Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

DATENSCHUTZBERICHT

2016/2017

www.datenschutz.rlp.de

Sechsundzwanzigster
Tätigkeitsbericht nach § 29 Abs. 2
Landesdatenschutzgesetz (LDSG)
für die Zeit vom 1. Januar 2016
bis 31. Dezember 2017

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

September 2019

INHALT

EINFÜHRUNG

I. GRUNDLINIEN DER ENTWICKLUNGEN DES DATENSCHUTZES UND DER BEHÖRDE

Dieser Tätigkeitsbericht ist der letzte, der als Zweijahresbericht erscheint. Auch hier wirft die Datenschutz-Grundverordnung ihre Schatten voraus, denn sie schreibt vor, dass künftig ein jährlicher Bericht zu erstellen ist. Im Vergleich zu den künftigen Neuerungen, die im Vorfeld der Wirksamkeit des neuen Datenschutzrechts bestehen, handelt es sich sicherlich um eine Kleinigkeit, die aber den Änderungsbedarf auch im Detail verdeutlicht.

1. Die Datenschutz-Grundverordnung und der LfDI

Viel bedeutender ist, dass die Datenschutz-Grundverordnung bereits im Vorfeld rechtspolitische und wirtschaftspolitische Auswirkungen zeigt. Sie bewirkt eine Bändigung der digitalen Quasimonopolisten! Lange Zeit sah es so aus, als könnten global tätige, digitale Unternehmen wie Facebook, Google, Amazon oder Apple mehr oder weniger im rechtsfreien Raum agieren. An geltendes Recht hielten sie sich nicht immer, insbesondere dann nicht, wenn es sich um europäisches Recht handelte. Dies scheint sich zu ändern. Die Datenschutz-Grundverordnung, die einen einheitlichen Rechtsrahmen des Datenschutzes für die Europäische Union schafft und damit für den gesamten Binnenmarkt, entfaltet Vorwirkung. Ein Binnenmarkt mit mehr als 500 Millionen Nutzerinnen und Nutzern wird unter wirtschaftlichen Gesichtspunkten so interessant, dass auch die Beachtung des Rechts, die eigentlich selbstverständlich sein sollte, verstärkt in den Blick der digitalen Weltkonzerne geraten ist.

Hinzu tritt die Rechtsprechung des Europäischen Gerichtshofes in Luxemburg, der sich als Datenschutz-Verfassungsgericht erweist. Eine Reihe von Urteilen verdeutlicht, dass es hier um eine strikte Grundrechtskontrolle geht, die erhebliche Auswirkungen für jeden Einzelnen und

insbesondere auch für die Wirtschaft hat. Die großen Leitentscheidungen der letzten Jahre, die unter den Stichwörtern Safe Harbor, Schrems usw. Furore gemacht haben, zeigen, dass es die Europäische Union mit dem Datenschutz ernst meint (vgl. II.1 Europa). Gesetzgebung und Rechtsprechung ziehen hier an einem Strang. Das hat Wirkung. Es gäbe keine European Cloud von Microsoft, wenn nicht die Datenübermittlung in die USA als teilweise rechtswidrig erachtet worden wäre. Dies ist nur ein Beispiel dafür, dass die Marktmacht der Europäischen Union Wirkung zeigt.

Die Datenschutz-Grundverordnung gibt den Datenschutzaufsichtsbehörden deutlich stärkere Befugnisse. Damit ist auch der LfDI in der Verantwortung, seine Aufgaben effektiv wahrzunehmen und seine Befugnisse angemessen auszuüben. Die Erweiterung und Stärkung dieser Befugnisse ist Teil des Konzepts der Datenschutz-Grundverordnung. Auch insoweit bestehen Vorwirkungen, da die Personalausstattung und die Zurverfügungstellung angemessener Ressourcen eine Voraussetzung für die rechtstreue Wahrnehmung der Aufgaben ist. Dies hat sich erfreulicherweise in der Personalsituation des LfDI bereits niedergeschlagen. Der Landtag hat im Doppelhaushalt 2017/2018 einen Stellenaufwuchs beschlossen. Die Wirksamkeit der Datenschutz-Grundverordnung im Mai 2018 wird weitere Herausforderungen auch an die Ressourcen des LfDI stellen, die sich dann im Haushalt 2019/2020 niederschlagen sollten. Die Organisation der Behörde des LfDI trägt den neuen Rahmenbedingungen bereits Rechnung. Nach sorgfältiger interner Vorabklärung wurde eine Neuorganisation der Behörde vorgenommen, die sich auch in modifizierter Geschäftsverteilung konkretisiert. Die Vorbereitung auf die Datenschutz-Grundverordnung, ihre Durchleuchtung und ihre Verwirklichung betreffen die gesamte Behörde. Die vier Bereiche für den materiellen Datenschutz

1. Gesundheit/Soziales/Justiz/Umwelt

2. Verwaltung/Kommunales/Wissenschaft, Forschung, Hochschulen/Statistik, Wahlen

3. Wirtschaft digital/Leben digital/Finanzen und Finanzdienstleister/Übermittlung an Drittstaaten

4. Medienbildung/Beschäftigtendatenschutz/Medien

sind auf die Themenfelder ausgerichtet, die den LfDI in den nächsten Jahren beschäftigten werden. Alle Bereiche des Datenschutzes sind von übergreifenden Themen wie etwa Fragen der Auftragsverarbeitung,

der Bestellung von Datenschutzbeauftragten, der Erweiterung von Betroffenenrechten oder der verstärkten Verhängung von Sanktionen betroffen. Die neu eingerichtete Stabsstelle Europa koordiniert diese Bemühungen im Hinblick auf die Datenschutz-Grundverordnung und hält den Kontakt zu anderen Behörden und der europäischen Ebene. Der Bereich Querschnittsaufgaben umfasst zuvorderst die Technik, zunehmend aber auch Fragen des proaktiven Datenschutzes wie Akkreditierung, Zertifizierung oder Gütesiegel. Auch eine eigene Stelle für Geldbußen wurde errichtet. Der Unsicherheit, welche Bereiche stärker und welche weniger stark belastet sein werden, ist durch flexible Mechanismen Rechnung getragen. Damit ist der LfDI zukunftsorientiert aufgestellt.

Die Europäisierung wird vor allem durch die Datenschutz-Grundverordnung, aber auch durch die Richtlinie zum Datenschutz in Polizei und Justiz verstärkt. Der Bereich Sicherheit ist daher ebenfalls als Stabsstelle eingerichtet, um dieser Übergangsphase der Umsetzung von Richtlinienvorgaben Rechnung zu tragen. Hier besteht eine enge Verknüpfung zu dem Recht der Europäischen Union.

Der LfDI vertritt seit 2017 die deutschen Länder im Beirat von Europol. Europol hat eine neue Rechtsgrundlage erhalten, mit der die Datenschutzkontrolle an den Europäischen Datenschutzbeauftragten übertragen wird. Dieser wird von einem Beirat unterstützt, der aus Vertreterinnen und Vertretern der Mitgliedstaaten besteht. Die Bundesrepublik Deutschland ist durch den Bund und einen Ländervertreter dort beteiligt. Der LfDI hat diese Aufgabe auf Bitte der Datenschutzkonferenz gerne übernommen. Im Schnittfeld zwischen Europäisierung und Sicherheit liegt ohnehin ein Schwerpunkt der Tätigkeit des LfDI. Das Verhältnis von Freiheit und Sicherheit auf der Grundlage der grundrechtlichen Rahmenbedingungen zu konkretisieren, stellt sich ihm als eine wichtige Aufgabe in der Situation dar, die sich durch technische Entwicklungen und sicherheitspolitische Herausforderungen dynamisch weiterentwickelt.

Vieles ändert sich, manches anderes bleibt beim Alten. Nach wie vor ist die Videoüberwachung ein Dauerbrenner in der Arbeit des LfDI https://s.rlp.de/videoberwachung. Das sog. Videoüberwachungsverbesserungsgesetz, das den Aspekt der Sicherheit höher gewichtet als zuvor, hat die Rahmenbedingungen für die Videoüberwachung durch private Stellen etwas geändert. Seine Verfassungsgemäßheit wird mit guten Gründen bezweifelt. Es hat allerdings auch in das Bundesdatenschutzgesetz Eingang gefunden, das neu erlassen wurde und gemeinsam mit der Datenschutz-Grundverordnung am 25. Mai 2018 in Kraft treten wird.

Dieses Bundesdatenschutzgesetz schafft die innerstaatlichen Rahmenbedingungen auf Bundesebene und damit insbesondere für den Datenschutz im Verhältnis zur Wirtschaft. Die unabhängigen Aufsichtsbehörden des Bundes und der Länder haben versucht, mit einer Reihe von Initiativen Einfluss auf die Gestaltung des Gesetzes zu nehmen. Daran war der LfDI engagiert mit beteiligt. Einige Verbesserungen konnten erreicht werden, jedoch bleiben eine Reihe von Unwägbarkeiten und zweifelhaften Regelungen. Das Landesdatenschutzgesetz muss gleichermaßen an die neuen Rahmenbedingungen angepasst werden https://s.rlp.de/ldsg. In dem Prozess der Entwicklung eines neuen Landesdatenschutzgesetzes hat sich der LfDI nachhaltig eingebracht. Frühzeitig wurden den gesetzgebenden Körperschaften Vorschläge zugeleitet, welche wesentlichen Gehalte ein künftiges Landesdatenschutzgesetz prägen sollen.

Die Bemühungen des LfDI, auf gesetzgeberische Maßnahmen gestaltend Einfluss zu nehmen, haben in hohem Maße Ressourcen gebunden. Gerade in einer Situation, in der aufgrund personeller Vakanzen und nicht besetzter Stellen Mitarbeiterinnen und Mitarbeiter ohnehin hoch belastet waren, haben die Mitarbeiterinnen und Mitarbeiter überaus engagiert und nachhaltig an den Aktivitäten auf strategischer Ebene mitgewirkt. Dafür sei ihnen ausdrücklich gedankt! Aus Sicht des LfDI hat er sein Möglichstes getan, um die rechtlichen Rahmenbedingungen im Sinne der Menschen zu beeinflussen. Der Gesetzgeber ist in seiner Entscheidung selbstverständlich frei, aber die Beratungsaufgabe des LfDI besteht dennoch.

2. Algorithmen, Big Data und ihre Rahmenbedingungen

Technische Entwicklungen treiben immer auch die Bestrebungen voran, Grundrechte informationstechnisch zu sichern. Datenschutz und IT-Sicherheit können oftmals Hand in Hand gehen. Im Zeitalter des mobilen Internets, von Smartphones mit hochauflösenden Kameras, von Wearable Computing und dem Internet der Dinge, von Smart Homes und Smart Cars, von Big Data und künstlicher Intelligenz ist Datenschutz endgültig kein abstraktes Problem mehr, dass für viele Bürgerinnen und Bürger in seinen Folgen schwer zu greifen ist. Die Probleme, die entstehen, wenn Datenschutz vernachlässigt wird, sind inzwischen für jeden im Alltag handfest zu erkennen und werden in Zukunft noch brisanter und weitreichender werden.

Für alle der aufgezählten Technologien spielen selbstlernende datenverarbeitende Systeme eine zentrale Rolle. Die allgemeine Debatte um

künstliche Intelligenz (KI oder AI-Artificial Intelligence) hat vielfältige Bezüge zum Datenschutz. Durch algorithmische Wahrscheinlichkeitsprognosen, die Big Data-Verfahren nutzen, können menschliche Eigenschaften und Verhaltensweisen immer tiefgreifender, genauer und schneller vorhergesagt werden. Diese weit fortgeschrittenen Persönlichkeitsprofile werden inzwischen genutzt, um automatisierte Entscheidungen gegenüber Menschen zu treffen (Scoring), Verhaltensvorschläge zu unterbreiten (Selbstoptimierung) und in hoch skalierbarer Weise individuell wirkungsvolle Verhaltensimpulse zu setzen (Nudging). Verhaltensbeeinflussung durch künstliche Intelligenzen wäre ohne die Verarbeitung personenbezogener Daten nicht möglich. Datenschutz wird daher im Zeitalter von künstlicher Intelligenz und Big Data endgültig zum wichtigsten Schutz der Willens- und Handlungsfreiheit und der Ausübung des Persönlichkeitsrechts.

Künstliche Intelligenzen lernen zwar, Entscheidungen selbst zu fällen. Es kommt aber darauf an, welche Kriterien insoweit zugrunde gelegt werden. Diese Kriterien werden von Menschen festgelegt. Sie sind keineswegs rein objektiv oder immer fair, sondern können schon von sich aus diskriminierend sein oder in der Anwendung diskriminierende Wirkungen entfalten. In diesem Zusammenhang hat in letzter Zeit eine Diskussion um Diskriminierungen und diskriminierende Kriterien im Zusammenhang von automatisierten Entscheidungen begonnen. Hier bestehen starke Berührungspunkte zur digitalen Ethik. Auch gegenüber digitaler Diskriminierung stellt der Datenschutz einen wichtigen Schutz dar.

Algorithmen haben kein Gewissen und kein Mitleid. Algorithmen sind aber ein zentrales Werkzeug, damit vielfältige heutige und zukünftige Anwendungen und Funktionen gute Ergebnisse erzielen können. Die allgemeine Diskussion um Algorithmen hat in den letzten beiden Jahren verstärkt Fahrt aufgenommen. Sie gründet auf der Analyse, dass Algorithmen keineswegs lediglich technische oder mathematische Spielereien darstellen. Sie können vielmehr die Demokratie beeinflussen, indem im Netz bestimmte Selektionen vorgenommen oder Richtungen eingeschlagen werden. Diskussionen um Social Bots und ihren Einfluss auf Wahlen sind hier nur ein Element der Diskussion. Die Datenschutz-Grundverordnung enthält durchaus auch in diesem Zusammenhang Inhalte, die für eine konstruktive Gestaltung fruchtbar gemacht werden können. Das Auskunftsrecht umfasst auch aussagekräftige Informationen über die Logik sowie die Tragweite von Algorithmen (Art. 15 DS-GVO). Zudem sind Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung von Daten beruhen, grundsätzlich unzulässig (Art. 22 DS-GVO). Über die rechtliche Diskussion hinaus ist aber eine gesellschaftliche Diskussion er-

forderlich, welche Anforderungen an die Wirkung künstlicher Intelligenzen im Zusammenhang von Big Data-Anwendungen zu stellen sind.

Der LfDI hat dazu in Kooperation mit der Verbraucherzentrale im Jahr 2016 eine Veranstaltung durchgeführt, die das automatisierte Fahren zum Gegenstand hatte. Die Algorithmen, die in Kraftfahrzeugen eingesetzt werden, können erhebliche Auswirkungen auf den Fahrspaß, aber auch auf die Überwachung der Betroffenen und die Verkehrssicherheit haben. Big Data-Anwendungen im Allgemeinen können nützlich sein, sie bergen aber auch Risiken.

Die Herausforderungen, Big Data-Anwendungen sinnvoll und dabei grundrechtsschonend zu entwickeln und dann auch einzusetzen, stellen sich insbesondere an die Verantwortlichen. Es ist aber auch Aufgabe des LfDI, auf die datenschutzkonforme Gestaltung moderner IT-Verfahren hinzuwirken. Aus diesem Grunde hat er Informationsoffensiven gestartet und Veranstaltungen durchgeführt, um in Kooperation mit anderen die digitale Entwicklung in grundrechtskonforme Bahnen zu lenken https://s.rlp.de/termine.

3. Datensouveränität und Profilbildung

Eine weitere gesellschaftspolitische Diskussionslinie betrifft die Datensouveränität. Von wirtschaftsfreundlicher Seite wird hier eine Neujustierung vorgeschlagen, die den angeblich überholten Datenschutz verstärkt durch das Prinzip der Datensouveränität ablösen soll. Im Kern geht es darum, dass verstärkt personenbezogene Daten in der Digitalwirtschaft ohne zu hohe Schranken verarbeitet werden können. Die Frage, wem die Daten gehören, soll dadurch beantwortet werden, dass sie zuvorderst der Wirtschaft gehören. Diese etwas überspitzte Präzisierung der Kernthese soll verdeutlichen, dass bei allem legitimen wirtschaftlichen Interesse hier über das Ziel hinausgeschossen wird.

Datensouveränität kann andererseits auch von der Nutzerin oder dem Nutzer aus gedacht werden. Die Nutzerinnen oder Nutzer sind dann der Souverän, damit dockt das Prinzip an die hergebrachte Konzeption des Selbstbestimmungsrechts über die personenbezogenen Daten einer betroffenen Person an. In jedem Falle kommen erhebliche Gestaltungsaufgaben auf Politik, Verantwortliche und auch auf die Nutzerinnen und Nutzer zu, denn die Art und Weise, wie Anwendungen genutzt werden, entscheidet über ihren wirtschaftlichen Erfolg und damit auch über die Frage, welche Anwendungen wie weiterentwickelt werden. Eine damit

eng verbundene Problemstellung ist die Zukunft der Einwilligung. In einer digitalisierten Welt wird es für den Einzelnen zunehmend schwieriger, informiert in bestimmte Dinge einzuwilligen. Gerade im Geschäftsverkehr ist es allerdings erforderlich, dass die Stellung des Einzelnen gegenüber digitalen Großkonzernen angemessen stark ist. Das Geschäftsprinzip im Zusammenhang der digitalen Wirtschaft und auf der Grundlage von sog. Big Data-Anwendungen ist es, Informationen und Daten über bestimmte Personen und Personengruppen zusammenzuführen. Problematisch daran ist regelmäßig, dass die Kriterien der Zusammenführung dem Einzelnen nicht oder nicht hinreichend bekannt sind. Durch Anreizsysteme wird außerdem versucht, möglichst viele Informationen über die Nutzerinnen und Nutzer zu erhalten. Ziel ist die Vorhersehbarkeit menschlichen Verhaltens. Dies kann mit der Freiheit des Einzelnen kollidieren.

Die Betroffenenrechte der Datenschutz-Grundverordnung ermöglichen den Schutz von Freiheit und sie sind effektiv. Hinzu kommen insbesondere die Pflichten der Verantwortlichen, angemessen und verständlich zu informieren und Transparenz herzustellen. Gerade an dieser Stelle sieht der LfDI künftig Fortschritte, weil auch digitale große Player verstärkt dazu übergehen müssen, diese Pflichten ernst zu nehmen. Vorzeichen sind durchaus erkennbar, etwa in den Bemühungen von Google, den Datenschutz aus seiner Sicht zu propagieren. Es kommen auf europäischer Ebene allerdings weitere rechtliche Vorhaben hinzu. Verhandelt wird zum einen die sog. E-Privacy-Verordnung, die spezifisch für den Bereich der Kommunikationsmedien Rahmenbedingungen setzen will. Sie betrifft künftig also gerade auch die Nutzung sozialer Medien wie Twitter oder Instagram. Zudem wird eine Richtlinie über digitale Inhalte verhandelt, bei der es darum geht, ob allgemeine Regeln über Kauf und Umtausch auch bei digitalen Inhalten anwendbar sein können https://www.lda.bayern.de/media/eprivacy_synopse.pdf. Die gesellschaftlichen und rechtlichen Diskurse in den letzten beiden Jahren werden insoweit sicherlich weitergehen und auch nach der Verabschiedung von rechtlichen Rahmenbedingungen nicht aufhören. Dann geht es um ihre Anwendung, ihre Durchführung und die Effektivierung des Schutzes des Einzelnen. Dies ist Aufgabe der Datenschutzaufsichtsbehörden.

Big Data-Anwendungen sollen Geld verdienen. Dies ist dem Grunde nach nicht ehrenrührig, es erfordert aber die Einhaltung der geltenden Rahmenbedingungen. Dies hat sich im Zusammenhang von Spracherkennungssoftware besonders deutlich herausgestellt https://s.rlp.de/bigdata. Kinderspielzeuge, die sich mit dem Internet verbinden, sind nur ein Beispiel dafür, wie Big Data-Anwendungen den Alltag durchdringen. Gerade wenn Kinder, die besonders schutzbedürftig sind, unbefangen mit

ihrer Puppe sprechen und diese Spracherkennungssoftware dann die Informationen ggf. über eine Cloudlösung weiterverarbeitet, wird die Notwendigkeit von Kontrolle und Regulierung deutlich. Spracherkennungssoftware wie Siri, Alexa, IBM Watson oder ähnliche stellen die gleichen Herausforderungen dar. Hier liegt ein zukunftsfähiger Markt. Dies betrifft auch Smart Home-Lösungen, weil man zu Hause eben per Stimme Befehle an seine Haushaltsgeräte geben kann https://s.rlp.de/smarthome. Die Frage ist nur, wer mithört. Denn sind diese Anwendungen aktiviert, werden alle Audioinformationen aufgezeichnet, verarbeitet und nach schwer oder gar nicht erkannten Kriterien weitergeleitet. Die von Amazon oder Apple erfassten Daten werden regelmäßig über die Cloud verarbeitet. Denn die Funktionen der Geräte benötigen regelmäßig die Auswertung der Sprache über das Internet im Rechenzentrum des Anbieters. Vorzuziehen sind lokale Lösungen, die eine Verarbeitung auf dem Gerät selbst ermöglichen. Zudem sollten die Geräte hinreichend abgesichert werden, damit sie nicht gehackt und missbraucht werden können, um in die Haushalte und damit die private Sphäre von Menschen einzudringen. Zumindest sind Maßnahmen der Pseudonymisierung oder am besten Anonymisierung zu ergreifen. Dies gilt für alle Anwendungen von Big Data und dem Internet der Dinge. Im Zusammenhang mit „Fake News“ und Hassbotschaften insbesondere in sozialen Netzwerken ist die Verantwortung der Intermediäre für die Inhalte ihrer Angebote und für die Verfolgung von Rechtsverstößen durch die Nutzerinnen und Nutzer stark in den Blick der Öffentlichkeit geraten https://s.rlp.de/fakenews. Intermediäre sind Betreiber von Kommunikationsdiensten wie Facebook, Google oder Twitter, die die Kommunikation zwischen einzelnen Teilnehmenden vermitteln und daher Zugriff auf die übermittelten Informationen nehmen können. Sie sind nicht nur neutrale Durchleitungsstationen, sondern greifen Daten ab und nehmen auch vielfältig Einfluss auf die Kommunikation. Daher können sich Intermediäre nicht aus der Verantwortung stehlen. Diese Verantwortung kann dem Grunde nach kaum vernünftig bestritten werden, ihre Reichweite dagegen bietet Anlass zu Diskussionen.

