den LfDI gewandt, dass bei der Neuzulassung von Kraftfahrzeugen RFID-Chips, die sich innerhalb des Aufklebers auf dem vorderen Kfz-Kennzeichen befinden und von außen fühlbar seien, eingebunden würden. Mit diesem Chip könne man allerlei Dinge machen, z.B. alle Fahrzeuge in Deutschland mit Standort, Halterdaten etc. überwachen.

Die Sorge des Petenten war unbegründet: Die Ausgestaltung von Kfz-Kennzeichen ist in § 10 FZV geregelt. Dort heißt es, dass die Stempelplakette einen verdeckt angebrachten Sicherheitscode bergen muss, der erst durch Freilegen unumkehrbar sichtbar gemacht werden kann. Die Stempelplakette muss so beschaffen sein und so befestigt werden, dass sie bei einem Entfernen zerstört wird. Die Stempelplakette einschließlich Druckstücknummer und Sicherheitscode muss gewisse Anforderungen erfüllen.

Wer ein solches Kennzeichen mit einem solchen Sicherheitscode hat, kann gem. § 14 Abs. 2 FZV ein Fahrzeug auch dadurch außer Betrieb setzen las-

sen, dass er dies direkt oder über ein vom Kraftfahrtbundesamt betriebenes informationstechnisches System bei der Zulassungsbehörde elektronisch beantragt. Bei dieser internetbasierten Außerbetriebssetzung werden das Vorlegen der Zulassungsbescheinigung Teil I und der Kennzeichenschilder u.a. durch die elektronische Übermittlung des Sicherheitscodes der Stempelplakette ersetzt.

Solche Sicherheitscodes werden also generell bei allen Zulassungsstellen in Deutschland auf Kennzeichen ab dem 1. Januar 2015 angebracht. Sie dienen lediglich dazu, das Kennzeichen bei einer internetbasierten Außerbetriebssetzung ungültig zu machen. In der Verordnungsbegründung heißt es hierzu ausdrücklich (BR-Drs. Nr. 435/13, S. 46): „Zur Beachtung des Datenschutzes sollen von der maschinenlesbaren Form Verfahren nicht erfasst sein, die ein Auslesen aus der Ferne ermöglichen, etwa mittels RFID (radio-frequency identification).“

13.4 Kommunale Verkehrsdatenerhebung zu Planungszwecken

Auch im zurückliegenden Berichtszeitraum haben sich immer wieder Bürgerinnen und Bürger mit datenschutzrechtlichen Bedenken an den LfDI gewandt, wenn ihnen ungewöhnliche „Verkehrsmaßnahmen“ aufgefallen sind bzw. sie sogar selbst davon betroffen waren. Oft werden z.B. Kameras an bestimmten Verkehrspunkten von Firmen aufgestellt, um den Verkehrsstrom zu messen. Im besten Fall weist ein Schild auf die Kamera, ihren Urheber und ihren Zweck hin. In einem Fall hielt sogar die Polizei Fahrzeuge an, damit deren Fahrer an einer Befragung zum Verkehrsverhalten teilnehmen konnten.

Solche Maßnahmen wecken bei Betroffenen datenschutzrechtliche Bedenken. Der LfDI ist dann stets darum bemüht, die Begleitumstände einer Verkehrszählung aufzuklären und ggf. Hinweise zu geben, wie eine solche Maßnahme datenschutzgerecht durchgeführt werden kann. Denn grundsätzlich ist es zulässig, dass eine Kommune für Planungszwecke Verkehrsdaten erhebt und verarbeitet. Diese Aufgabe kann auch Dritten übertragen werden, wenn ein entsprechender Vertrag zur Erhebung von Daten im Auftrag abgeschlossen wird (§ 4 LDSG). Nach dieser Vorschrift ist die auftragnehmende Stelle unter besonderer Berücksichtigung der Eignung der von ihr getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen. Darin sind bestimmte Einzelheiten zu regeln, insbesondere wie die Datenerhebung erfolgt, wie die Daten ausgewertet werden, wann sie gelöscht werden und wie die technisch-organisatorischen Anforderungen an den Datenverarbeitungsvorgang sein müssen. Insbesondere ist auch sicherzustellen, dass die Befragten auf die Freiwilligkeit der Teilnahme hingewiesen werden. Da die Kommune als auftraggebende Stelle verantwortlich bleibt für die Datenverarbeitung, muss durch sie sichergestellt werden, dass die Befragung der Verkehrsteilnehmerinnen und -teilnehmer in datenschutzgerechter Form erfolgt.

Dazu gehört, dass die Daten möglichst anonym erhoben werden. Wenn z.B. die Fahrzeuge mittels einer Videoaufzeichnung gezählt werden sollen, sollten technische Vorkehrungen getroffen werden, damit die Kennzeichen nicht mit erfasst werden. Ist die Erhebung zumindest personenbeziehbarer Daten (z.B. bei der Befragung zu bestimmten Wegen) nicht vermeidbar, sind die Daten so schnell wie möglich zu anonymisieren.

Solche Verkehrserhebungen werden aber in der Regel nicht durch die Polizei durchgeführt. Diese hat gem. § 36 Abs. 5 StVO nur die Befugnis, Verkehrsteilnehmerinnen und -teilnehmer zu Zwecken der Verkehrserhebung anzuhalten. Diese Befugnis beschränkt sich ausschließlich auf das reine Anhalten. Hierzu sind die Verkehrsteilnehmerinnen und -teilnehmer auch verpflichtet. Die Beantwortung von Fragen zur Verkehrserhebung ist dann aber den Angehaltenen freigestellt. Dies sollte bei der Maßnahme auch deutlich zum Ausdruck kommen. Insbesondere hält es der LfDI für empfehlenswert, bereits im Vorfeld einer Verkehrserhebung die geplanten Maßnahmen öffentlich zu machen. Hierbei ist es nicht notwendig, den genauen Tag anzugeben, sondern es reicht der Hinweis auf einen Zeitrahmen, um die Messergebnisse nicht zu verfälschen.