Hier setzt das sog. Netzwerkdurchsetzungsgesetz seinen Ansatz, das hoch umstritten, aber 2018 in Kraft getreten ist. Die Intermediäre werden darin verpflichtet, auf die Inhalte achtzugeben, die sie übermitteln und verbreiten. Facebook hat einen Beschwerdemechanismus eingerichtet, in dem geprüft wird, ob bestimmte Inhalte gelöscht werden. Auch Anträge und Anregungen von Nutzerinnen und Nutzern werden entsprechend aufgegriffen und bearbeitet. Überdies wurden die Pflichten zur Herausgabe von Bestands- und Nutzungsdaten im Telemediengesetz für die private Verfolgung von Verletzungen des Persönlichkeitsrechts (insbesondere Beleidigungen u.ä.) ausgeweitet. Gegen das Gesetz wurde

insbesondere eingewendet, dass sowohl durch das Entfernen von Inhalten, die als rechtswidrig eingestuft wurden, als auch durch die stärkere Verfolgung der Nutzung der Effekt einer „Zensur“ herbeigeführt werde.

Die Möglichkeit der Intermediäre, auf die Inhalte ihrer Dienste und damit auf die Wahrnehmungssphäre ihrer Nutzerinnen und Nutzer erheblichen Einfluss auszuüben, wurde in den letzten Jahren auch anhand von Suchmaschinen deutlich. Das sog. Recht auf Vergessen werden, dass nunmehr in Art. 17 DS-GVO seine Festlegung gefunden hat, betrifft insbesondere Suchmaschinen wie Google. Auf der Grundlage des Urteils des Europäischen Gerichtshofes zu Google Spain hat Google und haben andere Suchmaschinen einen Mechanismus eingerichtet, der Beschwerden von Betroffenen bearbeitet. Jede und Jeder kann beantragen, dass bestimmte Verweise auf sie betreffende personenbezogene Informationen gelöscht werden, insbesondere wenn die Informationen einen sehr weit zurückliegenden Sachverhalt betreffen. Das generelle Recht auf Löschung findet hier seinen spezifischen Niederschlag.

Das Internet ist eben kein rechtsfreier Raum. Auch mit den Mitteln des Internets dürfen keine Menschen herabgewürdigt oder verleumdet werden. Aus meiner Sicht ist das Netzwerkdurchsetzungsgesetz in seinem Ansatz daher durchaus zu begrüßen, weil es die Intermediäre in die Verantwortung nimmt. Einzelne Gestaltungen und Ausprägungen müssen sicherlich angesichts der Erfahrungen evaluiert und weiterentwickelt werden.

4. Rheinland-Pfalz

Datenschutz und Grundrechtsschutz sind Querschnittsthemen, die international, europäisch und national angegangen werden müssen. Auf der Ebene des Landes Rheinland-Pfalz sind insbesondere Kooperationsbemühungen hervorzuheben, die auch den LfDI beschäftigt haben. Der Digitaldialog in Rheinland-Pfalz hat in verschiedenen Zusammenhängen zu Beteiligungen des LfDI geführt https://s.rlp.de/digitaldialog. Mit einem Grundsatzpapier wurden wesentliche Positionen aus Sicht des LfDI eingebracht. In unterschiedlichen Gesprächskreisen haben Vertreterinnen und Vertreter der Behörde teilgenommen. Der LfDI hofft, dass damit eine wirksame Einflussnahme aus Sicht des Datenschutzes gewährleistet wird konnte und werde diese Bemühungen weiterführen.

Der Verbraucherdialog, den das Verbraucherschutzministerium gemeinsam mit der Verbraucherzentrale Rheinland-Pfalz und dem LfDI betreibt, hat 2016 zum Thema Smart Home ein tragfähiges und weiterführendes

Ergebnis hervorgebracht https://s.rlp.de/smarthome. Im Jahr 2017 wurde der nächste Verbraucherdialog zum Thema Wearables angestoßen, an dem der LfDI erneut Anteil hat.

Die Kooperation mit der Verbraucherzentrale Rheinland-Pfalz ist inzwischen gute Tradition https://mffjiv.rlp.de/de/themen/verbraucherschutz/forum-verbraucherdialog/. In jedem Jahr wird eine gemeinsame Veranstaltung durchgeführt. Im Jahr 2016 handelte es sich um die bereits erwähnte Veranstaltung mit den selbstfahrenden Autos. Im Jahr 2017 wurde eine Veranstaltung zum Thema Gesundheitsdatenschutz durchgeführt. Diese Veranstaltung stand aus Sicht des LfDI im Kontext des Schwerpunktthemas Gesundheit, dem das Jahr 2017 insgesamt gewidmet war. Im März 2017 konnte bereits eine Veranstaltung mit der Gesundheitsministerin durchgeführt werden, der dann im November 2017 in Kooperation mit der Verbraucherzentrale die Veranstaltung mit der Verbraucherschutzministerin folgte. Diese Veranstaltungen haben grundsätzliche Fragen der digitalen Medizin aufgegriffen und diskutiert. Im Nachgang werden weitere Aktivitäten folgen, die der LfDI gemeinsam mit anderen koordiniert, um das wichtige und doch komplizierte Thema des Gesundheitsdatenschutzes voranzutreiben.

Ein umfangreiches Projekt betraf den Datenschutz in der Kommunalverwaltung. Dieses Kommunalprojekt hat in Kooperation mit vier Kommunen aus Rheinland-Pfalz sehr praktisch und sehr sachnah das Ziel verfolgt, in unterschiedlichen Bereichen der Sozialverwaltung, der Meldebehörden und weiteren Behördenzweigen den Datenschutz zu verbessern. Der LfDI ist dabei auf viele interessierte und gutwillige Reaktionen gestoßen. Die konkreten Ergebnisse wurden auf einer Veranstaltung, zu der vielfältig Beteiligte eingeladen waren, in Diskussionsrunden vorgestellt. Sie stehen im Internetangebot des LfDI zur Verfügung https://s.rlp.de/kommunalprojekt. Die konkreten Ergebnisse haben auch die Stellung und Ausstattung der behördlichen Datenschutzbeauftragten im Visier gehabt. An diesem Punkt sind die Diskussionen besonders intensiv, auch im Nachgang, geführt worden. Die konstruktive Weiterführung dieser Diskussionen hin zu einer auch institutionell abgesicherten Wahrung des Interesses an handhabbarem effektivem Datenschutz beschäftigt den LfDI weiter.

Mit der Wirtschaft in Rheinland-Pfalz sind vielfältige Kontakte auf- und ausgebaut worden https://s.rlp.de/dsbunternehmen. Regelmäßige Gespräche werden mit einer Reihe von Beteiligten und Akteuren des Wirtschaftslebens geführt, als Beispiel seien die Gesprächskreise mit betrieblichen Datenschutzbeauftragten genannt. Im Vorfeld der Daten-

schutz-Grundverordnung besteht großer Informationsbedarf. Der LfDI versucht, mit umfangreichen Informationen in seinem Internetangebot und vielfältigen Veranstaltungen, Vorträgen und Publikationen diesem Informationsbedarf gerecht zu werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erarbeitet Kurzpapiere zum Verständnis der Datenschutz-Grundverordnung, an deren Ausarbeitung sich der LfDI beteiligt. Die Papiere werden im Internetangebot des LfDI zur Verfügung gestellt https://s.rlp.de/kurzpapieredsgvo. Hinzu kommen die Leitlinien von europäischer Seite, die aus Arbeitspapieren der sog. Artikel 29-Gruppe, in der die Datenschutzbeauftragten der Mitgliedstaaten vertreten sind, entstehen. Das Internetangebot des LfDI wird gerade an dieser Stelle ständig weiterentwickelt.

Der LfDI Rheinland-Pfalz ist ein genauer Beobachter der Technik des Internets, seiner Nutzung und auch des jeweiligen Nutzungsverhaltens. Aus diesem Grund hat er die Handlungsempfehlungen für Behörden zur Nutzung sozialer Medien überarbeitet https://s.rlp.de/sozialemedienfst. Das überarbeitete Handlungskonzept beinhaltet insbesondere, dass die Nutzung sozialer Medien nur dann zulässig ist, wenn es sich nicht um den einzigen Kommunikationskanal handelt. Es gilt das Gebot für ein Cross Media-Gebot. Behörden unterstehen einer besonderen Verantwortung. Gerade im Verhältnis zu digitalen Großunternehmen, die nicht alle rechtlichen Regeln einhalten, hat der Staat als Vorbild zu dienen. Daher muss ein Konzept entwickelt werden, welche sozialen Medien wie genutzt werden sollten. Die Gründe sind darzulegen. Auf der Grundlage eines solchen Konzepts, das die Erforderlichkeit von Datenverarbeitung in den Vordergrund stellt, kann die Arbeit von Ministerien, Behörden oder Kommunen auch soziale Medien mit berücksichtigen. Im Vordergrund dürfte dabei die Information stehen. Die drei Pfeiler für die Nutzung sozialer Medien sind dabei das Cross Media-Gebot, ein den Bedürfnissen und Rechtsregeln der jeweiligen Behörde entsprechendes Nutzungskonzept sowie die Berücksichtigung von Datenschutzaspekten durch entsprechende Hinweise. Auf dieser Grundlage sind moderne Öffentlichkeitsarbeit und weitere Aktivitäten möglich.

Der LfDI ist auf die datenschutzrechtliche Zeitenwende des Mai 2018 gut vorbereitet. Die Jahre 2016 und 2017 haben vielfältige Umstellungen gebracht. Das Erscheinungsbild nach außen mit Website und Logo wurde ebenso erneuert wie Organisation und Geschäftsverteilung. Inhaltlich wurden die europäischen Neuerungen aufgegriffen, in internen Workshops erarbeitet und in konstruktive Beratung der Verantwortlichen umgemünzt. Einige neue Kolleginnen und Kollegen sind hinzugestoßen, die sich mit großem Engagement in die Arbeit des LfDI einfügen. Damit war

eine personelle Umstrukturierung verbunden, die erfolgreich bewältigt wurde. In den letzten beiden Jahren hat sich viel getan. Der LfDI ist sicher, dass die erheblichen Umstellungen wesentlich dazu beitragen, dass seine Behörde auch unter dem Regime des künftigen Datenschutzrechts ihre konstruktive und kooperative Arbeit erfolgreich fortsetzen kann.

Prof. Dr. Dieter Kugelmann

II.
ENTWICKLUNG DES DATENSCHUTZES

II. ENTWICKLUNG DES DATENSCHUTZES

1. DIE INTERNATIONALE EBENE

1.1 Die ICDPPC

Der LfDI hat im Zusammenhang der Europäisierung und Internationalisierung des Datenschutzes auch an Aktivitäten auf globaler Ebene teilgenommen. Als Mitglied der International Conference of Data Protection and Privacy Commissioners (ICDPPC) hat er in einer Expertengruppe mitgewirkt, die versucht hat, eine länderübergreifende Zusammensetzung in der Rechtsdurchsetzung zu erleichtern. Die ICDPPC, die Internationale Datenschutzkonferenz, ist ein im Jahre 1979 gegründetes Forum, dem derzeit 120 Mitglieder aus 78 Staaten weltweit angehören. In ihrer 39. Konferenz im September 2017 in Hong Kong hat sich die ICDPPC insbesondere mit aktuellen Herausforderungen des Datenschutzes im globalen Kontext befasst und auf Vorschlag der deutschen Delegation eine Resolution zum Datenschutz in Kraftfahrzeugen verabschiedet.

1.2 Informationen zum EU-U.S. Privacy Shield - Ausbau des Online-Informationsangebots

Der LfDI hat sein Online-Informationsangebot zum EU-U.S. Privacy Shield ausgebaut. Sowohl Unternehmen als auch Bürgerinnen und Bürger finden hier wichtige Hinweise und weiterführende Links zum Thema, z.B. zur Liste aller Privacy Shield-zertifizierten US-amerikanischen Unternehmen.

Für deutsche und europäische Unternehmen, die personenbezogene Daten auf der Grundlage des Privacy Shield an US-Unternehmen übermitteln wollen, hat die Art. 29-Gruppe der Datenschutzbehörden der EU-Mitgliedstaaten anhand von vier Fragen und Antworten die wichtigsten Punkte zusammengefasst.

In einem Leitfaden der Europäischen Kommission zum EU-U.S. Privacy Shield können Bürgerinnen und Bürger mehr über ihre Rechte erfahren. Im Internetangebot des LfDI sind diese Rechte sowie mögliche Beschwerdeverfahren kurz skizziert. Dort stehen nun auch Formulare für die Einreichung von Beschwerden zum EU-U.S. Privacy Shield und für die Übermittlung von Anträgen an die US-Ombudsstelle zur Verfügung https://s.rlp.de/privacyshield.

Im Internetangebot des LfDI finden sich neben weiteren Informationen zur Datenübermittlung in die USA auch Informationen zu Datenübermittlungen in andere Drittländer, wie etwa das Kurzpapier Nr. 4 der Datenschutzkonferenz, in welchem die neue Rechtslage für Datenübermittlungen in Drittländer gemäß der Datenschutz-Grundverordnung erläutert wird https://s.rlp.de/drittlnder.

2. DIE EUROPÄISCHE EBENE

Nach jahrelangen Verhandlungen haben die Trilogparteien, d.h. die Europäische Kommission, das Europäische Parlament und der Rat der Europäischen Union, die Verhandlungen über die europäische Datenschutzreform im Dezember 2015 abgeschlossen. Damit kam ein langjähriger Prozess zum Abschluss, der eine Vereinheitlichung von Datenschutzstandards in Europa zum Ziel hatte. In der Folge sind sowohl die VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung perso-

nenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) als auch die RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Richtlinie für Polizei und Justiz) am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht worden und noch im Mai 2016 in Kraft getreten.

2.1 Datenschutz-Grundverordnung

Am 24. Mai 2016 ist die Datenschutz-Grundverordnung in Kraft getreten. Wirksam wird sie nach einer zweijährigen Übergangszeit zum 25. Mai 2018. Sie löst die Datenschutzrichtlinie von 1995 ab. Mit Wirksamwerden gilt sie unmittelbar in allen Mitgliedstaaten. Dies wird zu einem weitgehend einheitlichen Recht bei der Verarbeitung personenbezogener Daten in der gesamten Europäischen Union führen.

Die Datenschutz-Grundverordnung führt nicht zu einem völlig neuen Datenschutzrecht, sondern erhält viele bewährte Prinzipien. Auch zukünftig müssen personenbezogene Daten für eindeutig festgelegte Zwecke erhoben werden und dürfen nur soweit verarbeitet werden, wie dies mit diesen Zwecken vereinbar und für sie erforderlich ist. Die betroffenen Personen haben eine Reihe von Rechten, mit denen sie Einfluss auf die Verarbeitung ihrer personenbezogenen Daten nehmen können, z.B. das Recht auf Auskunft. Die Verarbeitung personenbezogener Daten im Auftrag ist auch nach der Datenschutz-Grundverordnung möglich.

Die Datenschutz-Grundverordnung enthält aber auch Neuerungen. Das Datenschutzrecht der Europäischen Union wird zukünftig nicht lediglich für in der Europäischen Union niedergelassene Unternehmen gelten, sondern auch für außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind (Marktortprinzip). Verantwortliche sind zur umfangreicheren Information der Betroffenen und größerer Transparenz verpflichtet als bisher. Neuerungen gibt es insoweit insbesondere in Bezug auf Löschpflichten mit dem sog. Recht auf Vergessenwerden: Machen betroffene Personen einen Löschungsanspruch geltend, müssen Verantwortliche, die diese Daten öffentlich gemacht haben, andere Stellen, die diese Daten verarbeiten, über das Löschbegehren informieren. Mit dem Recht auf Datenübertragbarkeit soll dem Einzelnen ermöglicht werden, seine personenbezogenen Daten von einem Diensteanbieter zu einem anderen zu übertragen. Die Verpflichtungen zu technischem und organisatorischem Datenschutz werden fortentwickelt. Insbesondere müssen Standardeinstellungen von Verfahren und Produkten so entwickelt und/oder ausgestaltet sein, dass nur die für den jeweiligen Zweck erforderlichen Daten erhoben werden (data protection by design und by default). Die Datenschutz-Grundverordnung fördert die datenschutzrechtliche Selbstregulierung der Verantwortlichen und hält hierzu mit Regeln für Codes of Conduct, Binding Corporate Rules und Zertifizierungsverfahren mehrere Instrumente bereit. Verantwortliche werden außerdem in Zukunft in vielen Bereichen verpflichtet sein, mit dem neuen Instrument der Datenschutz-Folgenabschätzung die von ihren Verarbeitungsvorgängen ausgehenden Risiken zu minimieren.

Die Aufsichtsbehörden bekommen eine große Anzahl neuer Aufgaben zugewiesen Auch der Bußgeldrahmen wird erheblich erweitert; in Betracht kommen Geldbußen in Höhe von

bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweit erzielten Jahresumsatzes bei einem Verstoß durch ein Unternehmen. Für jedes Unternehmen wird grundsätzlich eine Datenschutzbehörde federführend zuständig sein (one-stop-shop). Die europaweite Zusammenarbeit der Aufsichtsbehörden in grenzüberschreitenden Fällen wurde detailliert geregelt (Kohärenzverfahren). Jede Bürgerin oder jeder Bürger kann sich mit Eingaben an die Datenschutzbehörden wenden, die dann das Verfahren, wenn nötig, europäisch fortführen.

2.2 Richtlinie für Polizei und Justiz

Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung, oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit ist vom Anwendungsbereich der Datenschutz-Grundverordnung ausgenommen. Stattdessen wird der Datenschutz insoweit in der Richtlinie für Polizei und Justiz geregelt.

Die Richtlinie für Polizei und Justiz ist einen Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union am 4. Mai 2016 in Kraft getreten. Damit wird der Rahmenbeschluss von 2008 über den Schutz personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aktualisiert.

Ziel der Richtlinie ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, und die Sicherstellung, dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Europäischen Union nicht aus Gründen, die mit dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verbunden sind, eingeschränkt oder verboten wird.

2.3 Die Europol-Verordnung und ihr neues datenschutzrechtliches Kontrollregime – mit Mitwirkung des LfDI!

Die Anpassung und Modernisierung der datenschutzrechtlichen Rahmenbedingungen in der Europäischen Union haben auch vor den Europäischen Institutionen keinen Halt gemacht. Neben der Datenschutz-Grundverordnung und der Richtlinie für Polizei und Justiz wurde auch der Rechtsrahmen für Europol, der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung, erneuert. Mit dem 1. Mai 2017 ist die am 11. Mai 2016 in Kraft getretene Verordnung (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung vom 11. Mai 2016, ABl. EU vom 24. Mai 2016, S. 53 ff. (Europol-Verordnung) unmittelbar geltendes Recht geworden.

Neben zahlreichen – auch datenschutzrechtlichen – Neuerungen betrifft eine der maßgeblichen Änderungen die datenschutzrechtliche Kontrolle von Europol. Diese liegt nunmehr nach Art. 43 Europol-Verordnung bei dem Europäischen Datenschutzbeauftragten (EDSB) und nicht mehr bei der Gemeinsamen Kontrollinstanz, einem unabhängigen Gremium, bestehend aus Datenschutzaufsichtsbehörden der Mitgliedsstaaten, dessen Aufgabe darin bestand, die Einhaltung der Grundsätze des Datenschutzes durch Europol sicherzustellen.

Dem Umstand, dass die von Europol verarbeiteten Daten hauptsächlich aus den Mitgliedsstaaten stammen und damit die Aufsicht und Kontrolle der mitgliedsstaatlichen Datenschutzaufsichtsbehörden berührt sind, wird dadurch Rechnung getragen, dass bestimm-

te Kooperationsmechanismen zwischen dem Europäischen Datenschutzbeauftragten und den nationalen Kontrollbehörden in der Europol-Verordnung eingeführt wurden. Dies betrifft z.B. gemeinsame Kontrollen nach Art. 44 Europol-Verordnung und die Konsultation der betroffenen nationalen Kontrollbehörden nach Art. 47 Abs. 2 und Abs. 3 Europol-Verordnung im Beschwerdeverfahren nach Art. 47 Europol-Verordnung.

Daneben ist weiterhin eine strukturierte und beratende Zusammenarbeit in einem sog. Beirat für die Zusammenarbeit (Cooperation Board) vorgesehen (Art. 45 Europol-Verordnung). Dieser Beirat ist ein unabhängiges Beratungsgremium bestehend aus Delegierten der nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten. Zu seinen Aufgaben gehört u.a. die Befassung mit der allgemeinen Politik und Strategie Europols im Bereich der Überwachung des Datenschutzes und der Datenverarbeitungen durch Europol, mit Fragen zu der Ausübung der Rechte der betroffenen Personen und der Beratung und Erörterung von besonderen Fällen des bereits erwähnten Beschwerdeverfahrens. Instrumente dazu sind unter anderem die Erarbeitung von Stellungnahmen, Leitlinien und Empfehlungen sowie bewährte Verfahren.

In dem Beirat wirkt ein sog. gemeinsamer Vertreter jedes Mitgliedsstaats mit. Dies ist nach dem Europol-Gesetz die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Die Interessen der Länder vertritt außerdem in dem Beirat ein vom Bundesrat ernannter Vertreter der Länder. In der Drucksache 427/17 vom 07. Juli 2017 hat der Bundesrat beschlossen, gemäß § 5 EuropolG als Vertreter der Länder für den „Beirat für die Zusammenarbeit“ gemäß Art. 45 der Europol-Verordnung (EU) 2016/794 Herrn Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Rheinland-Pfalz, sowie eine seiner Mitarbeiterinnen als seine Stellvertreterin zu ernennen.

Der Beirat für die Zusammenarbeit tagte im Jahr 2017 zweimal. Die erste konstituierende Sitzung hatte vorwiegend die Verabschiedung der Geschäftsordnung und die Wahl des Vorsitzes zum Gegenstand. Anliegen des LfDI war es, darin insbesondere der föderalen Struktur Deutschlands ausreichend Rechnung zu tragen, und so ist in der Geschäftsordnung explizit vorgesehen, dass in jenen Ländern, in denen nach den nationalen Gesetzen mehrere Aufsichtsbehörden existieren - wie in Deutschland -, ein gemeinsamer Vertreter bestimmt werden soll, der wiederum einen Vertreter hat, der in den Sitzungen anwesend sein kann. In der zweiten Sitzung wurden vorwiegend Überlegungen zur zukünftigen Tätigkeit des Beirats angestellt. Die bisherigen Arbeiten der Gemeinsamen Kontrollinstanz sollen fortgeführt und an die neue Rechtsgrundlage angepasst werden. Eine enge und konstruktive Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten bei der Kontrolle von Europol ist erklärtes Ziel des Beirats.

2.4 Das Digital Clearing House – unter Mitwirkung des LfDI

Der Europäisierung trägt auch die Bemühung des Europäischen Datenschutzbeauftragten Rechnung, ein sog. Digital Clearinghouse zu initiieren. Dabei geht es um ein informelles Netzwerk von Stellen des Verbraucherschutzes, der Wettbewerbsbehörden und der Datenschutzbehörden in der Europäischen Union. Der LfDI ist von Beginn an beteiligt.