14. Weitere technische Themen

14.1 Einsatz privater Geräte bei der Nutzung von Ratsinformationssystemen

Zum Einsatz privater mobiler Geräte hat sich der LfDI in seinem Datenschutzbericht 2010/2011 geäußert (vgl. 23. Tb., Tz. II-1.6). Danach sind aus seiner Sicht für dienstliche Aufgaben grundsätzlich dienstlich bereitgestellte Geräte zu nutzen. Bei der Nutzung privater Geräte hat die Dienststelle letzten Endes nicht die vollständige bzw. alleinige Verfügungsgewalt. Ihr Einsatz kommt damit aus Sicht des LfDI nur ausnahmsweise in Betracht. Um Sicherheitsbeeinträchtigungen zu vermeiden, muss ein Einsatz privater Geräte auf Bereiche beschränkt bleiben, die verlässlich durch organisatorische Regelungen gehandhabt werden können

Der Einsatz privater Endgeräte für den Abruf und die Speicherung von Unterlagen aus Ratsinformationssystemen ist zulässig, wenn folgende Anforderungen bzw. Sicherheitsmaßnahmen erfüllt sind:

- Wenn es sich bei den bereitgestellten Daten um Unterlagen handelt, die in öffentlicher Sitzung behandelt werden und die im Rahmen des Landestransparenzgesetzes auf Antrag ohne Einschränkungen zugänglich gemacht werden können, unterliegen diese keinen besonderen Vertraulichkeitsanforderungen. In diesen Fällen begegnet eine Speicherung und Verarbeitung derartiger Unterlagen auf privaten Endgeräten keinen datenschutzrechtlichen Bedenken; besondere Maßnahmen zur Sicherung der Vertraulichkeit sind nicht erforderlich.

  Allerdings regelt § 19 Abs. 2 Nr. 2 LDSG, dass personenbezogene Daten zu löschen bzw. zu vernichten sind, wenn ihre Kenntnis zur Erfüllung der gesetzlich übertragenen Aufgaben nicht mehr erforderlich ist. Das dürfte regelmäßig nach dem Ende der jeweiligen Sitzung der Fall sein. Die Mandatsträgerinnen und -träger wären jedenfalls darauf hinzuweisen, dass die Vorlagen dann gelöscht bzw. datenschutzgerecht vernichtet werden. Eine weitere Speicherung bzw. Aufbewahrung wäre nur zulässig, wenn dies zu einer weiterhin andauernden Aufgabenerfüllung notwendig ist.

- Soweit vertrauliche Unterlagen oder Unterlagen für in nicht-öffentlicher Sitzung zu behandelnde Vorgänge betroffen sind (Daten mit normalem Schutzbedarf), sind Maßnahmen nach § 9 Abs. 2 Nr. 3 und 4 LDSG erforderlich, die gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Neben technischen Maßnahmen bei den eingesetzten Geräten (vgl. unten) bedarf es hierzu verbindlicher Vereinbarungen über den Abruf und die Nutzung von Unterlagen aus dem Ratsinformationssystem, dem Schutz vor unbefugter Kenntnisnahme und zur Löschung von Daten.

  Das Sicherheitsniveau der eingesetzten Privatgeräte muss grundsätzlich dem entsprechender dienstlicher Geräte vergleichbar sein. Neben einem ausreichenden Schutz vor Schadsoftware bedarf es hierzu technischer Zugriffsregelungen, die eine unbefugte Kenntnisnahme wirksam verhindern (z.B. getrennte Nutzerkennungen, Differenzierung von Zugriffsrechten auf Dokumente und Verzeichnisse).

  Häufig ist dies aufgrund fehlender technischer Kenntnisse der Besitzer der Geräte, des jeweiligen Nutzungsspektrums oder der Mitnutzung durch Dritte jedoch nicht verlässlich zu gewährleisten. In solchen Fällen bedarf es einer Verschlüsselung der auf Privatgeräten gespeicherten Daten. Dies kann auf Dokument- oder Verzeichnisebene oder durch die Nutzung verschlüsselter Laufwerke erfolgen. Bestehende Möglichkeiten hierzu sind im Internetangebot des LfDI dargestellt; die für die sichere Ablage von Daten auf Cloud-Speichern empfohlenen Verfahrensweisen eignen sich auch für die Speicherung vertraulicher Unterlagen auf Privatgeräten.

  Ohne einen ausreichenden Zugriffsschutz oder eine wirksame Verschlüsselung ist die Speicherung und Verarbeitung vertraulicher Unterlagen aus einem Ratsinformationssystem wegen Verstoßes gegen § 9 LDSG unzulässig.

Hinweise des LfDI zur sicheren Ablage von Dokumenten auf Cloud-Speichern
http://www.datenschutz.rlp.de/de/selbstds.php?submenu=cloud

- Eine besondere Situation ergibt sich bei der Nutzung privater mobiler Geräte wie Smartphones oder Tablet-PCs. Diese verfügen in der Regel systemseitig nicht über ausreichende Sicherheitsfunktionen und Möglichkeiten, Zugriffsrechte differenziert vergeben zu können; weiterhin besteht bei dieser Geräteklasse erfahrungsgemäß eine größere Gefahr des Verlusts oder Diebstahls.

  Soweit derartige Geräte für den Abruf und die Speicherung vertraulicher Unterlagen aus dem Ratsinformationssystem zugelassen werden sollen, bedarf es, um den Anforderungen aus § 9 LDSG zu entsprechen, zwingend des Einsatzes von Zusatzlösungen, die eine verschlüsselte Speicherung der Unterlagen sicherstellen und die Möglichkeit bieten, ein Gerät im Falle des Verlusts zu sperren oder die Daten zu löschen.

  Im Einzelnen hält der LfDI in diesem Zusammenhang folgende Maßnahmen für erforderlich:

  - Die Geräte müssen über einen Schutz unbefugter Inbetriebnahme oder Nutzung verfügen (z.B. PIN, Sperrmuster).
  - Es muss sichergestellt sein, dass eine Trennung zwischen privaten Anwendungen und Daten und den aus dem Ratsinformationssystem bezogenen Daten erfolgt; für letztere muss eine verschlüsselte Speicherung erfolgen. Beiden Anforderungen kann mit sog. „Container-Lösungen“ entsprochen werden, die eine Kapselung von Daten und ggf. Anwendungen ermöglichen. Soweit auf den Geräten ausschließlich eine Speicherung von Unterlagen aus dem Ratsinformationssystem erfolgt, kann auf die o.g. Lösungen zur sicheren Ablage von Dokumenten zurückgegriffen werden.
  - Die Betriebssysteme der Geräte müssen auf einem aktuellen Stand sein; System- und Sicherheitsfunktionen dürfen nicht durch unzulässige Maßnahmen verändert worden sein (kein „Jailbreak“ oder „Root“).
  - Die Eigentümerinnen und Eigentümer des Geräts müssen verpflichtet werden, die Sicherheitsmaßnahmen auf ihrem Gerät umzusetzen und auf letztgenannte Funktionen zu verzichten.

  Soweit diesen Anforderungen auf den vorgesehenen Geräten nicht entsprochen werden kann, ist von der Verwendung privater Smartphones und Tablet-PCs abzusehen.

  Die dargestellten Anforderungen gelten für Unterlagen und Daten mit normalem dienstlichem Schutzbedarf. In Fällen, in denen die Daten einen besonderen Schutzbedarf haben bzw. besonderen Vertraulichkeitsanforderungen unterliegen, scheidet eine Bereitstellung von Unterlagen über das Ratsinformationssystem möglicherweise grundsätzlich, zumindest jedoch deren Speicherung und Verarbeitung auf privaten Geräten aus. Dies ist aus Sicht des LfDI v.a. für besondere personenbezogene Daten nach § 3 Abs. 9 LDSG sowie für Daten zu prüfen, die einem besonderen Berufs- und Amtsgeheimnis (§ 203 StGB) unterliegen oder Personalangelegenheiten oder die Annahme von Spenden behandeln.

14.2 Wolkiger Datenschutz – Nutzung von Office365 durch öffentliche Stellen

Die Art. 29-Gruppe der EU hat mit einer Stellungnahme vom April 2014 bestätigt, dass die unternehmensspezifischen Cloud-Verträge von Microsoft im Einklang mit den europäischen Datenschutzvorschriften bzw. den EU-Standardvertragsklauseln zur Übermittlung personenbezogener Daten in Drittstaaten stehen. Die EU-Standardvertragsklauseln sollen den Schutz personenbezogener Daten auch dann sicherstellen, wenn Daten außerhalb der Europäischen Union verarbeitet werden. Durch die damit konformen Microsoft-Vertragsregelungen für Unternehmen ist damit grundsätzlich eine Übermittlung personenbezogener Daten an Microsoft möglich. Die Stellungnahme der Art. 29-Gruppe bezieht sich ausschließlich auf die EU-Vertragsklauseln, nicht jedoch auf deren Anhänge (Datenflüsse, technisch-organisatorische Maßnahmen). Hier müssen weiterhin spezifische Regelungen zwischen Datenexporteur und Datenimporteur vereinbart werden.

Stellungnahme der EU-Kommission zu den Microsoft Cloud-Verträgen http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf)

Die Nutzung von Office 365 stellt datenschutzrechtlich eine Übermittlung zum Zweck einer gezielten,

vertraglich festgelegten Datenverarbeitung dar (Software-as-a-Service).Die zulässigen Datenverarbeitungen und die einzuhaltenden technisch-organisatorischen Datenschutzmaßnahmen müssen deutlich und verbindlich vereinbart werden.

Voraussetzung ist weiter, dass die vorgelegten Nachweise eine verlässliche Einschätzung über die Einhaltung der vereinbarten technisch-organisatorischen Maßnahmen erlauben. Dies ist bei bloßen Erklärungen des Herstellers zumeist nicht ausreichend, da ein die Aussagen verifizierendes Element fehlt. Dieses kann durch Prüfungen oder Audits mit entsprechenden Zertifikaten oder Testate ersetzt werden, wenn gewährleistet ist, dass die Prüfung durch eine unabhängige und fachkundige Stelle auf der Grundlage des vertraglich vereinbarten IT-Sicherheits- und Datenschutzkonzepts (§ 4 Abs. 2 Nr. LDSG bzw. § 11 Abs. 2 Satz 2 Nr. 3 BDSG) erfolgt und anhand einer Dokumentation angemessen nachvollzogen werden kann.