2.5 Anwendungsvorrang des Unionsrechts

Ab dem 25. Mai 2018 wird folglich in der Bundesrepublik Deutschland der Datenschutz auf drei rechtlichen Ebenen gewährleistet werden. Mit der Datenschutz-Grundverordnung und der umzusetzenden Richtlinie für Polizei und Justiz bildet das Unionsrecht den Ausgangspunkt und die wesentliche Grundlage. Das Bundesrecht wirkt zum einen durch das Bundesdatenschutzgesetz und zum anderen durch die Fachgesetze, z.B. das Sozialgesetzbuch oder die Abgabenordnung. Auf Landesebene kommt das Landesdatenschutzgesetz zur Anwendung, darüber hinaus das einschlägige Fachrecht etwa im Schulrecht oder Kommunalrecht.

Im Falle inhaltlicher Konflikte des Rechts – d.h. wenn eine Regelung im Einzelfall eine bestimmte Rechtsfolge anordnet, die der Rechtsfolge einer anderen Bestimmung widerspricht – bedarf es Kollisionsregeln. Für Verordnungen der Europäischen Union greift die allgemeine Konfliktregel des Anwendungsvorrangs. Danach ist in einem konkreten Konfliktfall eine bestimmte innerstaatliche Rechtsvorschrift unanwendbar, weil sie mit einer vorrangigen Vorschrift des Unionsrechts kollidiert. Wichtig ist, dass es sich um einen Anwendungsvorrang handelt, nicht um einen Geltungsvorrang. Das innerstaatliche Recht tritt nicht außer Kraft, sondern es behält seine Geltung für die Sachverhalte, die vom Unionsrecht nicht berührt werden.

Die konkrete Auswirkung des Anwendungsvorrangs hängt von der jeweiligen Situation des Falles ab. Zwei Fallgruppen sind hier besonders maßgeblich:

Die erste Fallgruppe betrifft die Situation, dass der deutsche Gesetzgeber noch keine Anpassungsleistung erbracht hat. Es ist nicht auszuschließen, dass nach dem 25. Mai 2018 noch Fachrecht bestehen wird, das nicht an die Datenschutz-Grundverordnung angepasst ist. Enthält das Bundes- oder Landesrecht einzelne Bestimmungen, die nicht modifiziert wurden, geht im Konfliktfall die Regelung der Datenschutz-Grundverordnung vor. Die vorrangige Regelung der Datenschutz-Grundverordnung ist anzuwenden und nicht das widersprechende innerstaatliche „Altrecht".

Die zweite Fallgruppe betrifft das neu geschaffene Recht, insbesondere das Bundesdatenschutzgesetz und das jeweilige Landesdatenschutzgesetz. Sollte hier ein Widerspruch zur Datenschutz-Grundverordnung vorliegen, geht die Regelung der Datenschutz-Grundverordnung dem Grunde nach gleichermaßen vor. Allerdings ist hier sehr viel sorgfältiger zu prüfen, ob und wie der innerstaatliche Gesetzgeber aus seiner Sicht zulässige Spielräume der Datenschutz-Grundverordnung genutzt hat.

Da die Datenschutz-Grundverordnung Öffnungsklauseln enthält, die eine Spezifizierung durch den innerstaatlichen Gesetzgeber zulassen, kommt insoweit auch eine europarechtskonforme Auslegung innerstaatlichen Rechts in Betracht. Zunächst ist also zu prüfen, ob die innerstaatliche Bestimmung in einer Weise ausgelegt werden kann, dass sie mit den europarechtlichen Vorgaben in Einklang gebracht werden kann.

Behörden selbst können das nationale Recht in einem tatsächlich vorliegenden Konfliktfall unangewendet lassen, ohne dass eine Gerichtsentscheidung erforderlich ist. Der Europäische Gerichtshof hat festgehalten, dass bei Vorliegen der Voraussetzungen für die unmittelbare Anwendung des Unionsrechts alle Träger hoheitlicher Verwaltung einschließlich der kommunalen Behörden an diese Anwendung gebunden sind. Nur so kann dem Unionsrecht in der gesamten Europäischen Union zur einheit-

lichen Anwendung verholfen werden.

Die innerstaatlichen Gerichte können im Streitfall angerufen werden. Sie werden die Zweifelsfrage hinsichtlich der Anwendung des Unionsrechts dem Europäischen Gerichtshof zur Vorabentscheidung vorlegen. Der Europäische Gerichtshof hat das letzte Wort über Auslegung und Wirkung des Unionsrechts.

2.6 Die Geburt der kleinen Schwester der Datenschutz-Grundverordnung – die ePrivacy-Verordnung

Am 10. Januar 2017 veröffentlichte die Europäische Kommission einen Vorschlag für eine ePrivacy-Verordnung, die die bestehende Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG ersetzen soll. Die neue Verordnung wird Regelungen zur elektronischen Kommunikation enthalten und präzisiert und ergänzt damit die Datenschutz-Grundverordnung. Anders als die Datenschutzrichtlinie für elektronische Kommunikation wird die ePrivacy-Verordnung unmittelbar in allen Mitgliedstaaten gelten. Nach den derzeitigen Entwürfen wird ihr Anwendungsbereich sehr weit zu verstehen sein: Neben klassischen Kommunikationsdiensten wie Telefonie und SMS fallen auch internetbasierte Kommunikationsdienste, insbesondere Messenger wie Skype oder WhatsApp, sog.OTT-Dienste (Over-the-Top-Dienste), darunter.

Das Europäische Parlament nahm den Beschluss des federführenden LIBE-Ausschusses mit zahlreichen Änderungsanträgen am 26. Oktober 2017 an. Die Reaktion des Europäischen Rates steht noch aus. Ursprünglich sollte die neue ePrivacy-Verordnung zusammen mit der Datenschutz-Grundverordnung ab dem 25. Mai 2018 gelten und das Datenschutzniveau in Europa einheitlich regeln. Dieser Zeitplan wurde nun korrigiert. Der Trilog, d.h. die abschließende gemeinsame Verhandlung des Entwurfsverfassers, der Europäischen Kommission, mit den Gesetzgebern, dem Europäischen Parlament und dem Europäischen Rat, wird in der zweiten Hälfte des Jahres 2018 erwartet. Mit einer Verabschiedung der Verordnung ist frühestens zum Jahresende 2018 zu rechnen.

Bis zum Inkrafttreten der ePrivacy-Verordnung werden somit ab 25. Mai 2018 dann auch für den Bereich der elektronischen Kommunikation die Regeln der Datenschutz-Grundverordnung gelten. Jedenfalls für den privaten Bereich wird sich die Rechtmäßigkeit der Datenverarbeitung dann an Art. 6 Abs. 1 DS-GVO messen lassen müssen. Das Telemediengesetz wird für diesen Bereich nicht mehr gelten. Ob der nationale Gesetzgeber das Telemediengesetz für öffentliche Stellen aufgrund der Öffnungsklausel des Art. 6 Abs. 2 DS-GVO fortgelten lassen wird, ist noch offen.

3. ERGEBNISSE UND KONSEQUENZEN DER EUROPÄISIERUNG

3.1 Orientierung im neuen Recht - Arbeitspapiere und Kurzpapiere

Das Ziel des EU-Gesetzgebers war ein möglichst weitgehend harmonisiertes Datenschutzrecht in der Union. Um dieses Ziel zu erreichen, ist eine harmonisierte Auslegung und Anwendung der Verordnung durch die Aufsichtsbehörden der Mitgliedstaaten in der Praxis von zentraler Bedeutung. Diese Harmonisierung betrifft einerseits die Abstimmung zwischen den Aufsichtsbehörden und andererseits innerhalb der Dienststelle. Eine der Kernaufgaben der Stabstelle Europa ist sowohl bis

zur Geltung der Datenschutz-Grundverordnung als auch darüber hinaus die Organisation dieser Harmonisierungsarbeit nach außen und nach innen.

Zwischen den Aufsichtsbehörden soll die einheitliche Anwendung der Datenschutz-Grundverordnung bis zu deren Geltung durch gemeinsame Leitlinien der Art. 29-Datenschutzgruppe sichergestellt werden, ab Geltung der Datenschutz-Grundverordnung durch den neuen Europäischen Datenschutzausschuss. Um die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen kann der Europäische Datenschutzausschuss nach Art. 70 DS-GVO von sich aus oder auf Ersuchen der Kommission u.a. Leitlinien erlassen. Im Vorgriff darauf hat die Artikel-29-Gruppe bereits erste Leitlinien zur Umsetzung der Datenschutz-Grundverordnung erarbeitet. Nach Konstituierung des EU-Datenschutzausschusses sollen diese von diesem übernommen werden. In diesem Zusammenhang wurden im Berichtszeitraum folgende Leitlinien verabschiedet:

WP242 Guidelines on the right to data portability (Leitlinien zum Recht auf Datenübertragbarkeit)

WP243 Guidelines on Data Protection Officers (‚DPOs') (Leitlinien in Bezug auf Datenschutzbeauftragte (‚DSB'))

WP244 Guidelines for identifying a controller or processor's lead supervisory authority (Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters)

WP248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679 (Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt")

WP250 Guidelines on Personal data breach notification under Regulation 2016/679

WP251 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

WP253 Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679)

WP262 Guidelines on Art. 49 of Regulation 2016/679

Die Leitlinien können im Internetangebot sowohl in englischer als auch – soweit übersetzt und veröffentlicht – in deutscher Sprache abgerufen werden: https://s.rlp.de/leitliniendsgvo.

Zudem hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) eine Reihe von Kurzpapieren zu spezifischen datenschutzrechtlichen Themen erstellt und veröffentlicht, in denen die Neuerungen durch die Datenschutz-Grundverordnung themenspezifisch für die Verantwortlichen und die betroffenen Personen aufbereitet werden und die die gemeinsame Auffassung der Datenschutzkonferenz zur Datenschutz-Grundverordnung wiedergeben. Eine Zusammenstellung der Kurzpapiere ist ebenfalls im Internetangebot abrufbar https://s.rlp.de/kurzpapieredsgvo.

3.2. Die Europäisierung und der LfDI

3.2.1. Stabsstelle Europa

Um die Durchführung der EU-Datenschutzreform beim LfDI zu organisieren und zu systematisieren, wurde zum 1. Juli 2016 die „Stabstelle Europa“ als Organisationseinheit innerhalb der Geschäftsverteilung der Dienststelle etabliert und schrittweise personell ausgestattet. Die Stabstelle ist inzwischen mit drei Referentinnen und Referenten besetzt.

Die Stabstelle Europa erfüllt im Hinblick auf die EU-Datenschutzreform und das künftige Datenschutzrecht eine Reihe von Funktionen.

Die Stabstelle Europa beteiligt sich sowohl in den Subgroups/Expert Groups der Art.-29-Gruppe als auch in der Arbeitsgemeinschaft und den Arbeitskreisen der Datenschutzkonferenz an der Erstellung der jeweiligen Papiere und bringt hier den Standpunkt des LfDI ein. Hierbei wird regelmäßig die Expertise der Bereichsleitungen, der Fachreferentinnen und -referenten und Sachbearbeiterinnen und -bearbeiter der einzelnen Bereiche eingeholt und eingebunden.

Diese Arbeit steht in einem engen Verhältnis zur Harmonisierung nach innen. Diese besteht darin, den Standpunkt der Dienststelle zu bestimmten Themenfeldern der Datenschutz-Grundverordnung herauszuarbeiten, in der Dienststelle zu verbreiten und in die Harmonisierung nach außen zu tragen. Beide Richtungen der Harmonisierung stehen dabei in einem Austauschverhältnis, da etwa die Standpunkte anderer Aufsichtsbehörden zur Diskussion innerhalb der Dienststelle und Konsolidierung des eigenen Standpunkts führen können. Innerhalb der Dienststelle wird diese Arbeit durch Workshops geleistet, die von der Stabstelle Europa organisiert und inhaltlich gestaltet werden, durch Einzelgespräche mit den Bereichsleitungen, Fachreferentinnen und -referenten und Sachbearbeiterinnen und -bearbeitern durch das Verteilen der bereits zwischen den Aufsichtsbehörden abgestimmten Materialien.

Da bereits jetzt ein Teil der Abstimmungsprozesse in englischer Sprache erfolgt, wurden die Beschäftigten des LfDI zudem bereits im Jahr 2017 dahingehend geschult. Es wurden Englischkurse angeboten, die von den Beschäftigten angenommen wurden. In diesen wurden Schwerpunkte sowohl auf die schriftliche als auch die mündliche Korrespondenz gelegt. Das Angebot soll zukünftig für Interessierte und international Involvierte weitergeführt werden.

Die Stabstelle Europa ist auch an der Öffentlichkeitsarbeit im Hinblick auf die EU-Datenschutzreform maßgeblich beteiligt: Sie gestaltet Inhalte für das Online-Informationsangebot der Dienststelle, organisiert Informationsveranstaltungen und unterstützt die Fachreferentinnen und -referenten bei Informationsveranstaltungen in ihren Bereichen. Bereits Mitte des Jahres 2017 wurde das Internetangebot um das Themenfeld „Datenschutz-Grundverordnung“ erweitert. In diesem Rahmen wurden bestimmte Themen der Datenschutz-Grundverordnung als Artikel aufbereitet und bestimmte Informationen themenspezifisch zusammengestellt, damit sich Bürgerinnen und Bürger, Verwaltungen und Unternehmen zu den Neuerungen informieren können. Dieses Angebot wird fortlaufend aktualisiert. Auch im Rahmen des im Abstand von zwei Monaten erscheinenden Newsletters des LfDI werden gezielt regelmäßig Informationen zur Datenschutz-Grundverordnung und den Aktivitäten des LfDI zur Vorbereitung der Verantwortlichen zur Verfügung gestellt. Besonderes Interesse an den Neuerungen der Datenschutz-Grundverord-

nung konnte zudem durch den Adventskalender des LfDI zur Datenschutz-Grundverordnung geweckt werden. Am 1. Dezember 2017 startete erstmals der virtuelle Adventskalender des LfDI. Im Internetangebot des LfDI wurde bis Weihnachten hinter jedem der 24 digitalen Türchen eine Frage mit Antwort zu dem neuen Datenschutzregime der Europäischen Union und den daraus folgenden zahlreichen praktischen Konsequenzen für die Nutzerinnen und Nutzer, die Unternehmen und die Verwaltungen in Rheinland-Pfalz veröffentlicht. Die Türchen wurden in einen ausführlichen „Frequently asked Questions"-Katalog überführt, der auf dem Internetangebot unter dem Themenfeld zur Datenschutz-Grundverordnung verfügbar ist https://s.rlp.de/faqdsgvo.

Sowohl öffentliche als auch nicht-öffentliche Stellen treten auch initiativ bereits seit Inkrafttreten der Datenschutz-Grundverordnung mit konkreten Fragen zur Umsetzung des künftigen Datenschutzrechts im eigenen Unternehmen an den LfDI heran. Der LfDI kommt diesen Anfragen mit seinem Beratungsangebot nach. Dabei arbeitet die Stabsstelle Europa in der Regel mit den jeweils zuständigen Fachreferentinnen und -referenten zusammen, um den Verantwortlichen die bestmögliche Beratung zur Umsetzung des neuen Rechts zukommen zu lassen. Dabei geht es häufig um die Ausgestaltung des internen Datenschutzmanagements, die Überarbeitung bereits genutzter Instrumente, wie z.B. Einwilligungsformulare, Verträge zur Auftragsdatenverarbeitung, etc.; allerdings erreichen den LfDI auch komplexe Anfragen zu künftigen Konzernstrukturen mit der rechtlichen Gestaltung von Datenübermittlungen in Drittstaaten.

3.3 Rechtsprechung des Europäischen Gerichtshofs

3.2.1 Vorratsdatenspeicherung

Im Urteil des Europäischen Gerichtshofs vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15, Tele2 Sverige AB/Post-och telestyrelsen und C-698/15 Secretary of State fort he Home Department/Tom Watson u.a. erklärte das Gericht die Vorratsdatenspeicherung einer unbegrenzten Anzahl von Personen ohne Anlass für unzulässig. Konkret ging es um Regelungen in Schweden und Großbritannien, die entsprechende Vorratsdatenspeicherungen vorsahen. Der Europäische Gerichtshof sieht in den nationalen Regelungen einen Verstoß gegen das Europarecht.

Damit wurde klargestellt, dass das Europarecht auf Regelungen zur Vorratsdatenspeicherung von Daten auch künftig anwendbar ist. Maßstab sind die Grundrechte auf Privatleben, Datenschutz und freie Meinungsäußerung der europäischen Grundrechtecharta. Die den gegenständlichen nationalen Vorschriften zugrunde liegende Richtlinie über die elektronische Kommunikation ist geltendes Recht und wird derzeit immer noch bearbeitet.

Der Europäische Gerichtshof sieht innerstaatliche Regelungen zur umfangreichen Speicherung von Daten nur dann als gerechtfertigt an, wenn dies der Bekämpfung schwerer Straftaten dient. Er stellt fest, dass aus der Gesamtheit der umfangreichen gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der Personen gezogen werden können, die letztlich zu einem besonders schwerwiegenden Eingriff führen. Eine gezielte Speicherung aus bestimmtem Anlass ist sehr viel eher möglich. Die Zugriffsregelung für die Sicherheitsbehörden muss aber die materiellen und verfahrens-

rechtlichen Voraussetzungen nach einem objektiven Maßstab festlegen.

Das Urteil des Europäischen Gerichtshofs geht in seinen Wirkungen über die Vorratsdatenspeicherung hinaus. Jede Maßnahme der Sicherheitsbehörden, die keinen konkreten Anlass hat und dabei einen sehr großen Personenkreis erfasst, ist allenfalls unter engen Voraussetzungen zur Bekämpfung schwerer Kriminalität möglich. Dies betrifft auch Maßnahmen der Polizeigesetze auf Länderebene, wie etwa des rheinland-pfälzischen Polizei- und Ordnungsbehördengesetzes.

3.2.2 Dynamische IP-Adressen sind personenbezogene Daten

Alle, die im Internet unterwegs sind, gleich ob als Anbieterin und Anbieter oder Nutzerin und Nutzer, benötigen eine Internetprotokoll-Adresse („IP-Adresse“). Denn nur so können Daten vom Absender zum vorgesehenen Empfänger transportiert werden. Die IP-Adresse wird den Nutzerinnen und Nutzern vom jeweiligen Internetanbieter zugewiesen; im Fall, dass man ein eigenes Angebot vorhält, als dauerhafte, statische Adresse, zum Surfen oder für die Nutzung anderer Dienste temporär als sog. dynamische IP-Adresse.

Bei den statischen IP-Adressen wird bereits seit längerem überwiegend von einem Personenbezug ausgegangen. Hinsichtlich der Frage des Personenbezugs von dynamischen IP-Adressen bestand lange Zeit Uneinigkeit.

Auf Vorlage des Bundesgerichtshofs hat der Europäische Gerichtshof nun am 19. Oktober 2016 in der Rechtssache C-582/14 Patrick Breyer/Bundesrepublik Deutschland zu dieser Frage Stellung bezogen und entschieden, dass eine dynamische IP-Adresse eines Nutzers für den Betreiber der Website zumindest dann ein personenbezogenes Datum darstellt, wenn der Betreiber über rechtliche Mittel verfügt, die es ihm erlauben, den betreffenden Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen.

In Deutschland besteht die Möglichkeit für Anbieter von Online-Mediendiensten, sich an eine Behörde zu wenden, um sodann die fraglichen Informationen vom Internetzugangsanbieter zu erlangen.

Im Zuge dessen hat der Europäische Gerichtshof auf eine weitere Vorlagefrage des Bundesgerichtshofs im gleichen Verfahren entschieden, dass das Unionsrecht einer Regelung entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann. Konkret ging es um die Regelung des § 15 Telemediengesetz.

3.2.3 Kein Recht auf Vergessenwerden im Gesellschaftsregister

Nach Auffassung des Europäischen Gerichtshofs in seiner Entscheidung vom 9. März 2017 in der Rechtssache C-398/15 Camera do Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni können die Mitgliedstaaten natürlichen Personen, deren Daten im Gesellschaftsregister eingetragen sind, nicht das Recht garantieren, nach einer bestimm-

ten Frist nach Auflösung der Gesellschaft die Löschung der sie betreffenden personenbezogenen Daten verlangen zu können. Begründet wird diese Entscheidung im Wesentlichen mit der besonderen Funktion des Gesellschaftsregisters und dem geringen Schutzbedarf der natürlichen Personen.

Mit der Offenlegung von Gesellschaftsregistern soll Rechtssicherheit in Beziehungen zwischen Gesellschaften und Dritten sichergestellt werden. Damit sollen unter anderem die Interessen Dritter gegenüber Aktiengesellschaften und Gesellschaften mit beschränkter Haftung geschützt werden, da in solchen Fällen in der Regel nur das Gesellschaftsvermögen und nicht der Gesellschafter haftet. Auch Jahre nach der Auflösung können sich noch Fragen diesbezüglich stellen.

Auch der Schutzbedarf der natürlichen Person wird insoweit vom Europäischen Gerichtshof als gering eingestuft, als es sich um eine begrenzte Zahl an personenbezogenen Daten handelt und die natürlichen Personen sich bewusst dafür entschieden haben über eine Gesellschaft am Wirtschaftsleben teilzunehmen, bei der lediglich das Gesellschaftsvermögen haftet.

Erfreulich ist insoweit, dass der Europäische Gerichtshof aber nicht ausschließt, dass in besonderen Fällen und nach Ablauf einer hinreichend langen Frist nach Auflösung der Gesellschaft der Zugang zu dem Gesellschaftsregister zumindest beschränkt werden kann. Zu derartigen Regelungen sind die Mitgliedstaaten befugt.

4. DIE NATIONALE EBENE – DER BUND

Das nationale Datenschutzrecht – sowohl auf Bundes- als auch Landesebene – bedarf der Anpassung an das europäische Reformpaket.

Zwar entfaltet die Datenschutz-Grundverordnung als Verordnung im Sinne des Art. 288 AEUV grundsätzlich allgemeine und unmittelbare Wirkung. Dennoch enthält die Datenschutz-Grundverordnung Öffnungsklauseln, die weiterhin nationale Datenschutzregelungen ermöglichen, aber auch erfordern. Dem nationalen Gesetzgeber werden nicht lediglich Regelungsbefugnisse eingeräumt, sondern auch einzelne konkrete Regelungsaufträge erteilt. Um das nationale Recht mit der Datenschutz-Grundverordnung in Einklang zu bringen, hat der Gesetzgeber die nationalen Datenschutzregelungen anzupassen, dabei die Regelungsaufträge umzusetzen und – soweit gewünscht – die ihm gegebenen Regelungsbefugnisse zu nutzen.