Wenn US-Anbieter von Cloud-Lösungen beauftragt werden, kann vor dem Hintergrund US-amerikanischer Rechtsvorschriften problematisch sein, dass ein Zugriff durch US-Stellen möglich ist, auch wenn die Daten in Rechenzentren in der Europäischen Union verarbeitet werden (https://netzpolitik.org/2012/us-patriot-act-erlaubt-zugriff-auf-daten-in-der-cloud-auch-auserhalb-der-usa/). Dies wird durch eine aktuelle Entscheidung des United States District Court Southern District of New York gegenüber der Microsoft Corporation belegt, in der diese zur Herausgabe von Daten verpflichtet wird, die auf Cloud-Servern innerhalb der Europäischen Union gespeichert sind (http://www.cr-online.de/blog/2014/05/13/datenherausgabepflicht-fuer-cloud-anbieter-nach-us-recht-vs-eu-datenschutzrecht/). Vertragliche Regelungen vermögen dies nicht zu verhindern.

Unabhängig von dem oben Gesagten hat der Europäische Gerichtshof mit seinem Urteil vom 6. Oktober 2015 die Wirksamkeit der Standardvertragsklauseln der EU-Kommission in Frage gestellt. Er hat ausdrücklich zwar nur die Safe Harbor-Entscheidung der EU-Kommission für ungültig erklärt und damit vielen Datenübermittlungen in die USA die rechtliche Grundlage entzogen. Darüber hinaus aber kann dieses Urteil auch Auswirkungen auf andere Instrumente zur Legitimation des transatlantischen Datentransfers entfalten, die daher auf dem Prüfstand stehen.

Je nach Art der Datenverarbeitung steht dies einer Nutzung von Cloud-Lösungen von US-Anbietern entgegen. Möglich erscheint diese noch am ehesten dort, wo lediglich Speicherplatz oder Bandbreite aus der Cloud bezogen werden. Beim konsequenten Einsatz kryptografischer Verfahren können solche Szenarien datenschutzgerecht gestaltet werden. Weitere Ansatzpunkte sind Treuhänderszenarien, bei denen der Cloud-Anbieter keine Möglichkeit des Datenzugriffs hat. Wo jedoch personenbezogene Daten außerhalb einer wirksamen Kontrolle der Cloud-Nutzerinnen und -Nutzer verarbeitet werden, können die Risiken unter den gegenwärtigen Bedingungen in der Regel nicht kompensiert werden (vgl. 23. Tb., Tz. I-1.3).

Cloud-Lösungen von US-Anbietern wie Office 365, bei denen in der Regel eine Verarbeitung personenbezogenen Daten im Klartext erfolgt, sind vor diesem Hintergrund als problematisch anzusehen; letztlich bedarf es einer Bewertung im Einzelfall. Die Nutzung derartiger Verfahren für die Verarbeitung von Daten, die besonderen Berufs- und Amtsgeheimnissen unterliegen (§ 203 StGB), von besonderen personenbezogenen Daten nach § 3 Abs. 9 LDSG bzw. § 3 Abs. 9 BDSG oder von Verschlusssachen scheidet aus datenschutzrechtlicher Sicht aus.

14.3 Datenschutzkonforme Nutzung des Filehosting-Dienstes „WeTransfer“

Im Berichtszeitraum wurde der LfDI mehrfach hinsichtlich einer datenschutzkonformen Nutzung von FileHosting-Diensten wie z.B. „WeTransfer“ um Beratung gebeten. In der Regel betraf dies die Bereitstellung von Dokumenten, die die für einen E-Mail-Versand zu umfangreich sind und im Wege eines Downloads über eine Filehosting-Plattform wie z.B. „WeTransfer“ zur Verfügung gestellt werden sollen.

Dabei handelt es sich um einen Informationsdienst nach § 1 TMG, in dessen Rahmen sich die jeweilige Stelle der technischen Möglichkeiten von WeTransfer.com bedient. Das Unternehmen hat seinen Sitz in den Niederlanden und unterliegt damit europäi-

schem Datenschutzrecht. In der Datenschutzerklärung wird jedoch darauf hingewiesen, dass im Rahmen der technischen Abwicklung des Dienstes Daten auch auf Servern außerhalb der Europäischen Union verarbeitet werden können.

Unabhängig vom Inhalt der über „WeTransfer“ übertragenen Dateien werden an personenbezogenen bzw. personenbeziehbaren Daten ggf. folgende Angaben verarbeitet:

- E-Mail-Adresse der Absendenden
- E-Mail-Adresse der Empfangenden
- IP-Adressen von Absendenden und Empfangenden sowie
- etwaige Nachrichten an Empfangende

Deren Verarbeitung ist im Rahmen des § 12 TMG grundsätzlich zulässig. Für personenbezogene Daten in den Mediendateien selbst gelten die allgemeinen Datenschutzregelungen.

Die Bereitstellung erfolgt, indem die Mediendatei zunächst auf die Plattform wetransfer.com hochgeladen und anschließend eine URL für den Download durch den bzw. die Empfangenden erzeugt wird (Downloadlink). Der Download selbst muss vom Empfangenden vorgenommen werden. Für diesen Prozess bietet „WeTransfer“ zwei Möglichkeiten an:

a) Im Rahmen des Uploads können die E-Mail-Adresse des Bereitstellenden (notwendig für die Versandbenachrichtigung) sowie eine oder mehrere Empfängeradressen angegeben werden, an die der Downloadlink im Anschluss von „WeTransfer“ per E-Mail verschickt wird. Dem kann dabei eine Nachricht an den bzw. die Empfangenden mitgegeben werden.

b) Alternativ kann beim Upload als Option der erzeugte Downloadlink angezeigt, übernommen und durch den Bereitstellenden auf eigenen Wegen weitergegeben werden (z.B. eigene E-Mail, Website, Textnachricht o.ä.). Die Angabe der E-Mail-Adressen von Absendenden und Empfangenden ist hierbei gegenüber „WeTransfer“ nicht erforderlich.

Beim Abruf der Mediendatei wird u.a. die IP-Adresse der abrufenden Nutzerinnen und Nutzer übertragen, die ausweislich der Datenschutzerklärung von „WeTransfer“ für die Dauer von zwölf Monaten gespeichert wird. Zweck dieser Speicherung sei die Verfolgung etwaiger Missbräuche. Die Erforderlichkeit zur Verarbeitung der IP-Adresse nach § 15 Abs. 1 TMG ist mit einem erfolgreichen Download abgeschlossen. Für eine darüber hinausgehende Verarbeitung bedarf es einer anderweitigen Rechtsgrundlage. Als eine solche käme nach § 12 Abs. 1 TMG die Einwilligung der Nutzerinnen und Nutzer in Betracht. Diese kann nach § 13 Abs. 2 TMG unter den dort genannten Voraussetzungen elektronisch erteilt werden.

Mit Blick auf § 1 Abs. 3 LDSG sollte eine Nutzung des „WeTransfer“-Dienstes in Form der Alternative b) erfolgen, d.h. der Downloadlink sollte den Empfangenden durch die verantwortliche Stelle zur Verfügung gestellt werden, z.B. via E-Mail. Neben dem Verzicht auf die Preisgabe der E-Mail-Adressen böte dies die Möglichkeit, in der E-Mail auf die Speicherung der IP-Adressen beim Abruf hinzuweisen (vgl. § 13 Abs. 1 TMG). Ein nachfolgender Download, der in Kenntnis dieses Sachverhalts erfolgt, wäre als eindeutige bewusste Handlung i.S. des § 13 Abs. 2 Nr. 1 TMG und damit als Einwilligung zu sehen. Die Entscheidung der Nutzerinnen und Nutzer, ob sie diese Möglichkeit in Anspruch nehmen, liegt letztlich bei ihnen.

Für die Alternative a) müsste ggf. eine Auftragsdatenverarbeitung vereinbart werden, die den Anforderungen des § 4 LDSG genügt. Angesichts der bestehenden Alternative b) dürfte jedoch fraglich sein, ob die Verarbeitung der E-Mail-Adresse bei WeTransfer im Sinne des § 15 Abs. 1 TMG erforderlich ist, so dass dies ebenfalls nur auf der Grundlage einer (elektronischen) Einwilligung möglich wäre.

14.4 Das Standard-Datenschutzmodell als Maßstab für die datenschutzkonforme Gestaltung von Datenverarbeitungsverfahren

Bei Datenschutzprüfungen werden häufig die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html) herangezogen, weil es Datenschutz ohne Maßnahmen

und Mechanismen der Datensicherheit nicht geben kann und ein standardisiertes Prüfmodell Vorhersehbarkeit und Verlässlichkeit bietet. Um den Anforderungen des Datenschutzes zu genügen, sind über den Aspekt der IT-Sicherheit hinaus jedoch weitere Gesichtspunkte in den Blick zu nehmen. Dies ist im Baustein 1.5 „Datenschutz“ (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html) der IT-Grundschutzkataloge des BSI dargestellt, der über technisch-organisatorische Punkte hinaus die Zulässigkeit der Datenverarbeitung, die Wahrnehmung der Betroffenenrechte oder die Datensparsamkeit anspricht.

Hier setzt das im Auftrag der Datenschutzkonferenz entwickelte Standard-Datenschutzmodell (SDM) an. Es fußt auf dem Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ der Datenschutzkonferenz vom 18. März 2010. Das Modell greift die klassischen Ziele der IT-Sicherheit auf und ergänzt diese um weitere, datenschutzbezogene Schutzziele:

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit
- Transparenz,
- Intervenierbarkeit und
- Nichtverkettbarkeit sowie das
- Prinzip der Datensparsamkeit.

Das Standard-Datenschutzmodell bezieht sich dabei auf Daten, IT-Systeme und Prozesse und legt eine Risiko basierte Beurteilung zugrunde, indem es zwischen normalem, hohem und sehr hohem Schutzbedarf unterscheidet. Alle Schutzziele basieren auf gesetzlichen Vorgaben, wie sie auch in der EU-Datenschutzreform enthalten sein werden. Der wesentliche Unterschied zum IT-Grundschutz besteht darin, dass die Gewährleistungsziele von grundrechtlichen Anforderungen abgeleitet sind. Das bedeutet, dass vor allem auf den Schutz der Betroffenen bei der Verarbeitung personenbezogener Daten abgestellt wird und nicht primär auf die Sicherheit von Geschäftsprozessen.

Das Standard-Datenschutzmodell orientiert sich methodisch am IT-Grundschutz des BSI, überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen, gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse und berücksichtigt drei Schutzbedarfsabstufungen. Es berücksichtigt die grundlegenden Datenschutzprinzipien Zweckbindung, Erforderlichkeit, Wahrnehmung der Betroffenenrechte und Transparenz der Verarbeitung. Ein auf die Gewährleistungsziele abgestimmter Maßnahmenkatalog ist in Vorbereitung.

Das Modell gibt eine Methode an die Hand, um mit Hilfe von Schutzzielen rechtliche Datenschutzanforderungen sowie technische und organisatorische Funktionen und Schutzmaßnahmen in ein systematisch bestimmbares Verhältnis zueinander zu setzen. Es ermöglicht den für die Verarbeitung verantwortlichen Stellen, geeignete Maßnahmen zu planen und umzusetzen und fördert damit die datenschutzgerechte Gestaltung von informationstechnischen Verfahren. Den Aufsichtsbehörden bietet das Modell die Möglichkeit, mit einer einheitlichen Systematik transparent und nachvollziehbar ein IT-Verfahren und seine Komponenten zu bewerten.