Im Rahmen der genannten Öffnungsklauseln verfügt der nationale Gesetzgeber über gewisse Spielräume. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat mit der Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen“ vom 6./7. April 2016 in Schwerin https://s.rlp.de/entschliessung2016 gefordert, diese Spielräume zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Dabei müssen die Nationalen Regelungen auch mit denen der Datenschutz-Grundverordnung vereinbar sein.

Aber das nationale Rechts bedarf nicht lediglich der Anpassung an die Datenschutz-Grundverordnung. Auch die Richtlinie für Polizei und Justiz muss in das nationale Recht umgesetzt werden. Bis zum 6. Mai 2018 müssen die Mit-

gliedstaaten die zur Umsetzung der Richtlinie für Polizei und Justiz erforderlichen Rechtsvorschriften erlassen haben.

Auf Bundesebene wurde von Seiten des Bundesministeriums des Innern im Jahr 2016 ein Referentenentwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 erstellt. Mit diesem Entwurf soll letztlich sowohl die Anpassung des Bundesdatenschutzgesetzes an die Datenschutz-Grundverordnung erfolgen als auch die Richtlinie für Polizei und Justiz zumindest teilweise umgesetzt werden. Dieser Ansatz führt dazu, dass das Bundesdatenschutzgesetz letztlich völlig neu gefasst wird.

Den Verbänden wurde dieser erste Entwurf am 23. November 2016 zur Stellungnahme vorgelegt. Er gelangte zudem sodann in die Öffentlichkeit. Dieser Entwurf bot erheblichen Anlass zur Kritik. Diese Kritik haben die Aufsichtsbehörden des Bundes und der Länder sowohl eigenständig als auch gemeinsam miteinander mehrfach geäußert. Unter anderem wurden „Datenschutzrechtliche Eckpunkte zu den in die Öffentlichkeit gelangten Überlegungen des Bundesinnenministeriums für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs-und Umsetzungsgesetz EU – DSAnpUG-EU)“ erarbeitet https://s.rlp.de/umsetzungdsgvo. Zum anderen erstellten die Aufsichtsbehörden der Länder Bundesratsanträge, um damit auch in einem späteren Stadium noch Einfluss auf das Gesetzgebungsverfahren nehmen zu können und letztlich ein rechtskonformes und handhabbares Bundesdatenschutzgesetz zu erhalten. Im Rahmen des Datenschutz-Anpassungs- und -Umsetzungsgesetz EU wurde das Bundesdatenschutzgesetz-neu am 30. Juni 2017 verkündet und findet mit Inkrafttreten der Datenschutz-Grundverordnung Anwendung. Letztlich konnten jedoch nicht alle Bedenken hinsichtlich der Rechtskonformität beseitigt werden.

Darüber hinaus sollen in naher Zukunft noch die bereichsspezifischen datenschutzrechtlichen Vorschriften der Bundesgesetze angepasst werden – und zwar sowohl im Hinblick auf die Datenschutz-Grundverordnung als auch in Umsetzung der Richtlinie für Polizei und Justiz.

Die Erkenntnis, dass unterschiedliche Stellen und Behörden im Zusammenhang der digitalen Wirtschaft mit ihren jeweiligen Aufgabenbefugnissen in gleiche Richtungen wirken können, ist einer neuen Regelung im deutschen Wettbewerbsrecht geschuldet. Die Änderung des Gesetzes gegen den unlauteren Wettbewerb im Jahr 2017 hat das Bundeskartellamt verstärkt einbezogen in den Schutz des Einzelnen in der digitalen Wirtschaft. Das Bundeskartellamt verfügt nun über erweiterte Handlungsspielräume, weil das Gesetz klargestellt hat, dass ein Markt auch dann vorliegen kann, wenn zwischen den Beteiligten kein Geld fließt. Wird also mit Daten „bezahlt“, kann auch insoweit ein Markt vorliegen, der aufgrund der Eintrittsschwellen nun intensiver vom Bundeskartellamt überwacht werden kann. Es hat bereits begonnen, gegen Wettbewerbsverzerrungen auf digitalen Märkten vorzugehen, indem es ein Verfahren gegen Facebook eingeleitet hat.

5. DIE NATIONALE EBENE – DAS LAND

Auf Landesebene ist von der Datenschutz-Grundverordnung vorrangig das Landesdatenschutzgesetz betroffen. Das Landesdatenschutzgesetz ist an die Begriffe, Verständnisse und Regelungen der Datenschutz-Grundverordnung anzupassen. Darüber hinaus ist das gesamte Landesrecht betroffen, soweit in den bereichsspezifischen Gesetzen datenschutzrechtliche Vorschriften enthalten sind.

Die Richtlinie für Polizei und Justiz wird unter anderem zu einer Änderung des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz führen, hat allerdings auch erhebliche Auswirkungen auf das Landesdatenschutzgesetz.

Zur Unterstützung des rheinland-pfälzischen Gesetzgebers hat der LfDI frühzeitig bereits im Jahr 2016 Empfehlungen zur Anpassung der landesrechtlichen Datenschutzregelungen an die Datenschutz-Grundverordnung und die Richtlinie für Polizei und Justiz erarbeitet und dem Ministerium des Innern und für Sport zugeleitet.

Im Berichtszeitraum wurde die Anpassung des Landesdatenschutzgesetzes sowie des bereichsspezifischen Datenschutzrechts begonnen – mit Beteiligung des LfDI im Gesetzgebungsverfahren –, allerdings noch nicht abgeschlossen.

III. ÖFFENTLICHKEITS-ARBEIT UND VERANSTALTUNGEN

III. ÖFFENTLICHKEITSARBEIT UND VERANSTALTUNGEN

Die Öffentlichkeitsarbeit des LfDI versucht, unterschiedlichste Wege zu gehen, um möglichst viele Bürgerinnen und Bürger anzusprechen https://s.rlp.de/termine. Am 16. November 2017 wurde die erste Veranstaltung der „Mainzer Vorträge zum Sicherheits- und Informationsrecht“ durchgeführt, die Prof. Dr. Matthias Bäcker von der Johannes Gutenberg-Universität gemeinsam mit dem LfDI verantwortet. Verfassungsrichter Prof. Dr. Johannes Masing erörterte Aspekte der Entscheidung zum BKA-Gesetz und damit Grundfragen von Freiheit und Überwachung im modernen Verfassungsstaat.

Mit der Reihe „Datenschutz goes Kino“ wurde ein neues Format aus der Taufe gehoben, das im CinéMayence seinen Ort gefunden hat https://s.rlp.de/datenschutzgoeskino2017. Beginnend mit „Democracy – Im Rausch der Daten“, der hochspannenden Dokumentation über das Zustandekommen der Datenschutz-Grundverordnung, wird seitdem in unregelmäßiger Folge ein Film gezeigt, der zur Diskussion über Probleme des Datenschutzes anregt. Zuletzt griff der Dokumentarfilm „Pre-Crime“ die Frage des Predicitive Policing auf, also des Einsatzes von Softwareanwendungen durch die Polizei zur Verhinderung von Straftaten. Die Diskussion im Anschluss an die Filmvorführung führt der LfDI dann mit den Besucherinnen und Besuchern. Diese erfolgreiche Zusammenarbeit mit dem CinéMayence soll weitergeführt werden. In der Diskussion mit Bürgerinnen und Bürgern verwirklicht sich die Aufgabe des LfDI, aufzuklären und zu informieren. Zugleich werden die Erfahrungen und Vorstellungen der Bürgerinnen und Bürger in die Arbeiten des LfDI eingebracht. Datenschutz im Dialog in vielerlei Zusammenhängen ist ein zwingender Bestandteil der Aufgabenerfüllung des LfDI.

Die Website des LfDI hat am 1. Januar 2017 neue Gestalt angenommen. Ein umfangreicher Relaunch hat nicht nur die Inhalte, sondern auch das gesamte Erscheinungsbild modifiziert. Im Kern ging es darum, die Website auch von mobilen Endgeräten wie insbesondere Smartphones komfortabel abrufbar zu machen. Im Zusammenhang damit hat die Behörde ein neues Logo und eine neue Corporate Identity erhalten. Der Auftritt des LfDI nach außen erscheint damit in völlig neuem Gewand.

1. VERANSTALTUNGEN

28. Januar 2016: Veranstaltungsreihe: „Datenschutz goes Kino“ – Der LfDI im Dialog mit Kinobesucherinnen und -besuchern

Anlässlich des 10. Europäischen Datenschutztags am 28. Januar 2016 hatte der LfDI zur Vorführung des Dokumentarfilms „Democracy - Im Rausch der Daten“ ins CinéMayence eingeladen. Im Anschluss an den Film diskutierte er mit den einhundert Zuschauerinnen und Zuschauern intensiv über aktuelle Fragen des Datenschutzes.

Der Film erzählt die fesselnde und hochbrisante Geschichte von Jan Philipp Albrecht, der damaligen EU-Justizkommissarin Viviane Reding und einer Handvoll Politikerinnen und Politiker, die versuchen, die Gesellschaft in der digitalen Welt vor den Gefahren von Big Data und Massenüberwachung zu schützen. Wie aktuell und spannend diese Fragen sind, bewies der bis auf

den letzten Platz besetzte Kinosaal im Institut français. Die Resonanz und die angeregte Debatte machen deutlich, dass sich die Idee, den Datenschutz mit den Mitteln des Films in das Bewusstsein der Bürgerinnen und Bürger zu bringen, bewährt. Wegen der großen Nachfrage fand eine weitere Filmvorführung statt. Auch in deren Anschluss konnten die Gäste mit dem LfDI diskutieren.

16. Februar 2016: Daten- und Verbraucherschutz goes Schule – Play your part for a better internet

Anlässlich des Safer Internet Day fand am 16. Februar 2016 im ZDF-Kongresszentrum eine zentrale Veranstaltung für die Medienscouts in Rheinland-Pfalz statt. Verbraucherschutzminister Robbers eröffnete gemeinsam mit dem LfDI und einigen Medienscouts die Veranstaltung mit einer Podiumsdiskussion.

Im Rahmen des Aktionstages hatten die Medienscouts Gelegenheit, sich in zahlreichen Workshops aus den Bereichen Verbraucher-, Daten- und Jugendmedienschutz zu informieren. Das Spektrum reichte von Urheberrechten über Big Data bin hin zum Selbstdatenschutz vor fremdem Zugriff in Bezug auf das eigene Smartphone. Auch über Themen wie Hass im Netz oder Mediennutzung für Öffentlichkeitsarbeit konnten sich die Schülerinnen und Schüler austauschen.

Die Medienscouts.rlp vereinen jugendliche Expertise mit Beratungs- und Methodenkompetenz. Das schnelllebige Internet birgt mit seiner Vielzahl unterschiedlicher und immer neuer kommerzieller Angebote Vorteile, aber auch Risiken. Deshalb ist es wichtig, dass Schülerinnen und Schüler frühzeitig lernen, Angebote und Geschäftsmodelle kritisch zu bewerten und sich sicher und selbstbestimmt im Internet zu bewegen. Damit sie dazu in der Lage sind, muss ihnen frühzeitig vermittelt werden, wie sich beispielsweise mögliche Urheberrechtsverletzungen verhindern lassen, Kostenfallen umgangen werden können und auf welche Daten ein Dienst zugreift.

Der Aktionstag ist eine Kooperationsveranstaltung des Ministeriums für Bildung, Wissenschaft, Weiterbildung und Kultur und dem Ministerium der Justiz und für Verbraucherschutz in Zusammenarbeit mit dem LfDI und weiteren Partnern.

5. Juli 2016: Das vernetzte Auto – Vernetztes Fahren braucht Daten- und Verbraucherschutz

Das vernetzte Auto war am 5. Juli 2016 Thema einer Diskussionsveranstaltung der Verbraucherzentrale Rheinland-Pfalz und des LfDI im Mainzer Landesmuseum. Weltweit arbeiten Autohersteller und Zulieferindustrie, aber auch Internetunternehmen mit Hochdruck daran, die digitale Vernetzung der Fahrzeuge auf der Straße und darüber hinaus voranzutreiben. Sensoren sollen Komfort und Sicherheit beim Fahren erhöhen. Sie erstellen aber auch Bewegungs- und Verhaltensprofile, die sensible Informationen zur persönlichen Lebensführung preisgeben.

Über die Chancen, die Risiken und eine verbraucher- und datenschutzfreundliche Gestaltung des connected car diskutierten Alexander Roßnagel, Professor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik, Thoralf Schwanitz von Google Deutschland, Dr. Monika Sebold-Bender, Chief Country P&C Officer der Generali Versicherung in Deutschland, Sebastian Greß, Stellvertreter des Konzerndatenschutzbeauftragten bei Daimler, Ulrike von der Lühe, Vorstand der Verbraucherzentrale Rhein-

land-Pfalz, Klaus Müller, der Vorstand des Verbraucherzentrale Bundesverbandes, und der LfDI.

12. Januar 2017: Webauftritt des LfDI wird bürgerfreundlicher - Neugestaltete Homepage bietet rund um die Uhr Zugriff auf die Services des LfDI

Optimiert für mobile Endgeräte erscheint die Homepage des LfDI nicht nur im neuen Gewand, sondern mit zahlreichen neuen Serviceangeboten für Bürgerinnen und Bürger und für die Verwaltungen und Unternehmen im Lande. Seit Januar 2017 können die Internetnutzerinnen und -nutzer Beschwerden, Meldungen zu Datenschutzverstößen, Anträge auf Informationszugang oder Anmeldungen zu Veranstaltungen einfacher vornehmen. Mit dem verbesserten und noch bürgernäheren Angebot möchte der LfDI deutlich machen, dass er seinen Auftrag als Wahrer der Bürgerrechte – die informationelle Selbstbestimmung und der Zugang zu Informationen – zugunsten der Bürgerinnen und Bürger versteht. Im Falle von Datenpannen können sich Unternehmen und Behörden im informativen und klar strukturierten Angebot kundig machen, wann eine solche vorliegt, welche Maßnahmen ergriffen werden müssen und über ein Formular online die Meldung an den LfDI erstatten, zu der sie gesetzlich verpflichtet sind.

2. Februar 2017: Erster Newsletter des LfDI

Am 2. Februar 2017 ist der erste Newsletter des LfDI versendet worden. In zweimonatigem Abstand informiert er seitdem die Abonnentinnen und Abonnenten über aktuelle Entwicklungen und Veranstaltungen in den Bereichen Datenschutz und Informationsfreiheit. Ziel ist es, Bürgerinnen und Bürgern, Unternehmen und der Verwaltung Informationen über die Tätigkeitsfelder des LfDI zur Verfügung zu stellen und auf weitere, vertiefende Inhalte und Artikel auf der Webseite zu verweisen.

20. März 2017: Die Ausgestaltung der Digitalisierung ist eine gesamtgesellschaftliche Aufgabe

Bei der gemeinsamen Veranstaltung „Gesellschaft im Wandel – Selbstbestimmung auf der Strecke?“ des LfDI und des rheinland-pfälzischen Gesundheitsministeriums am 20. März 2017 im Landesmuseum in Mainz beleuchteten Expertinnen und Experten die Chancen und Risiken der Vernetzung im Gesundheitswesen. Der „Megatrend“ Digitalisierung und dessen Bedeutung bei der Entwicklung eines zukunftsfähigen Gesundheitswesens waren Kernpunkte der Veranstaltung.

Es referierten und diskutierten die Gesundheitsministerin Sabine Bätzing-Lichtenthäler, die Vorstandsvorsitzende der AOK Rheinland-Pfalz/Saarland, Dr. Irmgard Stippler, Sabine Strüder von der Verbraucherzentrale Rheinland-Pfalz, Professor Dr. Ignaz Wessler, ehemals stellvertretender Vorsitzender der Ethik-Kommission bei der Landesärztekammer Rheinland-Pfalz, und der LfDI . Es herrschte ein breiter Konsens unter den Expertinnen und Experten, dass in der globalisierten Welt des 21. Jahrhunderts Datenschutz nur im Zusammenwirken aller betroffenen Akteure funktionieren könne. Die Digitalisierung des Gesundheitswesens erfordere die Entwicklung eines Systems gestufter und differenzierter Verantwortlichkeiten. Nur wenn sich alle Beteiligten ihrer Verantwortung bewusst seien, könne in einem Prozess des offenen Dialogs der Prozess der Digitalisierung auch in solch vertraulichen Zusammenhängen wie einer ärztlichen Heilbehandlung datenschutzgerecht ausgestaltet

werden.

6. und 7. April 2017: 6. Speyerer Forum zur digitalen Lebenswelt: Die Digitalisierung verstehen und gestalten

Zum nunmehr sechsten Mal fand das „Forum zur digitalen Lebenswelt“ an der Universität in Speyer statt. Im Zentrum der Tagung standen die rechtlichen Aspekten der Digitalisierung, insbesondere im Hinblick auf Big Data, die Blockchain-Technologie, digitale Grundrechte, Wahlen im digitalen Zeitalter und die Algorithmenkontrolle.

Das „Speyerer Forum zur digitalen Lebenswelt“ ist über die Jahre zu einer renommierten Ideenwerkstatt gereift, die sich der zentralen Frage widmet: „Wie wollen wir im Zeitalter des Internets leben?“. Die Referentinnen und Referenten aus Verwaltung, Wirtschaft, Forschung und Presse diskutieren und philosophieren gemeinsam mit den Teilnehmerinnen und Teilnehmern über die Zukunft unserer Gesellschaft und entwickeln zeitgemäße Lösungen für digitale Fragestellungen. Die wissenschaftlichen Leiter Prof. Dr. Hermann Hill, LfDI Prof. Dr. Dieter Kugelmann und Prof. Dr. Mario Martini freuten über die Vielzahl an Gästen aus Verwaltung, Wissenschaft, Rechtspraxis, Politik, Zivilgesellschaft und Wirtschaft.

20. Juni 2017: Das kommunale Datenschutzmanagement gemeinsam stärken

Mit einer Fachveranstaltung und der Vorlage von Best-Practice-Empfehlungen hat der LfDI das von ihm initiierte Projekt zur Stärkung des kommunalen Datenschutzmanagements erfolgreich beendet. Hochrangige Vertreterinnen und Vertreter von Kommunen und Verbänden konnten sich ein Bild von den erzielten Ergebnissen und deren Übertragbarkeit in ihre Bereiche machen.

Vertreter der Projektkommunen, des rheinland-pfälzischen Innenministeriums sowie der kommunalen Spitzenverbände würdigten die Projektarbeit im Rahmen der Veranstaltung. Zu einem erfolgreichen Datenschutzmanagement gehört neben der Bereitstellung der erforderlichen personellen Ressourcen vor allem das Bewusstsein, dass Datenschutz Grundrechtsschutz ist. Angesichts der im Mai 2018 wirksam werdenden Europäischen Datenschutz-Grundverordnung, die die Verwaltungen als Ganzes zur Sicherstellung von Datenschutz und Datensicherheit verpflichtet, sind die nun vorgelegten Empfehlungen eine gute Grundlage für die Kommunalverwaltungen, sich auf die anstehende Rechtsänderungen vorzubereiten (vgl. Tz. …).

20. Juni 2017: Zukunftsweisende Datenschutz- und Transparenz-Projekte in Rheinland-Pfalz ausgezeichnet

Die vom LfDI neu ins Leben gerufenen LfDI-Awards in den Bereichen Data Protection und Transparency wurden am 20. Juni 2017 erstmals vom Präsidenten des rheinland-pfälzischen Landtags, Hendrik Hering, und dem LfDI, Prof. Dr. Dieter Kugelmann, in einer Feierstunde im Landesmuseum Mainz überreicht.

Der LfDI verfolgt mit den Awards mehrere Ziele: Zum einen sollen neue und kluge Strategien rheinland-pfälzischer Behörden in den Bereichen Informationsfreiheit und Transparenz ausgezeichnet werden. Darüber hinaus will der LfDI ein Forum bieten, um die Ideen und Maßnahmen bekannt zu machen, und andere Behörden dazu anregen, sich mit diesen Konzepten auseinanderzusetzen und sie bei Bedarf

zu übernehmen.

Alle Preisträger stellten dem Publikum ihre Projekte in kurzen Präsentationen vor: Die Stadt Mainz wurde für ihre Awareness-Kampagne zur Informationssicherheit ausgezeichnet und die Verbandsgemeindeverwaltung Pirmasens-Land erhielt den Data Protection Award für ihr spezielles Datenschutz-Schulungskonzept für Mitarbeiterinnen und Mitarbeiter.

Preisträger des Transparency Awards war nicht eine Behörde, sondern ein Zusammenschluss mehrerer rheinland-pfälzischer Akteure, die gemeinsam die prämierte Geodateninfrastruktur möglich machen. Die zugehörige Plattform ermöglicht es Verwaltungen, von ihnen bereit gestellte Geodaten wie z.B. Bodenrichtwerte, Flächennutzungs- oder Bebauungspläne, Luftbilder oder touristische Attraktionen visualisiert sowohl auf dem zentralen Portal als auch in ihren eigenen Informationsangeboten zur Verfügung zu stellen. Mit dieser Möglichkeit, die zunehmend genutzt wird, besteht ein positiver Anreiz für die Verwaltungen, eigene Daten bereitzustellen und transparent zu machen.

29. August 2017: Pressegespräch „Best of Datenschutz – Die interessantesten Datenschutzfälle des LfDI aus den vergangenen zwölf Monaten“

Zum ersten Mal übertrug der LfDI das in der Informationsfreiheit bereits bewährte Format und lud am 29. August 2017 Vertreterinnen und Vertreter der Medien zum Pressegespräch „Best of Datenschutz – Die interessantesten Datenschutzfälle des LfDI aus den vergangenen zwölf Monaten“ ein. Thematisiert wurden u.a. die Nutzung von WhatsApp zur Bestellung von Medikamenten in Apotheken, die Videoüberwachung im Bereich der Umkleidekabinen eines öffentlichen Hallenbads und der Fall eines schlafenden Auszubildenden, der am Arbeitsplatz von einer Kollegin gefilmt wurde (vgl. Tz. ...): Der LfDI stellte die interessantesten und skurrilsten Eingaben des Jahres vor und gab den anwesenden Pressevertreterinnen und Pressevertretern Hintergrundinformationen zu einem Dutzend spannender und öffentlichkeitswirksamer Fälle.

13. November 2017: Gesundheits-Apps – Mehr Transparenz und Sicherheit erforderlich

„Der vermessene Verbraucher - Mit Gesundheits-Apps am Puls der Zeit oder gläsern wider Willen?“ war das Thema einer gemeinsamen Diskussionsveranstaltung des LfDI und der Verbraucherzentrale Rheinland-Pfalz am 13. November 2017 im Mainzer Landesmuseum. Expertinnen und Experten aus Politik, Daten- und Verbraucherschutz und Medizin beleuchteten die Chancen und Risiken von Gesundheits-Apps und Wearables im medizinischen Einsatz.