Die Datenschutzkonferenz hat das Handbuch zum Standard-Datenschutzmodell im Oktober 2015 zustimmend zur Kenntnis genommen und empfiehlt dessen Anwendung in der Kontroll- und Beratungspraxis.

Im Rahmen der Novellierung des Datenschutzes auf europäischer Ebene soll das Standard-Datenschutzmodell als Prüfmaßstab bei der Umsetzung der europäischen Datenschutz-Grundverordnung vorgeschlagen werden.

Die vorliegende Version 0.9a steht zur Kommentierung durch die Fachöffentlichkeit zur Verfügung.

- Handbuch „Standard-Datenschutzmodell“ Version 0.9a (http://www.datenschutz.rlp.de/downloads/mat/SDM-Handbuch_V09a.pdf)
- Tagungsband AK Technik-Workshop 2015 „Das Standard-Datenschutzmodell – der Weg vom Recht zur Technik" (http://www.datenschutz.rlp.de/downloads/mat/Tagungsband_SDM.pdf)

14.5 Einsatz des Betriebssystems Microsoft Windows 10

Mit der Einführung von Windows 10 hat Microsoft grundlegende konzeptionelle Veränderungen seines Betriebssystems vorgenommen. Im Unterschied zu den bisherigen Versionen greift Windows 10 verstärkt auf internetbasierte Cloud-Services zurück. Die Nutzung einer Reihe von Funktionen ist danach nur möglich, wenn eine permanente Internetverbindung zu Microsoft besteht. In diesem Zusammenhang werden nach einer Standardinstallation regelmäßig eine Reihe von Daten an Microsoft übertragen. Dadurch erhält Microsoft Informationen, die es ihm erlauben, das Verhalten der Benutzerinnen und Benutzer nachzuvollziehen und zu analysieren. Um welche Daten es sich dabei handelt, ist in der Datenschutzerklärung von Microsoft dargestellt (https://www.microsoft.com/de-de/privacystatement/default.aspx).

Die Datenschutzkonferenz empfiehlt den Nutzerinnen und Nutzern Cloud-unterstützter Betriebssysteme wie Windows 10 daher, sich vor dem Kauf über die Funktionsweise zu informieren und die Möglichkeiten einer datenschutzfreundlicher Konfiguration zu nutzen (Entschließung der Datenschutzkonferenz „Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken“ vom 1. Oktober 2015 http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=090_cloud).

Soweit das Betriebssystem im behördlichen oder kommerziellen Umfeld eingesetzt wird, sind die verantwortlichen Stellen gehalten zu prüfen, wie sie bei der Nutzung des Betriebssystems ihrer datenschutzrechtlichen Verantwortung als datenverarbeitende Stelle gerecht werden können.

Erläuterungen zu den datenschutzrelevanten Einstellungsmöglichkeiten bei Windows 10:

- http://windows.microsoft.com/de-de/windows-10/windows-privacy-faq
- https://www.datenschutz.hessen.de/down-load.php?download_ID=342&download_now=1
- http://www.verbraucherzentrale-rlp.de/windows10
- http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/11/2015_okt-leitfaden-win-10.pdf

Im Zusammenhang mit der Safe Harbor-Entscheidung des Europäischen Gerichtshofs ist z.B. fraglich, in welchem Umfang und auf welcher Grundlage eine Datenübermittlung in die USA rechtlich zulässig ist (vgl. Tz. I-1.4, I-1.5). Dies bedeutet unter anderem, dass eine Übermittlung personenbezogener Daten (z.B. Kontaktdaten, Kalendereinträge) an Microsoft unterbunden werden muss, soweit diese nicht auf eine tragfähige rechtliche Grundlage, wie etwa die Einwilligung der Betroffenen, gestützt werden kann. Eine solche Übermittlung erfolgt z.B., wenn die Cloud-basierten Funktionen von Windows 10 zur Synchronisation der Einträge auf verschiedenen Geräten genutzt werden oder der Sprachassistent Cortana genutzt wird. Ähnliches gilt, wenn ein Zugriff auf E-Mail-, Kontakt- und Kalendereinträge durch andere Anwendungen zugelassen wird.

Bei einem geschäftsmäßigen Einsatz von Windows 10 sollten die entsprechenden Funktionen bzw. Übermittlungen daher deaktiviert und das Betriebssystem mit einem lokalen Benutzerkonto anstelle eines Microsoftkontos genutzt werden. Nicht zuletzt aufgrund der offenen Fragen hinsichtlich der Cloud-basierten Funktionen sollte seitens der datenverarbeitenden Stellen sichergestellt werden, dass mit der jeweiligen Nutzung des Betriebssystems Windows 10 den datenschutzrechtlichen Anforderungen entsprochen wird.

14.6 Datenschutz-Icons – Ein Bild sagt mehr als tausend Worte

Bereits seit einiger Zeit gibt es Überlegungen, die bislang in der Regel in Textform vorhandenen Datenschutzerklärungen bzw. Hinweise zur Erhebung und Verarbeitung von Nutzungsdaten durch entsprechende Symbole zu ergänzen oder solche für eine kompakte Erstinformation der Nutzerinnen und Nutzer zu verwenden. Exemplarisch kann hier auf die Aktivitäten der Federal Trade Commission aus dem Jahr 2012 verwiesen werden (http://www.insideprivacy.com/united-states/federal-trade-commission/ftc-working-on-privacy-nutrition-label-industry-focusing-on-icons/). Für die

Gestaltung entsprechender Symbole wurde bereits eine Reihe von Vorschlägen gemacht:

- https://netzpolitik.org/2007/iconset-fuer-datenschutzerklaerungen/
- http://www.azarask.in/blog/post/privacy-icons/
- http://blog.momswithapps.com/privacy-icon/

Auch entsprechende Projekte sind zum Teil bereits realisiert worden, etwa von der Mozilla-Foundation (https://wiki.mozilla.org/Privacy_Icons) oder der Digital Advertising Alliance (http://www.youradchoices.com/learn.aspx), wobei gerade Letzteres eine gewisse Verbreitung erfahren hat.