Verbraucherministerin Anne Spiegel sprach sich bei der Diskussion für zuverlässigen Datenschutz bei Gesundheits-Apps aus. Rainer Beckers, Geschäftsführer der ZTG Zentrum für Telematik und Telemedizin GmbH, stellte das Internet-Angebot App-Check vor, das Gesundheits-Apps bewertet. Dr. med. Sebastian Kuhn von der Universitätsmedizin Mainz brachte die Perspektive der Medizinerinnen und Mediziner in die Diskussion ein. Gemeinsam diskutierten sie mit Ulrike von der Lühe, Vorstand der Verbraucherzentrale Rheinland-Pfalz und dem LfDI, wie Datenschutz, medizinischer Nutzen und Verlässlichkeit der Messergebnisse in Einklang gebracht werden können, damit diese Produkte künftig auch bei der Prävention, Diagnostik und Therapie im Sinne der Patienten eingesetzt werden können.

16. November 2017: In der digitalen Gesellschaft sicher und frei leben

Prof. Dr. Matthias Bäcker, Inhaber des Lehrstuhls für Öffentliches Recht und Informationsrecht, insbesondere Datenschutzrecht an der Universität Mainz, und der LfDI haben am 16. November 2017 mit großer Resonanz die von ihnen ins Leben gerufene Reihe der „Mainzer Vorträge zum Sicherheits- und Informationsrecht“ eröffnet. Den ersten Vortrag hielt Bundesverfassungsrichter Prof. Dr. Johannes Masing. Er erläuterte das jüngste Urteil des Bundesverfassungsgerichts zum BKA-Gesetz. Sein zentrales Anliegen war es, die Fortentwicklung der Sicherheitsarchitektur mit Maß zu gestalten. Die Verfassung als Wertordnung und in ihrer Auslegung durch das Bundesverfassungsgericht würde dafür die Grundlage bilden. Der Rechtsstaat könne jedenfalls nicht um den Preis seiner Selbstpreisgabe erhalten werden.

30. November 2017: Licht auf den Datenschutz – Der Datenschutz-Adventskalender bietet Wissen zur Vorbereitung auf die Europäische Datenschutz-Grundverordnung

Am 1. Dezember 2017 startete erstmals der virtuelle Adventskalender des LfDI. Auf der Homepage des LfDI war bis Weihnachten 2017 hinter jedem der 24 digitalen Türchen eine Frage mit zugehöriger Antwort zu dem neuen Datenschutzregime der Europäischen Union und den daraus folgenden zahlreichen praktischen Konsequenzen für die Nutzerinnen und Nutzer, die Unternehmen und die Verwaltungen in Rheinland-Pfalz verborgen.

Zu den Kernaufgaben des LfDI gehört es, Bürgerinnen und Bürger, Unternehmen und öffentliche Stellen in Rheinland-Pfalz in Fragen des Datenschutzes und der Informationsfreiheit zu beraten. Da ab dem 25. Mai 2018 die Datenschutz-Grundverordnung wirksam sein wird, gibt es einen großen Bedarf an Informationen. Mit dem Adventskalender zeigte der LfDI die vielen neuen Facetten und gab Antworten auf die wichtigsten Fragen https://s.rlp.de/datenschutzadventskalender.

30. November 2017: Fortsetzung von „Datenschutz goes Kino“ am 30. November 2017 im CinéMayence zeigte „Pre-Crime – Willkommen in Deinem Minority Report“

Eine Software, die voraussagt, wo und wann ein Verbrecher zuschlägt. Was nach einem Science-Fiction-Szenario klingt, ist in Städten wie Chicago, London oder München bereits Realität. Ob ein Individuum gefährlich ist oder nicht, wird schon heute von Polizeicomputern entschieden. „Predictive Policing“ nennt sich die Methode und dieses Zukunftsversprechen ist nicht nur ein positives.

Der LfDI hatte für die Fortsetzung seiner im Jahr 2016 begonnenen Reihe „Datenschutz goes Kino“ den Film „Pre-Crime – Willkommen in Deinem Minority Report“ gewählt, um für die Risiken von Big Data zu sensibilisieren. Der Film wurde am 30. November 2017 im CinèMayence in Mainz gezeigt. Im Anschluss haben die Zuschauerinnen und Zuschauer wieder intensiv mit dem LfDI diskutiert. Mit dem Format „Datenschutz goes Kino“ erreicht der LfDI über das Medium Film Menschen aller Altersgruppen, die nach einem spannenden Kinoabend viele kritische Fragen stellen und sich – inspiriert durch den Film – mit der Frage auseinandersetzen, ob tatsächlich alle Annehmlichkeiten moderner Kommunikation und Datenverarbeitung ein Segen sind.

2. YOUNGDATA

Auch die Jugendseite der Datenschutzaufsichtsbehörden des Bundes und der Länder www.youngdata.de wurde im Berichtszeitraum kontinuierlich weiterentwickelt.

Innerhalb des Menüpunktes „Datenschutz-Tipps“ wurde der thematisch wichtige Bereich des Rechts am eigenen Bild aufgenommen. In der Rubrik „Selfies & Co“ veranschaulichen Videos, Grafiken und Texte in der bewährten Machart das Thema; weiterführendes Informationsmaterial ist in der rechten Spalte verlinkt: www.youngdata.de/datenschutz/datenschutz-tipps/selfies-co.

Darüber hinaus wurde Youngdata um ein neues Quiz erweitert. Das Quiz wurde in Zusammenarbeit mit dem Fachbereich Informatik und Mikrosystemtechnik der Hochschule Kaiserslautern entwickelt. Mit der CheckApp können Nutzerinnen und Nutzer prüfen, wie es um ihr Wissen in Sachen digitaler Selbstverteidigung bestellt ist. Ein umfangreicher Fragenpool in fünf Kategorien (Smartphones & Apps, Datenspuren, Kommunikation, Soziale Netzwerke und Onlinespeicher) muss bewältigt werden. Nach Beendigung des Quiz erhalten die Nutzerinnen und Nutzer weiterführende Informationen und wichtige Tipps und Tricks.

Seit April 2016 kann sich Youngdata als „internationales Projekt“ bezeichnen. Denn mit dem Datenschutzbeauftragten des Kantons Zürich konnte erstmals ein Kooperationspartner außerhalb der Bundesrepublik Deutschland hinzugewonnen werden.

Dank der guten Zusammenarbeit der Youngdata-Kooperationspartner konnte ein Hinweis der LfD Niedersachsen aufgegriffen und erstmal ein Datenschutz-Rap-Song („6 Regeln von Kevin - Scout bei der Beratungsplattform für Jugendliche, JUUUPORT.de) in das vielfältige Youngdata-Angebot aufgenommen werden.

IV. SACHGEBIETE DES DATENSCHUTZES – AUSGEWÄHLTE ERGEBNISSE AUS DER PRÜFUNGS- UND BERATUNGS-TÄTIGKEIT DES LFDI

IV. SACHGEBIETE DES DATENSCHUTZES – AUSGEWÄHLTE ERGEBNISSE AUS DER PRÜFUNGS- UND BERATUNGSTÄTIGKEIT DES LFDI

1. MEDIEN UND TELEKOMMUNIKATION

1.1 WhatsApp

Die Weitergabe von Chatnachrichten an Dritte beschäftigte den LfDI immer häufiger. Wiederholt wandten sich Betroffene an ihn, nachdem Chatnachrichten aus geschlossenen Benutzergruppen (z.B. unter Nutzung des Messengerdienstes WhatsApp) an Dritte weitergegeben wurden. Teilweise handelte es sich bei diesen Dritten um den Arbeitgeber der Betroffenen, der sodann mit arbeitsrechtlichen Konsequenzen drohte oder sogar Kündigungen aussprach.

Wenn die private Kommunikation unter Kollegen über einen Messengerdienst dem Arbeitgeber bekannt gegeben wird, greift dies in das Recht auf informationelle Selbstbestimmung der Kommunikationspartner ein. Grundsätzlich hat jeder Kommunikationspartner in einem Chatgespräch das Recht, selbst zu bestimmen, wem Äußerungen zugänglich gemacht werden, z.B. nur einem Gesprächspartner, einem bestimmten Adressatenkreis oder der Öffentlichkeit. Auch wenn z.B. an einem WhatsApp Chat mehrere Personen teilnehmen, wird dieser damit nicht öffentlich. Der Inhalt des Chats darf daher ohne die Einwilligung der Gesprächspartner nicht weitergegeben werden.

Ein Arbeitgeber darf die Daten aus einem privaten Chat u.a. nur dann erheben, wenn dies nach § 32 Abs. 1 Satz 1 BDSG für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich war. Dürfen die Daten vom Arbeitgeber nicht erhoben werden, dürfen darauf auch keine arbeitsrechtlichen Maßnahmen gestützt werden (Verwertungsverbot). In der Regel sind private Unterhaltungen in Chats – auch wenn die Unterhaltungen unter Kollegen stattfinden – nicht für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich (vgl. Arbeitsgericht Mainz, Urteil vom 15. November 2017, Az. 4 Ca 1240/17). Nur in seltenen Ausnahmefällen ist eine Weitergabe datenschutzrechtlich gerechtfertigt.

Eine Aufarbeitung und rechtliche Einschätzung zu diesem Thema steht im Internetangebot des LfDI zur Verfügung: https://s.rlp.de/chatnachrichtenarbeitgeber1.1.2 Die Nutzung von WhatsApp und die damit verbunden datenschutzrechtlichen Probleme

WhatsApp ist ein sog. Instant-Messenger-Dienst, der es erlaubt, zwischen registrierten Nutzerinnen und Nutzern Text- und Sprachnachrichten sowie Fotos, Videos, Audiodateien und Kontaktdaten auszutauschen und via IP-Telefonie über das Internet zu telefonieren. Der Dienst wurde 2009 gegründet und sitzt in den USA.

WhatsApp gehört seit 2014 zur Facebook-Unternehmensgruppe, ist jedoch weiterhin ein selbständiges Unternehmen. Es verfügt bislang über keine deutsche oder europäische Niederlassung und ist damit derzeit nicht an deutsches oder europäisches Datenschutzrecht gebunden. Die Rechtslage ändert sich mit dem sog. Marktortprinzip der ab Mai 2018

wirksamen Europäischen Datenschutz-Grundverordnung. Deren Anwendungsbereich erstreckt sich nach Art. 3 Abs. 2 DS-GVO dann auch auf außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind. Voraussetzung ist, dass sich ein Angebot an einen bestimmten nationalen Markt in der Europäischen Union richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der Europäischen Union dient.

In seinen Nutzungsbedingungen weist WhatsApp darauf hin, dass es als Teil der Facebook-Unternehmensgruppe Informationen von den Unternehmen dieser Unternehmensgruppe erhält und Informationen mit ihnen teilt. Dabei wird ausdrücklich darauf verwiesen, dass die Informationen für Werbezwecke verwendet werden können. Um welche Informationen es sich im Einzelnen handelt, wird nicht näher dargestellt, genannt sind jedoch die Telefonnummer und nicht weiter spezifizierte „Account-Informationen". Daraus lassen sich teils detaillierte Beziehungs-, Kommunikations-, Bewegungs-, Nutzungs- oder Interessenprofile bilden.

Bei Social Media-Diensten außereuropäischer Anbieter besteht die allgemeine Problematik darin, dass die Verarbeitung von Nutzungsdaten vielfach nicht den Vorgaben des § 15 Abs. 3 TMG entspricht (pseudonyme Verarbeitung, Information der Nutzerinnen und Nutzer, Widerspruchsmöglichkeit). Daneben ergibt sich bei WhatsApp zusätzlich die Besonderheit, dass der Dienst regelmäßig die Telefonnummern im Mobiltelefon-Adressbuch der Nutzerinnen und Nutzer erhebt. Betroffen davon sind nicht nur die Telefonnummern von WhatsApp-Nutzerinnen und –Nutzern, sondern auch diejenigen der sonstigen Kontakte, d.h. von Personen, die mit WhatsApp in keinerlei Verbindung stehen. WhatsApp verlagert die Verantwortung hierfür auf die Nutzerinnen und Nutzer, indem diese mit der Anerkennung der Nutzungsbedingung bestätigen, zur Weitergabe der Daten autorisiert zu sein.

Die dabei unterstellte Abstimmung einer Nutzerin oder eines Nutzers mit den in seinem Adressbuch genannten Personen über deren Einverständnis in die Weitergabe ihrer Daten an WhatsApp bzw. die Löschung der Kontakte, die ihre Einwilligung hierzu nicht erteilen, erfolgt nach Einschätzung des LfDI in der Praxis nicht. Damit würden in den allermeisten Fällen Daten ohne Kenntnis und Zustimmung Betroffener an WhatsApp übermittelt.

Eine Nutzung für persönliche oder familiäre Zwecke, wie sie für eine WhatsApp-Nutzung von Privatpersonen wohl überwiegend anzunehmen ist, unterfällt nach Ansicht des LfDI nicht dem Bundesdatenschutzgesetz (§ 1 Abs. 2 Nr. 3 BDSG). Betroffene, die mit der Übermittlung ihrer Daten an Facebook nicht einverstanden sind, sind damit auf die Geltendmachung zivilrechtlicher Ansprüche beschränkt (z.B. Unterlassungsanspruch). Zum Teil wird vertreten, dass diese Ausnahme dahin auszulegen ist, dass deren Grenzen überschritten werden, wenn personenbezogene Adressdaten an Dritte, welche die Daten zu eigenen, unternehmerischen Zwecken verarbeiten, übermittelt werden (vgl. EuGH, Urteil vom 06. November 2003, Rs C-101/01 - Bodil Lindqvist).

Unternehmen hingegen können sich grundsätzlich nicht auf die sog. Haushaltausnahme berufen. Denn eine Datenverarbeitung der Adressdaten zu wirtschaftlichen Zwecken, wie der Kontaktaufnahme zu Kundinnen und Kunden oder deren Betreuung über Kommunikationsdienste, schließt die Annahme der Verarbeitung der Daten zu rein familiären oder privaten Zwecken stets aus, weil davon bereits begrifflich nur Tätigkeiten erfasst sind, die zum Privat- oder Familienleben zählen.

Auch das Amtsgericht Bad Hersfeld nahm in seinem Beschluss vom 15. Mai 2017 (Az.: F 120/17 EASO) im Rahmen eines Familienrechtsstreits zu der Zulässigkeit der Übermittlung von Telefonbucheinträgen an WhatsApp Stellung. Nach Ansicht des Gerichts bestehe für alle Nutzerinnen und Nutzer von WhatsApp eine latente Gefahr, von einem der eigenen Telefonbuchkontakte abgemahnt zu werden. Wie groß diese Gefahr wirklich ist, ist fraglich, da dem LfDI bisher keine Fälle dieser Art bekannt wurden.

Beim LfDI bestand hingegen in einem anderen Bereich der Nutzung von WhatsApp ein großer Beratungsbedarf. Wiederholt wendeten sich Betroffene an den LfDI, nachdem Chatnachrichten aus geschlossenen Chatgruppen an Dritte weitergegeben wurden https://s.rlp.de/chatnachrichtenarbeitgeber.

1.2 Umfrage zu Social Media-Nutzung durch oberste Landesbehörden zeigt erfreuliche Ergebnisse

Im August 2016 veröffentlichte der LfDI einen Handlungsrahmen für die Nutzung von „Sozialen Medien“ durch öffentliche Stellen (vgl. 25. Tb., Tz. III 1.3). In diesem gab er den öffentlichen Stellen auf, ein Social Media-Konzept vor der Nutzung von Sozialen Medien zu entwickeln. Dies nahm der LfDI im November 2017 zum Anlass, alle Ministerien sowie die Staatskanzlei und den Landtag zu bitten, ihm die erarbeiteten Konzepte vorzulegen. Bis auf ein Ministerium nutzen alle adressierten Stellen Soziale Medien, um Bürgerinnen und Bürger sowie Multiplikatoren auf diesen modernen Kommunikationswegen anzusprechen. Dabei kommunizieren alle über den Kurznachrichtendienst Twitter, während nur die Hälfte der Befragten über einen Facebook-Auftritt verfügt. Einen YouTube Kanal betreiben nur der Landtag und die Staatskanzlei, die darüber hinaus noch Instagram und Flickr nutzt.

Die Auswertung der Umfrage hat gezeigt, dass alle der angeschriebenen Stellen über ein Social Media-Konzept verfügen, die sich – von drei Konzepten abgesehen - zum größten Teil mit den Anforderungen des Handlungsrahmens für die Nutzung von „Sozialen Medien“ durch öffentliche Stellen decken. Kleinere Verbesserungsvorschläge hinsichtlich einer Evaluierung und der Veröffentlichung des Konzeptes konnten hier angebracht werden. Erfreulich bei der Auswertung der Konzepte war, dass sich alle angefragten Stellen an die Vorgabe halten, alternative Weg zur Informationsbeschaffung anzubieten. Der LfDI gibt vor, dass die bereitgestellten Informationen nicht nur im Rahmen des Social Media-Angebots zu finden sein dürfen, sondern immer auch auf einem alternativen Weg – etwa auf der Webseite der Verwaltung -, da die meisten Sozialen Netzwerke eine Vielzahl personenbezogener Daten ihrer Besucherinnen und Besucher sammeln und in den USA speichern. Die meisten Konzepte sahen auch die geforderten halbjährlichen Sensibilisierungsmaßnahmen in den Sozialen Netzwerken vor. Bei der Umsetzung dieser Maßnahmen gab es zum Teil noch Verbesserungsbedarf. Da ein Teil der Stellen die Social Media-Kanäle erst seit kurzer Zeit nutzt, ist hier abzuwarten, wie sich die Häuser in Zukunft verhalten werden.

Lediglich drei Konzepte bedürfen einer Überarbeitung. Der LfDI hat die entsprechenden Behörden kontaktiert und ihnen Verbesserungsvorschläge unterbreitet. Anhand der Umfrage hat sich gezeigt, dass der Handlungsrahmen für die Nutzung „Sozialer Medien“ nicht nur rechtlich gebotene Empfehlungen gibt, sondern sich auch im Praxistest bewährt https://s.rlp.de/sozialemedienfst. Der Handlungsrahmen ist bereits zum „Exportschlager“ geworden. Auch der LfDI Baden-Württemberg hat einen

solchen Handlungsrahmen nach Vorbild des rheinland-pfälzischen vor wenigen Monaten veröffentlicht.

1.3 Unzulässige Veröffentlichungen von Insolvenzdaten privater Schuldner

Immer häufiger wenden sich Privatinsolvenzschuldner an den LfDI, da deren Insolvenzdaten von privaten Dritten veröffentlicht werden. Zumeist geschieht diese Veröffentlichung auf Webseiten im Internet, die eine einfache Suche nach Name, Straße, Ort oder auch Postleitzahl ermöglichen; aber auch Apps, die neben dieser einfachen Suchfunktion die Insolvenzdaten in Verbindung mit Landkarten so aufbereiten, dass Schuldner direkt lokalisiert werden können, sind Gegenstand zahlreicher Beschwerden.

Insolvenzdaten von privaten Insolvenzschuldnern sind hochsensible personenbezogene Daten. Eine Veröffentlichung dieser Daten kann sich nicht nur negativ auf das allgemeine Ansehen eines Schuldners in der Gesellschaft sowie seine Wirtschaftsfähigkeit auswirken, sondern auch negative Folgen für seine Reputation nach sich ziehen. Die Schuldner fürchten sich daher bei weltweit unbegrenzten Veröffentlichungen vor Reaktionen im privaten Umfeld, insbesondere auch seitens ihres Arbeitgebers oder Vermieters.

Zumeist sind diese Veröffentlichungen von Insolvenzdaten durch private Dritte aus datenschutzrechtlicher Sicht nicht zulässig. Zwar greifen die Anbieter auf Daten aus einer allgemein zugänglichen Quelle zurück – nämlich auf solche, die von den jeweils zuständigen Insolvenzgerichten auf dem deutschlandweiten Portal „www.insolvenzbekanntmachungen.de“ veröffentlicht werden. Allerdings werden diese Daten häufig aus datenschutzrechtlicher Sicht aufgrund des Verknüpfens mit anderen Daten unzulässig verändert und/oder zu lange veröffentlicht. Dies kann zu Datenschutzverstößen führen, gegen die vorgegangen werden kann und die geahndet werden können.

Ist der Betreiber eines solchen Angebotes zu ermitteln und hat dieser seinen Sitz in Deutschland, kann eine (weitere) Veröffentlichung möglicherweise verhindert werden. Die datenschutzrechtlichen Aufsichtsbehörden können einschreiten und auch die Gerichte auf Antrag eines Schuldners hin tätig werden und eine Überprüfung vornehmen.

So war dies auch in einem Fall, der den LfDI im Berichtszeitraum umfänglich befasste. Es ging um eine App, die man käuflich erwerben konnte und im Anschluss sodann die Schuldnerdaten aus den Insolvenzverzeichnissen einer aufbereiteten Kartenansicht entnehmen konnte. Gegen den rheinland-pfälzischen Betreiber dieser App wurde zunächst ein Auskunftsverfahren eingeleitet, in dessen Rahmen der LfDI seine Rechtsauffassung zu dieser Form der Veröffentlichung mitteilte. Daraufhin kam es unmittelbar zu einer Änderung der App dergestalt, dass eine Anzeige von Privatinsolvenzen nicht mehr erfolgte.

Dass die betroffenen Schuldner sich in diesen Fällen auch erfolgreich an die Gerichte wenden können, zeigt auch eine Entscheidung des Amtsgerichts Rockenhausen in Rheinland-Pfalz aus dem Jahre 2016 (Urteil vom 09. August 2016, Az. 2 C 341/16), deren Gegenstand ebenfalls die App war, die Schuldnerdaten aus Insolvenzverzeichnissen veröffentlichte.

Das Problem ist jedoch häufig, dass die Betreiber der jeweiligen Webangebote nicht zu ermitteln oder im Ausland ansässig sind, sodass die deutschen Datenschutzaufsichtsbehörden derzeit schwerlich gegen die Veröffentlichung

vorgehen können. Auch solche Eingaben erreichten den LfDI sehr häufig.

Der Hamburgische Datenschutzbeauftragte hat im Zuge dessen nunmehr erreicht, dass zumindest Google einige Webseiten, auf denen personenbezogenen Daten aus Insolvenzverfahren unzulässigerweise veröffentlicht wurden und deren Betreiber nicht zu ermitteln oder im Ausland ansässig sind, nicht mehr als Treffer bei einer Suche anzeigt werden. Dies ist ein großer Schritt in die richtige Richtung. Allerdings verhindert dies nicht die Veröffentlichung der Insolvenzdaten durch private Dritte an sich.