Angesichts der Vielzahl von Szenarien, in denen Nutzungsdaten verarbeitet werden, ist aus Sicht des Datenschutzes eine für die Nutzerinnen und Nutzer leicht erfassbare und einzuordnende Information, die erkennen lässt, ob und wie Nutzungsdaten verarbeitet werden, von besonderer Bedeutung. Dies gilt allgemeine, in besonderer Weise jedoch für mobile Endgeräte mit geringerer Bildschirmgröße. Entsprechende Aktivitäten sind daher aus Sicht des Datenschutzes zu begrüßen.

Der Ansatz hat auch Eingang in die kommende europäische Datenschutz-Grundverordnung gefunden. Danach sollen Nutzungsbedingungen künftig leicht verständlich formuliert sein; standardisierte Symbole (Icons) sollen die Zustimmung oder Ablehnung vereinfachen (vgl. Erwägungsgründe (48) und (129) sowie Art. 12 des Verordnungsentwurfs).

Aus Sicht des LfDI kommt es bei der Entwicklung und dem Einsatz entsprechender Symbole auf zwei grundsätzlich Aspekte an:

Zum einen sollten durch die Symbole die wesentlichen Aspekte abgedeckt werden, die für die Entscheidung der Nutzerinnen und Nutzer, ob sie einer entsprechenden Datenverarbeitung zustimmen, von Bedeutung sind. Dies geht über die Information zur Verarbeitung der IP-Adresse hinaus und betrifft die Zwecke der Verarbeitung, die anonyme oder pseudonyme Verarbeitung, die Dauer der Speicherung, die Weitergabe an Dritte, u.a.m. Zum anderen bedarf es eines definierten und standardisierten Satzes an Symbolen, um die notwendige Eindeutigkeit bei der Aussage der Symbole sicherzustellen und die Verbreitung und Erkennbarkeit zu fördern.

Eine entsprechende Diskussion wird im Zusammenhang mit der Umsetzung der europäischen Datenschutz-Grundverordnung auf europäischer Ebene geführt werden. Art. 66 des Verordnungsentwurfs weist dem künftigen Europäischen Datenschutzausschuss hier die Aufgabe zu, der Europäischen Kommission entsprechende Vorschläge zu unterbreiten.

14.7 Transparenz, Vertrauen und Sicherheit in der digitalisierten Welt – Datenschutzzertifizierung und Datenschutzsiegel

Gütesiegel und Zertifikate zum Datenschutz sind wertvolle Instrumente, um gegenüber Verbraucherinnen und Verbrauchern die Datenschutzkonformität digitaler Angebote nachzuweisen. Glaubwürdige Prüfzeichen erleichtern die Entscheidung zwischen verschiedenen Anbietern und Angeboten, sie geben Orientierung und können das Vertrauen in neue Technologien fördern. Mit Ihnen kann z.B. zum Ausdruck gebracht werden, dass auf eine besonders datensparsame Gestaltung geachtet wurde oder datenschutzfreundliche Technologien wie Pseudonymisierung oder Anonymisierung zum Einsatz kommen.

Für Unternehmen setzen derartige Gütesiegel und Zertifikate Anreize in Form zusätzlicher Werbemöglichkeiten und bringen Wettbewerbsvorteile. Sie schaffen Transparenz, Vertrauen und Sicherheit, innerhalb von Unternehmen und gegenüber Kundinnen und Kunden und Geschäftspartnerinnen und -partnern. Die Vorteile entsprechender Zertifizierungen von Unternehmen waren daher Gegenstand der am 15. Oktober 2015 gemeinsam mit der Landesregierung veranstalteten Landesdatenschutzkonferenz.

Landesdatenschutzkonferenz Rheinland-Pfalz
Transparenz, Vertrauen und Sicherheit in der digitalisierten Wirtschaft (vgl. Tz. III-2.3)
http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2015101501

Die genannten Aspekte spielen primär in der Wirtschaft eine Rolle, wo Verbraucherinnen und Ver-

braucher zwischen verschiedenen digitalen Angeboten wählen können. Aus sachlichen und kompetenzrechtlichen Gründen dürfte hier für landesbezogene Regelungen kein Raum sein. Gleichwohl sollten die bestehenden Einwirkungsmöglichkeiten, auf nationaler Ebene entsprechende Mechanismen zu etablieren, genutzt werden. Dies gilt aus Sicht des LfDI insbesondere für die absehbaren Rechtsangleichungen, die im Zusammenhang mit der Umsetzung der europäischen Datenschutz-Grundverordnung erfolgen müssen (vgl. Tz. I-1.3). Diese sieht die Einführung von Zertifizierungsverfahren, Datenschutzsiegeln bzw. Prüfzeichen vor. Als inhaltlicher Maßstab eignet dabei insbesondere das im Projekt „EuroPriSe“ entstandene europäische Datenschutzgütesiegel (www.european-privacy-seal.eu).