Die ab Mai 2018 wirksame Datenschutz-Grundverordnung wird aber den Datenschutzaufsichtsbehörden insbesondere auch im Hinblick auf im Ausland ansässige Betreiber mehr Befugnisse einräumen, um gegen unzulässige Veröffentlichungen von Insolvenzdaten vorzugehen.

Nähere Informationen zur Zulässigkeit von Veröffentlichungen von Insolvenzdaten durch Private: https://s.rlp.de/datenschutzinsolvenzdaten.

2. WIRTSCHAFT

2.1 Bußgeldverfahren gegen Immobilienmakler

Der LfDI führte ein Bußgeldverfahren gegen einen Immobilienmakler.

Ein Mitarbeiter eines Immobilienmaklers hatte durch eine Recherche Eigentumsdaten bestimmter Grundstücke, insbesondere auch dahingehend, wer Allein- oder Miteigentümer ist, erhoben und diese Daten zu werblichen Ansprachen benutzt. Diese Datenerhebung und anschließende Datenspeicherung zum Zwecke der werblichen Ansprache erfolgte ohne datenschutzrechtliche Rechtfertigung (§ 4 Abs. 1 BDSG). Weder lag eine Einwilligung der Betroffenen vor noch war die Datenverarbeitung durch einen Rechtfertigungstatbestand des Bundesdatenschutzgesetzes (§§ 28 ff. BDSG) gerechtfertigt.

Die Daten waren auch nicht allgemein zugänglich. Allgemein zugängliche Quellen sind alle Träger von Informationen, die geeignet und bestimmt sind, der Allgemeinheit, also einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen (BVerfGE 27, 71 (83), auch NJW 1970, 235). Zu den allgemein zugänglichen Quellen zählen insbesondere sämtliche veröffentlichte Printmedien, öffentliche Datenbanken, öffentliche Anschläge, der Rundfunk, öffentliche Veranstaltungen; öffentliche Register nur dann, wenn ihre Einsichtnahme nicht von einem besonderen berechtigten Interesse abhängt. Die konkreten Eigentümerdaten, insbesondere ob Allein- oder Miteigentum vorliegt, sind nicht in einer allgemein zugänglichen Quelle vorhanden gewesen.

Aufgrund der Tatsache, dass es sich um eine

werbliche Ansprache handelte, war diese auch unabhängig von der Frage der allgemeinen Zugänglichkeit der Daten mangels Vorliegens der Voraussetzungen des § 28 BDSG insoweit nicht zulässig.

Bis zum Ablauf des Berichtszeitraums war das infolge eines Einspruchs gegen den erlassenen Bußgeldbescheid zwischenzeitlich bei Gericht anhängige Ordnungswidrigkeitenverfahren noch nicht abgeschlossen.

2.2 Bußgeldverfahren gegen Unternehmen für Labordiagnostik

Im Berichtszeitraum führte der LfDI ein Bußgeldverfahren gegen ein rheinland-pfälzisches Unternehmen, das in der Entwicklung, der Produktion und dem Vertrieb von Testsystemen für die Labordiagnostik tätig ist. Im Rahmen der Testung eines Blutserums kam es zur unbefugten Erhebung und Verarbeitung von personenbezogenen Daten eines Petenten sowie zu einer unrichtigen Auskunftserteilung. Die Ordnungswidrigkeitentatbestände des § 43 Abs. 2 Nr. 1 bzw. § 43 Abs. 1 Nr. 8a BDSG waren damit erfüllt. Der aufgrund dessen erlassene Bußgeldbescheid mit einem Bußgeld in fünfstelliger Höhe ist rechtskräftig.

2.3 Bestellung einer Rechtsanwalts-Partnerschaftsgesellschaft zum betrieblichen Datenschutzbeauftragten

Den LfDI erreichten auch Anfragen bezüglich der Möglichkeit der Bestellung von Rechtsanwalts-Partnerschaftsgesellschaften zum betrieblichen Datenschutzbeauftragten.

Den Ausgangspunkt zur Beantwortung der Frage, ob die Bestellung einer Rechtsanwalts-Partnerschaftsgesellschaft zum betrieblichen Datenschutzbeauftragten unter dem derzeitigen Bundesdatenschutzgesetz zulässig ist, bildet § 4f BDSG.

Der Wortlaut der Norm gibt zunächst keinen Hinweis darauf, was von dem Begriff „Beauftragter für den Datenschutz“ konkret umfasst wird. Dies bedeutet allerdings nicht automatisch, dass eine Wahrnehmung der in § 4g BDSG statuierten Aufgaben ausschließlich durch eine natürliche Person zu erfolgen hätte. § 4f Abs. 2 Satz 3, 1. Halbsatz BDSG spricht insoweit nur von der Möglichkeit der Bestellung einer „Person“ außerhalb der verantwortlichen Stelle. Eine Beschränkung auf natürliche Personen hat dort nicht stattgefunden, was darauf schließen lässt, dass der Gesetzgeber eine solche Ausschließlichkeit nicht vor Augen hatte. Insofern ergibt sich zunächst kein Hindernis für die Bestellfähigkeit juristischer Personen unmittelbar aus dem Gesetz.

Dass das Gesetz insoweit von einer Person und damit der Einzahl spricht, steht auch der Bestellung einer Personengesellschaft als Beauftragter für den Datenschutz nicht zwingend entgegen. Durch Einfügen des § 4f Abs. 2 Satz 3, 1. Halbsatz BDSG sollte lediglich sichergestellt werden, dass es auch externe Datenschutzbeauftragte geben darf (wie in der Richtlinie 95/46/EG vorgesehen). In diesem Zusammenhang wurde der Begriff „Person“ im Zusammenhang mit dem betrieblichen Datenschutzbeauftragten erstmals in § 4f BDSG verwendet. Dies bedeutet aber nicht zwingend, dass dadurch die Möglichkeit der Bestellung einer Partnerschaftsgesellschaft oder sonstiger Personengesellschaften ausgeschlossen werden sollte. Dann hätte es einer ausdrücklichen Normierung in Form von „natürliche Person“ oder „natürliche und juristische Personen“ bedurft.

Es wird die Ansicht vertreten, dass sich ein

Hindernis für die Bestellfähigkeit juristischer Personen aus den in § 4f Abs. 2 S. 1 BDSG genannten Anforderungen an einen Datenschutzbeauftragten ergebe. „Zuverlässigkeit" und „Fachkunde" seien Eigenschaften, die nur von einer natürlichen Person erbracht werden könnten (vgl. Gola/Schomerus, BDSG, 10. Auflage 2010, § 4f Rn. 19; Erbs/Kohlhaas/ Ambs, Strafrechtliche Nebengesetze, 210. Ergänzungslieferung September 2016, BDSG § 4f, Rn.3). Dem kann jedoch nicht uneingeschränkt gefolgt werden. Dies zunächst im Hinblick darauf, dass die Merkmale der Zuverlässigkeit und Fachkunde auch Eingang in andere Gesetze und Regelungsbereiche gefunden haben, wo ebenfalls keine Beschränkung auf natürliche Personen stattgefunden hat (so z.B. § 19 ASiG oder § 4 SigG oder auch § 35 GewO). § 2 Abs. 1 Nr. 1 VOB/A normiert sogar explizit die Vergabe an fachkundige, leistungsfähige und zuverlässige Unternehmen (auch Knopp, Dürfen juristische Personen zum betrieblichen Datenschutzbeauftragten bestellt werden?, DuD 2015, 98, 99 f.).

In der vorliegenden Konstellation kommt noch hinzu, dass es sich nicht um eine juristische Person, sondern um eine Partnerschaftsgesellschaft handelt. Gemäß § 7 Abs. 2 PartGG wird ihr lediglich Teilrechtsfähigkeit zugestanden. Ihr Zweck liegt darin begründet, dass sich mehrere Freiberufler zusammenschließen, um ihrer Tätigkeit in diesem gesellschaftsrechtlichen Zusammenschluss gemeinschaftlich nachzugehen. Aufgrund des stark personenbezogenen Charakters dieses Zusammenschlusses handelt es sich um eine Personengesellschaft (Kilian/ Seibert, Nomos-Kommentar Partnerschaftsgesellschaftsgesetz, 1. Auflage 2012, § 1 Rn. 2). § 7 Abs. 4 PartGG normiert, dass die Partnerschaft als Prozess- und Verfahrensbevollmächtigte beauftragt werden kann. Sie handelt dabei durch ihre Partner und Vertreter, in deren Person die für die Erbringung rechtsbesorgender Leistungen gesetzlich vorgeschriebenen Voraussetzungen im Einzelfall vorliegen müssen. Damit hat der Gesetzgeber eine allgemeine, alle Arten der Vertretung vor Gerichten und Behörden mit Ausnahme der Strafverteidigung umfassende Regelung getroffen (Carsten/ Schäfer, Münchener Kommentar BGB, PartGG, 6. Auflage 2013, § 7 Rn. 21). Zuverlässigkeit und Fachkunde sind „gesetzlich vorgeschriebene Voraussetzungen" im Sinne des § 7 Abs. 4 S. 2 PartGG. Dies deutet schon darauf hin, dass es sich bei der Partnerschaft um eine besondere Art des Zusammenschlusses natürlicher Personen handelt, bei der vornehmlich auf das Vorhandensein gesetzlicher Voraussetzungen bei diesen die Partnerschaft bildenden Personen abzustellen ist. Gerade bei einer Partnerschaft bestehend aus Rechtsanwälten ist davon auszugehen, dass ihre Zuverlässigkeit schon in ihrem Berufsethos begründet liegt. Die nötige Fachkunde kann in einer Partnerschaft gerade durch eine Mehrheit von Personen und die daraus folgende Bündelung von Expertise gesichert werden. Dies ist gerade im Hinblick auf die wachsenden Anforderungen im Bereich des Datenschutzes vorteilhaft.

Das Vorhandensein einer Mehrheit von Personen in der Partnerschaft steht auch nicht dem Erfordernis des § 4f Abs. 5 Satz 2 BDSG entgegen. Danach müssen sich Betroffene jederzeit an die Datenschutzbeauftragten wenden können. Würde nun eine juristische Person bestellt, könnte eine gewisse Intransparenz entstehen und sich für Betroffene die Frage nach dem konkreten Ansprechpartner stellen. Bei genauerer Betrachtung kann aber festgestellt werden, dass dieses Problem in gleicher Form bei Bestellung einer natürlichen Person entstehen kann, da gemäß § 4f Abs. 5 Satz 1 BDSG den Datenschutzbeauftragten, soweit es zur Erfüllung ihrer Aufgaben erforderlich ist, Hilfspersonal zur Verfügung gestellt werden kann. Je nach Größe des Betriebes vari-

iert auch die Anzahl der erforderlichen Hilfspersonen. Außerdem kann der Problematik der Intransparenz dadurch begegnet werden, dass für alle möglicherweise Betroffenen erkennbar ein Hauptansprechpartner innerhalb der juristischen Person benannt wird und alle an der Arbeit des Beauftragten Beteiligten beispielsweise in einem Organigramm dargestellt werden. Wie oben bereits ausgeführt, kommt im vorliegenden Fall noch hinzu, dass es sich nicht einmal um eine juristische Person, sondern um eine Partnerschaft handelt, welche in ihrem Umfang überschaubar genug ist, um die erforderliche Transparenz herzustellen (ähnlich auch Knopp, Dürfen juristische Personen zum betrieblichen Datenschutzbeauftragten bestellt werden?, DuD 2015, 98, 101).

Die oben genannte Problematik im Rahmen der Bestellung eines Datenschutzbeauftragten stellt sich auch im Hinblick auf die Datenschutz-Grundverordnung. Diese beschäftigt sich in Art. 37 mit der Benennung eines Datenschutzbeauftragten und sieht in Abs. 5 Folgendes vor:

„Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben."

Dazu, ob zum Datenschutzbeauftragten auch eine juristische Person oder eine Personalgesellschaft bestellt werden kann, verhält sich die Datenschutz-Grundverordnung ebenfalls nicht ausdrücklich. Wie bei § 4f BDSG lassen sich hier für beide Standpunkte Argumente finden. Jedoch muss festgestellt werden, dass die Datenschutz-Grundverordnung keinen expliziten Ausschluss nicht natürlicher Personen bei der Benennung zum Datenschutzbeauftragten vorsieht. Angesichts der eher hohen Regelungsdichte im Bereich des EU-Rechts könnte davon ausgegangen werden, dass der Verordnungsgeber eine entsprechende Regelung eingefügt hätte, wenn ein solcher Ausschluss vorgesehen wäre.

2.4 Datenschutz bei der Übermittlung in Drittländer – Prüfung und Sensibilisierung der Unternehmerinnen und Unternehmen in Rheinland-Pfalz

Im Zuge der immer stärkeren weltweiten Vernetzung von Unternehmen und der Auslagerung von Geschäftsprozessen werden personenbezogene Daten inzwischen in erheblichem Umfang auch in Staaten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums übermittelt. Ob Rechnungslegung, Fernwartung, Reisemanagement oder Cloud-Computing: Nicht nur große, international tätige Konzerne, sondern auch kleinere und mittlere Unternehmen nutzen die außereuropäischen Angebote – sei es um Kosten zu sparen oder aus Mangel an vergleichbaren Angeboten in der Europäischen Union bzw. dem Europäischen Wirtschaftsraum.

Personenbezogene Daten von Kundinnen und Kunden, Beschäftigten, Geschäftspartnerinnen und -partnern usw. lassen sich zwar mühelos um den Globus schicken, aber nicht immer sorgenlos. In Deutschland bzw. – mit der kommenden Datenschutz-Grundverordnung – in ganz Europa wurde ein hohes Datenschutzniveau erreicht, mit welchem andere Länder nicht immer mithalten können. Das Kapitel V der Datenschutz-Grundverordnung zeigt Wege auf, wie man den Datentransfer in Drittländer dennoch europarechtskonform gestalten kann. Diese sollten die Unternehmerinnen und Unternehmer beschreiten. Denn auch Verstöße gegen diese Vorschriften sind mit empfindlichen

Sanktionen bewährt. Die Datenschutz-Grundverordnung hat insofern eine Strahlungswirkung über die europäischen Grenzen hinaus.

Erfahrungen aus den Beratungen der Datenschutzaufsichtsbehörden zeigten, dass manche verantwortlichen Stellen sich gar nicht bewusst sind, dass und welche personenbezogenen Daten sie in Drittländer übermitteln oder, sofern sie sich dessen bewusst waren, verunsichert waren, auf welcher Grundlage sie dies datenschutzkonform durchführen können. Unabhängig von der Bewertung der für den internationalen Datenverkehr zur Verfügung stehenden Mittel ist durch die Verabschiedung des EU-U.S. Privacy Shields im Sommer 2016 eine neue Situation eingetreten. Dies nahm eine große Anzahl der deutschen Datenschutzaufsichtsbehörden, einschließlich des LfDI, zum Anlass für eine koordinierte Prüfung des internationalen Datenverkehrs. Die Ergebnisse der Prüfung in Rheinland-Pfalz werden im Frühjahr 2018 im Internetangebot des LfDI veröffentlicht.

Die ersten Zahlen und Fakten zeigen: Etwas mehr als die Hälfte der in Rheinland-Pfalz ansässigen befragten Unternehmen übermittelt Daten in Drittstaaten. Zielländer sind auf allen Kontinenten zu finden. Als geeignete Garantie für die Einhaltung des geforderten Datenschutzniveaus (Art. 46 DS-GVO) nutzt mehr als die Hälfte der befragten Unternehmen die Standardvertragsklauseln der Europäischen Kommission. Deren Rechtmäßigkeit wird gerade vor dem Europäischen Gerichtshof verhandelt. Fast ein Drittel der Unternehmen, die Daten in die USA übermitteln, stützen sich auf das EU-U.S. Privacy Shield. Auch dessen Zukunft ist ungewiss. Nach der ersten, jährlich stattfindenden Überprüfung vor Ort sind die europäischen Datenschutzaufsichtsbehörden nach wie vor nicht vom Vorliegen eines angemessenen Datenschutzniveaus überzeugt.

Die anstehende Gesetzesänderung im Datenschutzrecht sollte jede Unternehmerin und jeder Unternehmer zum Anlass nehmen, die gewählten Rechtsgrundlagen für den internationalen Datentransfer nach Kapitel V der Datenschutz-Grundverordnung und unter Berücksichtigung aktueller rechtlicher Entwicklungen zu überprüfen. In jedem Fall sollte insbesondere bei der Übermittlung personenbezogener Daten in Drittländer großer Wert auf die Datensicherheit gelegt werden, z.B. mithilfe von aktueller Verschlüsselungstechnik.

3. BESCHÄFTIGTENDATEN-SCHUTZ

3.1 Der schlafende Azubi

Eine Vorgesetzte in einer Gemeindeverwaltung bemerkte, dass ein Auszubildender während der Mittagspause eingeschlafen war und laut schnarchte. Sie filmte ihn während seines „Büroschlafs“ und verschickte das Video an andere Kollegen. Der Vorgang wurde dem Bürgermeister gemeldet, um zu prüfen, ob gegen den Azubi disziplinarisch vorgegangen werden solle. Die behördliche Datenschutzbeauftragte bat den LfDI um eine Einschätzung.

Im vorliegenden Fall war aus Sicht des LfDI weniger eine Dienstpflichtverletzung des Azubis als vielmehr das Filmen seines Mittagsschlafs zu würdigen.

Denn das heimliche Filmen oder Fotografieren einer anderen Person verletzt diese in ihrem Recht am eigenen Bild als Teil des allgemeinen Persönlichkeitsrechts. Darüber hinaus macht sich nach § 201a StGB strafbar, wer eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt. Ebenso wird nach dieser Norm bestraft, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht. Für den Fall, dass vorliegend die fragliche Aufnahme in sozialen Medien veröffentlicht worden wäre, wäre auch noch eine Strafbarkeit nach dem Kunsturhebergesetz in Betracht gekommen.

Unabhängig vom strafrechtlichen Gehalt dürften auf zivilrechtlicher Ebene gegenüber der Vorgesetzten Unterlassungs- und Beseitigungsansprüche und ggf. Schadensersatzansprüche des Auszubildenden bestehen.

Wie die behördliche Datenschutzbeauftragte mitteilte, wurde das fragliche Video zwischenzeitlich gelöscht. Der LfDI empfahl darüber hinaus, die Gemeindeverwaltung und insbesondere auch den Auszubildenden über die o.g. rechtlichen Aspekte zu informieren. Dies wurde auch befolgt. Der Azubi konnte somit für sich selbst entscheiden, ob er ggf. unter Hinzuziehung eines Rechtsanwaltes gegenüber der Vorgesetzten tätig werden möchte.

3.2 Heimliche GPS-Ortung von Beschäftigten durch ihren Arbeitgeber

In den vergangenen Jahren wurde der LfDI wiederholt von Beschäftigten um Hilfe gebeten, die sich mittels GPS-Technik durch den Arbeitgeber überwacht fühlten. Beschäftigte einer Feuerwehreinheit fühlten sich durch den Einbau eines GPS-Trackers, der den Standort des Fahrzeuges zu jeder Zeit an die Zentrale meldete, unter einem ständigen Beobachtungsdruck. Ebenfalls von dieser Überwachung betroffen waren Beschäftigte im Bereich der Autobahnmeisterei, deren Fahrzeuge mit GPS-Geräten versehen waren, um ihre Arbeitsleistung und Routen genauestens nachvollziehen zu können. Daneben waren wiederholt Beschäftigte, die im Außendienst arbeiten, von der Überwachung mittels GPS betroffen. Firmenfahrzeuge, die zum Teil auch zur privaten Nutzung den Beschäftigten überlassen wurden, stattete der Arbeitgeber mit GPS-Technik aus, um den Standort der Beschäftigten ohne deren Wissen ermitteln und Arbeitseinsätze einfacher planen zu können.

Doch während GPS sowohl im privaten als auch im beruflichen Leben viel Zeit und Ärger sparen kann, eröffnet es nebenbei ganz neue Kontroll-

möglichkeiten. Während vor 20 Jahren nur die Fahrerin oder der Fahrer selbst wusste, wo er sich gerade befand, kann mittels GPS Technik heute auch mancher Dritter an jedem Ort der Welt auf das GPS-Signal zugreifen und erfahren, wann und wo sich ein Fahrzeug oder ein Smartphone befindet.

Sicherlich kann dies in einer Reihe von Fällen gut und sinnvoll sein, z.B. bei einem Unfall oder einem Unglück, jedoch greift diese neue Überwachungsmethode – wenn sie heimlich stattfindet – tief in das Recht auf informationelle Selbstbestimmung des Betroffenen ein. Bei GPS-Daten eines Gerätes handelt es sich nämlich regelmäßig um personenbezogene Daten – und die sind gesetzlich geschützt. Sobald das Gerät oder das Fahrzeug, in dem das Gerät verbaut ist, einer bestimmten Person zugeordnet werden kann, sind diese Daten ein schützenswertes Gut.

Der LfDI hat dies zum Anlass genommen und ein Positionspapier zur Zulässigkeit von GPS-Technik zur Überwachung im Beschäftigtenverhältnis veröffentlicht: https://s.rlp.de/gps

3.3 Das Bundesarbeitsgerichts und der Europäische Gerichtshof für Menschenrechte stärken den Datenschutz im Beschäftigtenverhältnis

Der Datenschutz im Beschäftigtenverhältnis im privaten Bereich wird durch die Regelung des § 32 BDSG bestimmt. Diese Regelung bestimmt jedoch sehr unscharf die Voraussetzungen für Datenerhebung, -verarbeitung und -verwendung im Beschäftigtenverhältnis. Umso wichtiger sind daher die Vorgaben, die die Rechtsprechung in den vergangenen Jahren dazu entwickelt hat. Das Bundesarbeitsgericht sowie der Europäische Gerichtshof für Menschenrechte haben in den vergangenen zwei Jahren in mehreren Entscheidungen klargestellt, welche Anforderungen die Arbeitgeberschaft beim Beschäftigtendatenschutz berücksichtigen muss.

Auch in Zukunft werden die Vorgaben aus der Rechtsprechung entscheidend für den Datenschutz im Beschäftigtenverhältnis sein. Am 25. Mai 2018 tritt ein neues Bundesdatenschutzgesetz in Kraft. Der Beschäftigtendatenschutz wird dann in § 26 BDSG-neu geregelt. Die Regelung deckt sich jedoch in weiten Teilen mit der alt bekannten Regelung des § 32 BDSG. Die dazu entwickelte Rechtsprechung wird daher auch weiterhin anwendbar bleiben. Auch in Zukunft wird die Rechtsprechung Antworten auf eine Vielzahl von neuen Fragestellungen im Beschäftigtenverhältnis finden müssen, da auch § 26 BDSG-neu als unscharf und wenig konkret kritisiert wird.

In einem spektakulären Fall zur privaten Internetnutzung eines Beschäftigten während der Arbeitszeit musste das Bundesarbeitsgericht am Ende nicht mehr entscheiden, da sich die Parteien vor der mündlichen Verhandlung verglichen. Das Landesarbeitsgericht Berlin-Brandenburg hatte zuvor in diesem Fall entschieden, dass eine fristlose Kündigung wegen exzessiver privater Internetnutzung am Arbeitsplatz, die durch eine verdeckte Auswertung der Internetnutzung des Beschäftigten aufgedeckt wurde, rechtmäßig war (vgl. Landesarbeitsgericht Berlin-Brandenburg, MDR 2016, 533; Urteil vom 14. Januar 2016, Az. 5 Sa 657/15). Mangels einer eindeutigen Regelung zur Internetnutzung zu privaten Zwecken war in diesem Fall auch eine gegenteilige Entscheidung nicht unwahrscheinlich, da der Arbeitgeber seinen Beschäftigten keine klar umrissenen Vorgaben zur Internetnutzung gemacht hatte. Der LfDI empfiehlt Unternehmen zur Vermeidung solcher Fälle, Betriebsvereinbarungen zur Internet- und E-Mail-Nutzung zu schließen. Die

Datenschutzaufsichtsbehörden haben hierzu 2016 eine gemeinsame Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz verabschiedet https://s.rlp.de/datenschutz-arbeitsplatz.

Auch der Europäische Gerichtshof für Menschenrechte musste sich mit der Zulässigkeit von Überwachungsmaßnahmen der privaten Internetnutzung im Beschäftigtenverhältnis befassen (Europäischer Gerichtshof für Menschenrechte ZD 2017, 571; Urteil vom 5. September 2017, – Application N. 61496/08 - Bărbulescu v. Romania). Er räumt den Mitgliedsstaaten ein weites Entschließungs- und Auswahlermessen bzgl. der zu ergreifenden Maßnahmen ein. Jedoch sind bei Überwachungsmaßnahmen im Beschäftigtenverhältnis angemesse Maßnahmen gegen Willkür zu ergreifen. Der Gerichtshof gibt den Mitgliedsstaaten einen Prüfkatalog an die Hand, der sich in weiten Teilen mit dem durch die Rechtsprechung des Bundesarbeitsgerichts entwickelten Voraussetzungen für die Zulässigkeit der Überwachung im Beschäftigtenverhältnis deckt.

Das Bundesarbeitsgericht musste sich auch erneut mit der Verwertung von verdeckten Videoüberwachungsmaßnahmen zur Aufklärung von Diebstählen beschäftigten, die zufällig eine Pfandmanipulation aufdeckten (Bundesarbeitsgericht NJW 2017, 843; Urteil vom 22. September 2016, Az. 2 AZR 848/15). Der Arbeitgeber sprach daraufhin die Kündigung aus, die auch vom Bundesarbeitsgericht bestätigt wurde, weil es sich um eine Videoüberwachung handelte, die zur Aufdeckung von Straftaten im Beschäftigtenverhältnis nach § 32 Abs. 1 S. 2 BDSG installiert worden war.

Mit seiner Entscheidung zum Einsatz sog. Keylogger stärkt das Bundesarbeitsgericht das Recht der Beschäftigten, nicht ohne konkreten Verdacht „ins Blaue hinein“ durch sogenannte Keylogger überwacht zu werden (Bundesarbeitsgericht, NZA 2017, 1327; Urteil vom 27. Juli, Az. 2017 – 2 AZR 681/16). Die Erfurter Richter bestätigen mit ihrer Entscheidung die Linie, dass eine lückenlose technische Überwachung am Arbeitsplatz in der Regel rechtswidrig ist. Weitere Informationen zu dieser Entscheidung: https://s.rlp.de/keylogger.

3.4 Du verlässt uns – doch dein Name bleibt: Weiterverwendung von personalisierten E-Mail Adressen von ehemaligen Beschäftigten

Auch wenn die Trennung von einem Beschäftigten einvernehmlich erfolgt, gibt es Fälle, in denen der ehemalige Arbeitgeber ein Interesse hat, mit dem Namen des ehemaligen Beschäftigten weiter auf seinem Internetauftritt zu werben oder eingehende E-Mails auf die personalisierte E-Mail Adresse des ehemaligen Beschäftigten zur Kontaktpflege mit Kundinnen und Kunden weiterhin zu empfangen.

Die ehemaligen Beschäftigten haben in diesen Fällen selten Verständnis dafür, dass die früheren Arbeitgeber ihre Namen weiterhin für ihre Geschäftszwecke verwenden. Dies müssen ehemalige Beschäftigte auch nicht dulden. Nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn die Speicherung unzulässig ist. Des Weiteren haben nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG nicht öffentliche Stellen personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist.

Die Verwendung einer personalisierten

E-Mail-Adresse oder des Namens der Beschäftigten auf dem Internetauftritt ist nach Beendigung des Beschäftigungsverhältnisses für dieses nicht mehr notwendig, sodass eine weitere Verwendung ihrer Daten nach § 32 Abs. 1 Satz 1 BDSG nicht gerechtfertigt ist. In vielen Fällen widerrufen die Beschäftigten ihre Einwilligungen zur weiteren Verwendung ihrer Namen zusätzlich noch oder verlangen explizit die Löschung. Die Speicherung der personalisierten E-Mail-Adresse ist somit weder aufgrund einer Rechtsvorschrift noch aufgrund einer Einwilligung erlaubt, sodass die weitere Speicherung unzulässig ist und das Datum nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG zu löschen ist.

Durch die Beendigung des Beschäftigungsverhältnisses ist daneben auch der ursprüngliche Zweck für die Speicherung der personalisierten E-Mail-Adresse und die Speicherung des Namens im Internetauftritt entfallen. Beides erfolgt, um den direkten Kontakt zwischen Beschäftigten und Kunden zu ermöglichen. Scheidet der Beschäftigte aus dem Unternehmen aus, entfällt dieser Zweck und die Speicherung ist somit für den Zweck der Kontaktaufnahme zwischen den Beschäftigten und den Kundinnen und Kunden nicht mehr erforderlich.

Allein das unternehmerische Interesse über die personalisierte E-Mail-Adresse der Beschäftigten nach ihrem Ausscheiden aus dem Unternehmen mit Kunden in Kontakt zu treten, rechtfertigt keine weitere Speicherung der personalisierten E-Mail-Adresse. Nach dem Abschalten der E-Mail-Adresse erhält der Versender einer neuen Nachricht durch eine Meldung vom Mailserver davon Kenntnis, dass das E-Mail-Konto unbekannt ist. Der Versender der E-Mail ist somit darüber informiert, dass seine E-Mail nicht angekommen ist und kann sich auf einem anderen Weg mit dem Unternehmen in Verbindung setzen.

4. SICHERHEIT

4.1 Auswirkungen der angespannten Sicherheits- und sicherheitspolitischen Lage auf die Gesetzgebung

Angesichts der zunehmend angespannten Sicherheitslage in Deutschland und Europa, die aufgrund diverser Anschläge für die Bürgerinnen und Bürger spürbar wurde, wurden die Sicherheitsgesetze sowohl durch den Bundes- als auch den Landesgesetzgeber verschärft. Die maßgebliche Rolle spielten dabei die Ausweitung von Datenverarbeitungs- und Überwachungsbefugnisse der Sicherheitsbehörden. Diese sind mit Augenmaß so auszugestalten, dass die Freiheitsrechte Unbeteiligter den Sicherheitsbestrebungen nicht über dem Maß zum Opfer fallen. Dies ist den Gesetzgebern nicht immer gelungen.

4.1.1 Das neue Bundeskriminalamtgesetz und das Fluggastdatengesetz

Einen Höhepunkt der Gesetzgebungsbestrebungen bildete der 27. April 2017, an dem der Bundestag eine Reihe von Gesetzgebungsvorhaben im Akkord beschlossen hat. Neben dem Datenschutzanpassungs- und –umsetzungsgesetz wurde das BKA-G novelliert und das Fluggastdatengesetz verabschiedet. Die Gesetze werden weitreichende Folgen für den Datenschutz in Deutschland haben.

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BKA-G) änderte das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Das nationale polizeiliche Informationswesen wird beim BKA als Zentral- und Kontaktstelle für die internationale Zusammenarbeit zentrali-

siert. Dazu ist unter anderem die Umstrukturierung des bisherigen Informationsverbundes der Polizeien des Bundes und der Länder zu einem beim BKA zentralisierten „Informationspool“ ohne ausdifferenzierte Dateienstruktur eingeführt worden. Korrespondierend wurden die Errichtungsanordnungen abgeschafft und damit ein maßgebliches Instrument der Datenschutzkontrolle, sowohl der Selbstkontrolle der Polizeien der Länder als auch der Fremdkontrolle durch die Datenschutzaufsichtsbehörden. Einige Änderungen wurden durch die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder nachdrücklich in der Entschließung „Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte“ (https://s.rlp.de/entschliessungdsk032017) der 93. Datenschutzkonferenz kritisiert. Auf die ursprünglich geplante Neuregelung der Löschfristen, die zu dauerhaften und ausufernden Speicherungen geführt hätten, wurde letztlich erfreulicherweise verzichtet.

Wie bereits bei dem BKA-G und den Novellierungen der Polizeigesetze der Länder steht bei dem Gesetz über die Verarbeitung von Fluggastdaten (Fluggastdatengesetz) die Terrorismusabwehr im Vordergrund. Dazu sollen die Fluggastdaten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität verarbeitet werden. Der Datenumfang ist nicht unerheblich. Neben den personenbezogenen Stammdaten der Passagiere sollen auch Daten wie Kreditkartennummer, Reiseverlauf, Gepäckangaben und sogar die Essensbestellung Gegenstand des gespeicherten Datensatzes sein. Kritikwürdig an dieser Speicherung ist die Streubreite, die in erster Linie unbescholtene Reisende betrifft und sie – ohne Anlass – zum Gegenstand von polizeilichen Datenabgleichen und Profiling der Polizeibehörden werden lässt.

Das Gutachten des Europäischen Gerichtshofs (EuGH) (https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084de.pdf) zu der zugrunde liegenden Richtlinie führte zur Stärkung der Grundrechte in diesem Bereich. In seinem Gutachten vom 26. Juli 2017 zum geplanten Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung von Fluggastdaten hat der EuGH festgestellt, dass dieses in seiner jetzigen Form nicht geschlossen werden darf. Dieses Gutachten hat insbesondere mit seinen Begründungen erhebliche Auswirkungen auch auf andere Abkommen, Rechtsakte der Union und deutsche Gesetze. In dem Gutachten hat der EuGH unter anderem klargestellt, dass besonders sensible Daten grundsätzlich nicht übermittelt werden dürfen. Es gilt, mögliche Diskriminierungen etwa wegen der Religion, zu vermeiden. Die strenge Bestimmtheit und Verhältnismäßigkeit, die der EuGH fordert, muss als Messlatte auch an andere Regelungen angelegt werden. Zudem sei die Speicherdauer von 5 Jahren zu lang.

Das Flugastdatengesetz bedarf nun der Überprüfung. Es könnte an einigen Stellen eine Nachsteuerung erforderlich sein. Dies betrifft genauso die Richtlinie selbst wie auch die bereits bestehenden Abkommen. Aber nicht nur das Fluggastdatengesetz, sondern auch andere europäische Rechtsakte, die die Verarbeitung von Reisedaten betreffen, wie die Einführung des Einreise- und Ausreisesystems (Entry/Exitsystem), müssen auf die Kriterien des EuGH-Gutachtens hin überprüft und nachgebessert werden. Dies hat die Konferenz der Datenschutzbehörden des Bundes und der Länder (DSK) in ihrer Entschließung „Keine anlasslose Vorratsspeicherung von Reisedaten“ (https://s.rlp.de/entschliessungdsk112017) auf ihrer 94. Datenschutzkonferenz in Oldenburg gefordert.

4.1.2 Konsequenzen in der Praxis

Die Konsequenzen der Neuerungen für die Praxis und damit auch für die betroffenen Personen sind sicherlich vielfältig, aber im Einzelnen schwer absehbar. Es gilt abzuwarten, wie deren konkrete Umsetzung gestaltet werden wird. Die Bundesbeauftragte und die Landesbeauftragten für den Datenschutz sind nun dazu angehalten, gemeinsam mit der Praxis auf eine datenschutzkonforme Ausgestaltung der Umsetzung der Befugnisse hinzuwirken und Kontrollmechanismen zu etablieren, durch die das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und das Recht auf Datenschutz gem. Art. 8 GRCh gewährleistet werden kann. Defizite, die aufgrund der Geschwindigkeit und Kumulationen der Gesetzgebungsverfahren nicht aus der Welt geschafft werden konnten, sind nun soweit möglich bei der Auslegung und Anwendung der Regelungen zu mildern. Sollten weitere Verschärfungen der Sicherheitsgesetze anstehen, ist dies nicht nur in der Ausgestaltung der Gesetze, sondern auch in deren Gesetzgebungsverfahren zu berücksichtigen. Die Maßgaben und Leitlinien des EuGH sollte der nationale Gesetzgeber dabei im Blick haben.

4.2 Sicherheitsgesetzgebung auf Landesebene

Das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz (POG) wurde ebenfalls im Laufe des Jahres novelliert. Auch wenn der LfDI bei einer Reihe von Detailregelungen Anlass zu Verbesserungen im Sinne von Freiheitssicherungen sah, hält die Gesetzesnovelle insgesamt dem Druck stand, angesichts einer schwierigen Sicherheitslage voreilig die Freiheit aller in überzogenem Maße einzuschränken.

Der rheinland-pfälzischen Polizei wurden durch die Gesetzesänderungen neue Befugnisse zuerkannt, vorhandene Befugnisse wurden ausgeweitet. Ein schwieriger Aspekt ist die Ausweitung der polizeilichen Gefahrenabwehr auf Personen, die noch davon entfernt sind, eine konkrete Gefahr darzustellen. Diese so genannten Gefährder sind schwer zu definieren und rechtsstaatlich schwer zu verfolgen und von Straftaten abzuhalten. Die Abwehr einer schwer absehbaren Gefahr fordert vom Gesetzgeber ein hohes Maß an Bestimmtheit und Verhältnismäßigkeit der Einschreitschwellen. Die Abwehr terroristischer Gefahren darf nicht zu Lasten der Freiheit das Gefahrenabwehrrecht im Ganzen verwässern.

Wesentliche Merkmale der Novelle bestanden in der Neuaufnahme der Kfz-Kennzeicherfassung, des Einsatzes von BodyCams, einer erweiterten Regelung der Videoüberwachung und der erneuten Einführung der Kennzeichenerfassung. Die Erfassung und der Abgleich von Kennzeichen sollen anlassbezogen erfolgen; sowohl die eingeführte Schwelle als auch das vorgesehene Verfahren halten sich im Rahmen der Vorgaben des Bundesverfassungsgerichts. Im Hinblick auf ein bestimmtes Ereignis oder eine bestimmte Gefahrenlage müssen nachvollziehbare Tatsachen vorliegen, die dann den Einsatz der entsprechenden Lesegeräte begründen. Die Eingriffsintensität der Maßnahme ergibt sich aus ihrer erheblichen Streubreite. Im Rahmen der Prüfungspflichten und Prüfungsrechte wird auch diese Maßnahme zukünftig im Hinblick auf die Verhältnismäßigkeit überprüft werden.

Der Landesgesetzgeber war bestrebt, die Videoüberwachung bei Großveranstaltungen zu erleichtern und die Eingriffsschwelle abzusenken. Dem Grunde nach ist es nachvollziehbar, bei der Zusammenkunft vieler Personen Videoüberwachung als ein Element des Sicher-

heitskonzepts einzusetzen. Dies hilft auch den Rettungskräften und der Gesamtorganisation. Jedoch müssen diese Einsatzsituationen hinreichend konkret begrenzt werden, um eine Ausweitung auf Situationen, die eine umfassende Aufnahme von Personen ermöglichen, auszuschließen. Es sollen nicht alle Besucher aller Großveranstaltungen anlasslos überwacht werden, sondern es soll auf eine konkrete Veranstaltung bezogen die Technik gezielt und begrenzt eingesetzt werden. Dies konnte im Rahmen des Gesetzgebungsverfahrens erreicht werden.

Der Einsatz von BodyCams dient vorrangig der Eigensicherung der Polizeibeamtinnen und Polizeibeamten. Sowohl von dem sog. Pre-Recording als auch dem Einsatz in Wohnungen wurde Abstand genommen. Damit sind die verfassungsmäßigen Grenzen gewahrt und das Einwirken des LfDI bereits in der Erprobung des Instruments konnte Früchte tragen (siehe unten sowie TB 2014/2015, S. 59).

Weiterer Gegenstand der Gesetzesnovellierung waren teilweise komplexe Anpassungen der (verdeckten) Datenverarbeitung an die Vorgaben des Bundesverfassungsgerichts, die es in seinem Urteil zum BKA-G vom 20. April 2016 aufstellte. Mechanismen des kompensatorischen Grundrechtsschutzes wurden präzisiert. Bei den eingriffsintensiven verdeckten Überwachungsmaßnahmen ist ein effektiver Kernbereichsschutz unabdingbar.

Prüfpflichten des LfDI bezüglich dieser und anderen grundrechtsintensiven Maßnahmen komplettieren diese Architektur und gewährleisten die rechtskonforme Wahrnehmung der Befugnisse. Die im POG neu aufgenommene Regelung des § 41b POG, die turnusmäßige Pflichtkontrollen von verdeckten Überwachungsmaßnahmen mindestens alle zwei Jahre vorsieht, dient der Umsetzung der Vorgaben aus dem Urteil zum BKA-G zwecks Gewährleistung einer wirksamen Kontrolle der Aufsichtsbehörde.

Die Änderungen des Polizei- und Ordnungsbehördengesetzes stellen einen wesentlichen Schritt zur Fortentwicklung des rheinland-pfälzischen Gefahrenabwehrrechts dar. Angesichts der Sicherheitslage insgesamt und der vielfältigen aktuellen Bedrohungen halten sich die Änderungen im Rahmen der grundrechtlichen Grenzen. Eine Reihe von, in der allgemeinen rechtspolitischen Diskussion, verfolgten Tendenzen werden erfreulicherweise nicht aufgegriffen. Weder wurde eine Regelung zur sog. elektronischen Fußfessel, noch zur Vorratsdatenspeicherung eingeführt. Damit bewegt sich die Novelle im Vergleich zu den in anderen Ländern und dem Bund novellierten Polizeigesetzen auf einem akzeptablen Niveau zur Wahrung von Freiheit. In der Folge muss dieses Niveau beibehalten werden. Weitere Verschärfungen oder die zusätzliche Einführung neuer Befugnisse würden die Balance zwischen Freiheit und Sicherheit sprengen. Jede Verschärfung wäre ein rechtsstaatlicher Rückschritt. Dies ist bei der anstehenden zweiten Gesetzesnovelle, die die Umsetzung der Richtlinie für Polizei und Justiz zum Gegenstand hat, zwingend zu berücksichtigen. Der Werkzeugkasten der fähigen rheinland-pfälzischen Polizei sollte zunächst erprobt werden, bevor er ohne Notwendigkeit erweitert wird. Dafür sprechen auch die Ergebnisse der Evaluation der bisherigen Befugnisse der rheinland-pfälzischen Polizei (siehe unten).

4.3 Polizei und Datenschutz – Hochschulgesprächstage Flugplatz Hahn

Seit 2016 unterstützt der LfDI auf Einladung der Hochschule der Polizei Rheinland-Pfalz im Rahmen der Hochschulgesprächstage den „Tag des Datenschutzes“ an der Hochschule in

Frankfurt Hahn.

Das zweimal jährlich stattfindende ganztägige Veranstaltungsformat, bestehend aus einem Einführungsvortrag des LfDI, themenorientierten Workshops und einer abschließenden Podiumsdiskussion von Vertretern der Hochschule, Studierenden und des LfDI, bringt die Polizeianwärterinnen und -anwärter anhand von Beispielen aus der Anwendungspraxis mit dem Datenschutz und der Informationsfreiheit in Kontakt. Das thematische Spektrum der Workshops reicht vom Verhalten in den sozialen Netzwerken und Big Data über polizeiliche Ermittlungsstrategien im Internet bis hin zu den Auswirkungen der Enthüllungen von Whistleblowern auf die Online-Kommunikation und den bestehenden Möglichkeiten, Datenspuren und die Ausforschung des eigenen Nutzungsverhaltens zu vermeiden. Auch in Zukunft soll diese Kooperation weitergeführt werden, um die Polizeianwärterinnen und Polizeianwärter in ihrem Selbstdatenschutz zu stärken und für die sensiblen Aufgaben und Befugnisse der polizeilichen Datenverarbeitung zu wappnen.

4.4 Evaluation der polizeigesetzlichen Eingriffsregelungen – Mehr Transparenz und weiterer Prüfstand

Nachdem die Landesregierung von ihrem Vorhaben einer vorgezogenen Evaluation der Maßnahmen gem. § 100 POG Abstand nahm (s. TB 2014/2015 S.60/61), erfolgte diese zum gesetzlich vorgegebenen Zeitablauf nach dem 31. März 2016.

Wie auch in dem davor liegenden Berichtszeitraum (1. April 2011 – 31. März 2016) stellt sich nach der Evaluation verstärkt die Frage, ob die Nichtnutzung vorhandener Ermächtigungsgrundlagen deren Erforderlichkeit insgesamt infrage stellt. Die betraf insbesondere die Maßnahme der Wohnraumüberwachung, die Funkzellenüberwachung und z.B. auch die Rasterfahndung. Sämtliche der o.g. Maßnahmen kamen im Evaluationszeitraum nicht zur Anwendung. Anders als dies vom wissenschaftlichen Institut und von Seiten der Landesregierung vertreten wurde, begründet dies aus Sicht des LfDI Zweifel an der Verfassungsmäßigkeit solcher Ermächtigungsgrundlagen.

Nachholbedarf scheint auch in Sachen Transparenz zu bestehen. Kritisch zu betrachten ist insbesondere, dass in einem erheblichen Prozentsatz der im Evaluationszeitraum durchgeführten Telekommunikationsüberwachungsmaßnahmen auf eine Unterrichtung deshalb verzichtet wurde, weil sich ein strafrechtliches Verfahren angeschlossen hat. Laut dem Evaluationsbericht erfolgte bei den 35 durchgeführten Telekommunikationsüberwachungsmaßnahmen in knapp der Hälfte der Fälle keine Unterrichtung, wobei in 8 Fällen ein sich anschließendes Strafverfahren als Grund genannt wurde.