Formelle Nachweise der Datenschutzkonformität sind jedoch auch in der Verwaltung von Bedeutung. Mit Blick auf das zunehmende Angebot digitaler E-Government-Dienste sollten die Möglichkeiten genutzt werden, gegenüber Bürgerinnen und Bürgern durch entsprechende Kennzeichnungen auf eine datenschutzfreundliche oder datensparsame Gestaltung der Verfahren hinzuweisen. Entsprechende Nachweise geben Sicherheit und fördern das Vertrauen in die elektronischen Lösungen der Verwaltung. Geeignete Möglichkeiten ergeben sich auch hier im Rahmen der kommenden Datenschutz-Grundverordnung. So könnte bei der notwendigen Anpassung des Landesdatenschutzgesetzes analog zu der bereits vorhandenen, bereichsspezifischen Regelung in § 41a POG vorgesehen werden, dass öffentliche Stellen zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren sowie ihre technischen Einrichtungen prüfen und bewerten lassen. Einen entsprechenden Vorschlag hat der LfDI an die Landeregierung herangetragen.

Voraussetzung für ein glaubwürdiges Siegel ist, dass der Verleihung ein transparenter Katalog geeigneter Kriterien zugrunde liegt, deren Erfüllung in einem festgelegten Verfahren evaluiert wird. Erfahrungen des LfDI und entsprechende Untersuchungen zeigen, dass insbesondere dann, wenn die Verleihung eines Gütesiegels allein auf einer Selbsterklärung der verantwortlichen Stellen beruht oder Kriterien und Verfahren für die Vergabe des Siegels intransparent sind, nur eingeschränkt auf die mit einem Gütesiegel zum Ausdruck gebrachte Verlässlichkeit vertraut werden kann. Zentrale Aspekte für die Vergabe eines solchen Nachweises sind daher aus Sicht des LfDI

- ein transparenter Katalog geeigneter Anforderungen,
- die Prüfung und Evaluierung von deren Umsetzung durch eine fachkundige Stelle (Audit),
- die Bestätigung durch eine unabhängige Stelle (Zertifizierung),
- die Möglichkeit, bei Nichterfüllung von Anforderungen ein erteiltes Zertifikat zu entziehen,
- eine Befristung der Gültigkeit mit der Möglichkeit einer Nachzertifizierung.

Abkürzungsverzeichnis

Gesetze und Verordnungen

AEUV	Konsolidierte Fassung des Vertrages über die Arbeitsweise der Europäischen Union
AGBMG	Landesgesetz zur Ausführung des Bundesmeldegesetzes
AO	Abgabenordnung
ATDG	Antiterrordateigesetz
BDSG	Bundesdatenschutzgesetz
BezO	Bezirksordnung für den Bezirksverband Pfalz
BGB	Bürgerliches Gesetzbuch
BKAG	Bundeskriminalamtgesetz
BMG	Bundesmeldegesetz
BPersVG	Bundespersonalvertretungsgesetz
BZRG	Bundeszentralregistergesetz
EMRK	Europäische Menschenrechtskonvention
FZV	Fahrzeugzulassungsverordnung
GemO	Gemeindeordnung
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union
HeilBG	Heilberufsgesetz
HochSchG	Hochschulgesetz
IFG	Informationsfreiheitsgesetz
JI-Richtlinie	Richtlinie für den Datenschutz in Polizei und Justiz
KWG	Kommunalwahlgesetz
KWO	Kommunalwahlordnung
LDSG	Landesdatenschutzgesetz
LKO	Landkreisordnung
LKRG	Landeskrebsregistergesetz
LMG	Landesmediengesetz
LuftVG	Luftverkehrsgesetz
LuftVO	Luftverkehrs-Ordnung
MeldFortG	Gesetz zur Fortentwicklung des Meldewesens
MG	Meldegesetz
NTS	NATO-Truppenstatut

PAuswG	Personalausweisgesetz
POG	Polizei- und Ordnungsbehördengesetz
SchulG	Schulgesetz
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB V	Sozialgesetzbuch – Fünftes Buch –
SGB VIII	Sozialgesetzbuch – Achtes Buch –
SGB X	Sozialgesetzbuch – Zehntes Buch –
SGB XII	Sozialgesetzbuch – Zwölftes Buch –
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVO	Straßenverkehrsordnung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UKlaG	Unterlassungsklagegesetz
ZA-NTS	Zusatzabkommen zum NATO-Truppenstatut
ZPO	Zivilprozessordnung

sonstige Abkürzungen

Abs.	Absatz
App	Application
Art.	Artikel
Az.	Aktenzeichen
BCR	Binding Corporate Rules
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BIP	Bruttoinlandsprodukt
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BR-Drs.	Bundesratsdrucksache
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
Datenschutz-konferenz	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
Drs.	Drucksache
DuD	Zeitschrift für Datenschutz und Datensicherheit
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte-Zeitschrift
FSJ	Freiwilliges Soziales Jahr
GCHQ	Government Communications Headquarters
GKV	Gesetzliche Krankenversicherung
GVBl.	Gesetz- und Verordnungsblatt
IP	Internet Protocol
i.S.	im Sinne
i.V.m.	in Verbindung mit
KIS	Krankenhausinformationssystem
KMK	Kultusministerkonferenz
LfDI	Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
LT-Drs.	Landtagsdrucksache
MMS	Multimedia Messaging Service

NFC	Near Field Communication
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
QR	Quick Response
RFID	Radio Frequency Identification
Rs.	Rechtssache
SD	Secure Digital
SMS	Short Message Service
Tb.	Tätigkeitsbericht
TKÜ	Telekommunikationsüberwachung
Tz.	Textziffer
URL	Uniform Resource Locator
VGH	Verwaltungsgerichtshof
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
ZD	Zeitschrift für Datenschutz
ZIRP	Zukunftsinitiative Rheinland-Pfalz