Auch eine Unterrichtung von sonstigen betroffenen Personen nach § 40 Abs. 5 Satz 2 POG unterblieb in 5 Fällen mit dieser Begründung.

Für den LfDI ist die Frage einer nachträglichen Unterrichtung Betroffener bei verdeckten polizeilichen Maßnahmen aus Gründen der Transparenz von erheblicher datenschutzrechtlicher Bedeutung. Die anstehende Novellierung zur Anpassung des Polizei- und Ordnungsbehördengesetzes an die Richtlinie für Polizei und Justiz wird zu Nachbesserungen im Bereich der Benachrichtigungspflichten führen, sofern der Landesgesetzgeber dem Umsetzungsauftrag gerecht werden möchte.

4.5 BodyCams bei der Polizei

Die Einführung von BodyCams bei der Polizei wurde durch den LfDI weiter begleitet. Nach Abschluss der Pilotphase, die wegen der Vorfälle an Silvester 2015/2016 mit Einverständnis des LfDI verlängert wurde, erfolgte die Ausdehnung des Einsatzes der Körperkameras auch auf andere Polizeipräsidien. Eine Vorabaufnahme (Pre-Recording) war aufgrund der hierfür fehlenden Rechtsgrundlage nicht zulässig und wurde deaktiviert. Auch der Einsatz der BodyCams in Wohnungen war in dem Pilotprojekt nicht vorgesehen, was aus verfassungsrechtlicher Sicht nicht nur begrüßenswert, sondern zwingend notwendig ist. Dies ergab auch der Sachverständigenbericht im Nachgang des Piloteinsatzes. Der Piloteinsatz führte zur Schaffung einer rechtsstaatlichen und maßvollen Ermächtigungsgrundlage im Rahmen der Novellierung des Polizei- und Ordnungsbehördengesetzes (siehe oben). Die Einsatzbedingungen wurden in einer Verfahrensregelung zum Einsatz von BodyCams unter Beteiligung des LfDI festgelegt. Für die Polizei ist landesweit eine Anschaffung von ca. 250 Körperkameras geplant.

4.6 Unverschlüsselte Bestandsdatenabfragen der Polizei bei Dienstanbietern

Durch Presseveröffentlichungen wurde der LfDI darauf aufmerksam, dass Mitarbeiter der Polizei Auskunftsersuchen zu Bestandsdaten direkt an die Dienstanbieter mittels unverschlüsselter E-Mail stellen. Dadurch wurden vertrauliche personenbezogene Daten offen elektronisch versandt. Ursächlich waren die fehlende Verfügbarkeit einer Verschlüsselungssoftware an einigen Arbeitsplätzen sowie eine fehlende Entschlüsselungssoftware bei den Dienstanbietern. Außerdem kritikwürdig war, dass entgegen der gesetzlichen Anforderungen die Rechtsgrundlage für das Auskunftsersuchen nicht angegeben wurde. Teilweise wurden die Anfragen auch an Funktionsadressen gesandt.

Der LfDI nahm dies zum Anlass das Verfahren auf Sicherheit und Vertraulichkeit hin zu untersuchen und diesbezügliche Vorstellungen einer elektronischen Übermittlung von vertraulichen personenbezogenen Daten in technischer und datenschutzrechtlicher Hinsicht darzulegen. Auch wurde auf die Nutzung der rechtskonformen Möglichkeit der Bestandsdatenauskunft an die Bundesnetzagentur gem. § 26 POG i. V. m § 112 Abs. 1, Abs. 2 Nr. 2, Abs. 4 TKG hingewiesen, mittels der es den Polizeibehörden möglich ist, Bestandsdaten über eine zentralisierte, gesicherte Schnittstelle bei der Bundesnetzagentur anzufragen.

Dem Ministerium des Innern und für Sport und dem Landeskriminalamt war daran gelegen, die Fälle aufzuklären und ein sicheres und vertrauliches Verfahren zu etablieren. So wurde die Installation eines Verschlüsselungsprogramms auf sämtlichen Arbeitsplatzrechnern der Bediensteten der Polizei Rheinland-Pfalz im Auftrag des Ministeriums des Innern und für Sport durch die Zentralstelle für Polizeitechnik (ZPT) veranlasst und schlussendlich durchgeführt.

Die Mitarbeiter der Polizei Rheinland-Pfalz wurden durch eine von der Hochschule der Polizei erstellte Kurzanleitung informiert und auf die bestehende Dienstvereinbarung zur Verschlüsselung von Nachrichten an externe Empfänger hingewiesen und sensibilisiert.

Zur Minimierung der Fehlerquellen hält der LfDI die Implementierung einer zentralisierten Verfahrensweise auch für die manuelle Bestandsdatenabfrage für sinnvoll.

4.7 Lichtbildanforderungen bei der Bearbeitung von Straßenverkehrsordnungswidrigkeiten der Zentralen Bußgeldstelle Speyer (ZBS)

Den LfDI erreichte im Berichtszeitraum eine Vielzahl von Eingaben zur Ermittlungstätigkeit der Zentralen Bußgeldstelle des Polizeipräsidiums Rheinpfalz in Ludwigshafen. Im Mittelpunkt stand dabei der Lichtbildabgleich zur Feststellung der Fahreridentität, der nach Einschätzung des LfDI in einigen Fällen nicht im Einklang mit dem Rundschreiben des Ministeriums des Innern und für Sport v. 10.06.1996 (zuletzt geändert am 17.08.2011, MinBl. 2011, S. 179) „Vorlage und Übermittlung von Lichtbildern aus dem Pass- und Personalausweisregister im Rahmen der Verfolgung von Straßenverkehrsordnungswidrigkeiten“ stand.

Des Weiteren entsprach die Auslegung der Rücksendefrist des Anhörbogens durch den Fahrzeughalter nach Auffassung des LfDI nicht den datenschutzrechtlichen Erfordernissen, da diese unmittelbare Auswirkungen auf die folgende Lichtbildanforderung bei der Meldebehörde hatte.

In einem gemeinsamen Gespräch in Speyer, der eine Besichtigung der Räumlichkeiten der Bußgeldstelle vorausging, konnten die Standpunkte ausgetauscht werden. Es sollte eine Lösung gefunden werden, die sowohl dem Recht der betroffenen Personen auf ein transparentes Verfahren und der Achtung ihrer Persönlichkeitsrechte als auch dem Interesse der Bußgeldstelle und der Gerichte, ihre Verfahren effektiv durchführen zu können, Rechnung trägt. Mit der Verlängerung der Frist auf 10 Tage nach Zugang der Anhörung konnte ein Konsens gefunden werden.

Im Rahmen der Ermittlungstätigkeit der Zentralen Bußgeldstelle Speyer ist der Lichtbildabgleich eine Frage des Einzelfalls:

Wenn die Ermittlungen des Fahrzeugführers unmöglich oder der Aufwand unverhältnismäßig hoch wäre, kann das bei einer Radarüberwachung angefertigte Lichtbild mit dem bei der Ausweisbehörde hinterlegten Lichtbild des Fahrzeughalters abgeglichen werden, soweit diese Vorgehensweise geeignet ist, den Fahrzeugführer zu ermitteln. Dies stellt in der Regel ein im Vergleich zur Nachbarschaftsbefragung milderes Mittel dar, da mit der Ermittlung im sozialen Umfeld der betroffenen Person schwerwiegendere Eingriffe in dessen allgemeines Persönlichkeitsrecht gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG einhergehen.

Wenn aufgrund der Vielzahl in Betracht kommender Fahrzeugführer im Angehörigenkreis/in der Hausgemeinschaft des Fahrzeughalters der einzelne Lichtbildabgleich nicht erfolgsversprechend ist, sollten nicht wahllos auf einen beschränkten Personenkreis mehrere Lichtbildabgleiche erfolgen. Vorzugswürdig ist es dann, die in Betracht kommenden Personen zunächst mündlich oder schriftlich anzuhören. Erst wenn dies nicht aussichtsreich ist, kommt eine Ermittlung zur Fahreridentifikation in der Nachbarschaft in Betracht und ist in dieser Konstellation als milderes Mittel gegenüber der Ermittlung durch Lichtbildabgleiche anzusehen.

Die Abstimmungen mit der ZBS werden im Zusammenhang mit der geplanten Einführung einer neuen Bearbeitungssoftware auch im Jahr 2018 fortgeführt.

4.8 Öffentlichkeitsfahndungen durch Private

Der Kunde einer Fast-Food-Kette hatte dem LfDI mitgeteilt, dass an der Eingangstür zum

Restaurant ein Fahndungsplakat mit dem Zusatz angebracht sei, dass die darauf abgebildeten Personen wegen Diebstahls gesucht werden. Hinweise zu den beiden Personen wären an die Restaurantleitung zu richten. Die Verifizierung des Sachverhalts ergab, dass das Foto aus einer Videoüberwachung innerhalb der Räumlichkeiten des Restaurants stammte und durch den Geschäftsführer zum Aushang gebracht wurde. Beide Personen sollen mit einem Diebstahl eines Sitzkissens aus dem Fanartikelangebot eines Fußballvereins in Zusammenhang stehen, das im Thekenbereich als Dekoration ausgelegt war. Die Tat wurde mittels Videoüberwachung im Innenbereich des Restaurants aufgezeichnet.

Die Zielrichtung des Aushangs war nach den Angaben des Geschäftsführers die Identifizierung der Täter verbunden mit der Aufforderung zur Rückgabe des Sitzkissens. Der Geschäftsführer war mit der sofortigen Entfernung des Plakats einverstanden. Auf Grundlage des geschilderten Sachverhalts dürfte ein Verstoß gegen § 4 BDSG vorliegen. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt, anordnet oder der Betroffene eingewilligt hat. Im vorliegenden Fall dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Durch die Veröffentlichung werden die abgebildeten Personen in ihrem Recht am eigenen Bild verletzt (§ 22 KUG). Liegt keine Einwilligung vor, verletzt die Verbreitung des Fotos die Persönlichkeitsrechte des Abgebildeten und verstößt gegen § 22 KUG. Nur die Polizei ist gem. § 131b StPO befugt, bei Straftaten von „erheblicher Bedeutung“ Abbildungen eines Beschuldigten zu veröffentlichen, wenn andere Formen der Aufenthaltsermittlung erheblich weniger Erfolg versprechend oder wesentlich erschwert wären. Die Anordnung obliegt gem. § 131 StPO dem Staatsanwalt oder Richter. Gem. § 24 KUG ist es der Polizei als Behörde außerdem erlaubt, Bildnisse ohne Einwilligung des Berechtigten sowie des Abgebildeten zu vervielfältigen, zu verbreiten und zur Schau zu stellen.

Im Rahmen eines Auskunftsverfahrens werden zunächst die weiteren Umstände u. a. auch die Zulässigkeit der Videoüberwachung, mittels der das Lichtbild gefertigt wurde, durch den LfDI geprüft.

4.9 Akkreditierung und Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Großveranstaltungen, die seit jeher Gegenstand vielschichtiger Sicherheitsbemühungen der Sicherheitsbehörden und Veranstalter sind, sind in den vergangenen Jahren vermehrt Ziel terroristischer Anschläge oder der Drohung mit der Verübung solcher geworden. Dies nehmen die Veranstalter und Sicherheitsbehörden zum Anlass, die Sicherheitsvorkehrungen zu verschärfen und spezifischer auf die terroristischen Bedrohungen auszurichten.

Verstärkt sind dazu in den Sicherheitskonzepten bei Großveranstaltungen Zuverlässigkeitsüberprüfungen von Personen vorgesehen, die bei und im Vorfeld von Veranstaltungen Zutritt zu dem Veranstaltungsbereich haben. Der betroffene Personenkreis setzt sich je nach Art der Veranstaltung aus Beschäftigten, freiwilligen Helfern und externen Dienstleistern zusammen. Aus Anlass des Tages der Deutschen Einheit, der im Jahr 2017 in Mainz von der Staatskanzlei ausgerichtet wurde und aufgrund von Anfragen von anderen Veranstaltern und Eingaben von betroffenen Personen ist der LfDI mit der Thematik befasst.

Datenschutzrechtliches Spannungsverhältnis

Im Gegensatz zu anderen Bundesländern (z.B. Hessen, Hamburg, Thüringen) existiert in Rheinland-Pfalz keine bereichsspezifische Befugnis zur Zuverlässigkeitsüberprüfung durch die Polizei. Die Zuverlässigkeitsüberprüfungen erfolgen derzeit in der Regel einwilligungsbasiert. Diese Zuverlässigkeitsüberprüfungen einwilligungsbasiert vorzunehmen, ist zunächst aufgrund der fehlenden Freiwilligkeit der Einwilligung problematisch. Freiwilligkeit besteht dann, wenn die betroffenen Personen eine echte Wahlfreiheit haben. Diese entfällt in dem vorliegenden Fall deswegen, da die Versagung der Einwilligung, die Versagung der Akkreditierung zur Folge hat. Ohne Akkreditierung ist es den betroffenen Personen jedoch nicht möglich, bei der Veranstaltung mitzuwirken und sie haben damit wirtschaftliche Nachteile zu befürchten, die dadurch entstehen, dass sie ihrem Beschäftigtenverhältnis nicht nachgehen können oder es nicht eingehen können. Insoweit fehlen eine echte Freiwilligkeit und damit auch das konstituierende Element einer wirksamen Einwilligung.

Fehlende bereichsspezifische Rechtsgrundlage

Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Mit ihnen sind weitreichende Recherchen in polizeilichen Informationssystemen verbunden. Die betroffenen Personen werden in zahlreichen Dateien der Sicherheitsbehörden abgefragt, obwohl sie persönlich keinen Anlass gegeben haben und zu diesem Zeitpunkt keine Anhaltspunkte bestehen, dass von ihnen eine besondere Gefährdung ausgeht.

Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder, die Sicherheits- und Zuverlässigkeitsüberprüfungen für sicherheitsempfindliche Tätigkeiten regeln, sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig.

Das Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz beinhaltet keine bereichsspezifische Befugnis zur Zuverlässigkeitsüberprüfung durch die Polizei. Staatliche Eingriffe in das Recht auf informationelle Selbstbestimmung sind nur zulässig, wenn überwiegende Allgemeininteressen dies erfordern und sie auf einer gesetzlichen Grundlage beruhen, die den Grundsatz der Verhältnismäßigkeit beachtet und aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 65, 1). Die Schaffung einer Rechtsgrundlage würde für diesen Problemkomplex somit bereits zu einem höheren Maß an Rechtsstaatlichkeit beitragen.

Anforderung an eine bereichsspezifische Norm und ein rechtsstaatliches Verfahren

› Bereichsspezifische Bestimmung von Anlässen der Zuverlässigkeitsüberprüfungen

Die Anlässe, die solche polizeilichen Zuverlässigkeitsüberprüfungen erforderlich machen, sollten präzise bestimmt und dadurch gleichermaßen begrenzt werden. Neben der Sicherheit bei Großveranstaltungen betreffen weitere mögliche und regelungsbedürftige Zwecke die polizeiliche Zuverlässigkeitsüberprüfung von Personen, die eine Tätigkeit als Bediensteter in Sicherheitsbehörden anstreben (Zuverlässigkeitsüberprüfungen im Rahmen von Bewerbungsverfahren).

› Gefahrenschwelle bei Großveranstaltungen

Komplementär zu vergleichbaren Regelungen sollte der Kreis der betroffenen Großveranstaltungen auf solche beschränkt werden, die „besonders gefährdet sind".

› Datenschutzanforderungen und Erforderlichkeitsgrundsatz

Durch die Regelung des Erforderlichkeitsgrundsatzes („soweit erforderlich") soll gesichert werden, dass der Umfang der Dateien, die zur Überprüfung der Zuverlässigkeit abgefragt werden, sowie der Personenkreis, bei denen diese Abfragen notwendig sind, auf das erforderliche Maß beschränkt werden. Für die Zuverlässigkeitsüberprüfung erhoben werden sollten lediglich die Daten, die für die Identitätsfeststellung erforderlich sind.Daneben sollten spezifische Anforderungen an den Umfang der Übermittlung der Daten, die bei der Zuverlässigkeitsüberprüfung erhoben wurden (Sicherheitsbedenken ja oder nein), an den Veranstalter geregelt werden, sowie die spezifisch erforderliche Speicherdauer und die damit korrespondierenden Löschpflichten.

› Beteiligung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Die Regelungen sollten ein Anhörungsrecht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit enthalten, damit dieser beratend auf eine datenschutzkonforme, insbesondere datensparsame Ausgestaltung und Beschränkung der spezifischen Zuverlässigkeitsüberprüfung hinwirken kann (vgl. § 13b Abs. 1 S. 2 HSOG).

› Transparentes Verfahren

Die Regelung sollte die Zustimmung/Einwilligung der betroffenen Personen als transparenzsteigernde Verfahrensvoraussetzung (so auch im § 8 Abs. 2 S. 1 LSüG) vorsehen und den Rechten der betroffenen Personen angemessen Rechnung tragen, wie z.B. dem Recht auf Auskunft. Es sollten zudem Verfahrensgarantien vorgesehen werden, wie die Anhörung der betroffenen Person vor negativer Entscheidung.

› Datenschutz-Folgenabschätzung

Die Eingriffsintensität der Überprüfungen und die Sensibilität der Daten macht es erforderlich, entsprechend der Anforderungen sowohl der Datenschutz-Grundverordnung als auch der Richtlinie für Polizei und Justiz im Vorfeld einer Veranstaltung eine Datenschutz-Folgenabschätzung durchzuführen.

Auch in anderen Bundesländern gewinnt diese Thematik zunehmend an Relevanz. Mit der Entschließung „Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren" (https://s.rlp.de/entschliessungdsk042018) fordert die Konferenz der Datenschutzbehörden des Bundes und der Länder die Verantwortlichen dazu auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Der LfDI wird weiterhin mit den Verantwortlichen darauf hinwirken, ein Verfahren zu etablieren, das dem Verantwortlichen Rechts- und Handlungssicherheit und den betroffenen Personen ein Höchstmaß an Transparenz und Rechtsstaatlichkeit gewährleistet.

4.10 Digitalisierung der Polizei – Kontrolle des TKÜ-CC

Die Digitalisierung macht auch vor den Sicherheitsbehörden keinen Halt. Der rheinland-pfälzischen Polizei ist stets daran gelegen, ihre Arbeit und Ermittlungsarbeit an dem Stand der Technik auszurichten. Dass dies nur in datenschutzgerechter und datensicherer Weise geschehen sollte, wird durchweg durch die Einbeziehung des LfDI gewährleistet. Dies geschieht durch Projektvorstellungen und durch Kontrollen des LfDI als Follow-Up zu den Projekten.

Im Jahr 2012 wurde bei dem Landeskriminalamt Rheinland-Pfalz für die rheinland-pfälzische Polizei das „Competence-Center Telekommunikationsüberwachung" eingerichtet. Nachdem die Errichtung von dem LfDI bereits beratend betreut wurde, wurde im Jahr 2017 eine Kontrolle des TKÜ-CC vorgenommen. Im Vorfeld der Kontrolle wurden Fallzahlen und Statistiken zu den gegenständlichen Maßnahmen erfragt. So konnten besondere Kontrollbedarfe erfragt werden, um in der Kontrolle sinnvolle Schwerpunkte setzen zu können. Zahlenmäßige Angaben konnten zum überwiegenden Teil geliefert werden; für die Differenzierung zwischen Erst- und Verlängerungsanordnungen musste beim Ministerium für Justiz angefragt werden. Wünschenswert wäre eine regelmäßige zweijährige Lieferung der Statistiken durch das LKA (z.B. zum 1.3. des Folgejahres eines Zweijahreszeitraums).

Im Rahmen von drei Kontrollterminen wurden folgende Komplexe untersucht:

› Technische Infrastruktur für die TKÜ; Organisatorische und technische Durchführung einer TKÜ, Kernbereichsschutz

› Stille SMS/Funkzellenortung, IMSI-Catcher

› Funkzellenabfragen

Maßnahmen im Rahmen einer Quellen-TKÜ wurden bislang nicht durchgeführt. Als technische Lösungen stünden dafür ein vom BKA entwickeltes Tool (PC/Mobil), sowie ein kommerzielles Produkt zur Verfügung; teilweise stand die Freigabe der Lösungen für den operativen Einsatz jedoch noch aus. Eine Lösung zur Online-Durchsuchung war noch in der Entwicklung.

Die festgestellten Verfahrensweisen und Abläufe begegneten keinen grundsätzlichen Bedenken. Dokumentation und Nachvollziehbarkeit waren in ausreichendem Umfang gewährleistet. Im Ergebnis haben sich kleinere Anpassungsnotwendigkeiten ergeben (z.B. Dokumentationsmängel, Aktualisierungsbedarfe bei Dienstanweisungen, einzelne Umsetzungsdefizite, Überarbeitung Rollen- und Berechtigungskonzept, Umsetzung der Kennzeichnungspflichten). Insgesamt bewegt sich die TKÜ durch das Landeskriminalamt jedoch im Rahmen der rechtlichen Vorgaben. Die erforderlichen Anpassungen wurden veranlasst.

Bei der Prüfung hat sich ergeben, dass das LKA, abgesehen von eigenen TKÜ-Maßnahmen, lediglich technischer Dienstleister für die ermittlungsführenden Dienststellen ist. Aufgrund dieser Service-Funktion verfügt das LKA für die Masse der Maßnahmen nur über einen Teil der notwendigen Dokumentation. Bestimmte, für die Datenschutzkontrolle relevante Fragen (z.B. Benachrichtigung der betroffenen Personen, Abwägungsgesichtspunkte, Verhältnismäßigkeitsprüfungen, Begründungen, Einhaltung von verfahrenssichernden Voraussetzungen) befinden sich in der Ermittlungsakte der jeweiligen Polizeidienststellen bzw. der Staatsanwaltschaften, da sie auch ausschließlich deren Aufgabenbereiche betreffen. Es ist daher vorgesehen 2018 bei ausgewählten Präsidien/

Staatsanwaltschaften entsprechende Folgekontrollen durchzuführen.

4.11 Videoüberwachung

4.11.1 Aktuelle Entwicklungen

Videoüberwachungsverbesserungsgesetz

Durch das sog. Videoüberwachungsverbesserungsgesetz wurde 2016/2017 das Bundesdatenschutzgesetz dahingehend geändert, dass der Betrieb von Überwachungskameras durch nicht-öffentliche Stellen in öffentlich zugänglichen Bereichen erleichtert wird. Ziel der Bundesregierung war auch hier die Erhöhung der Sicherheit im öffentlichen Raum. Dazu wurde der § 6b BDSG dahingehend geändert, dass bei der Videoüberwachung von öffentlich zugänglichen, großflächigen Anlagen wie Sportplätzen und Einkaufszentren sowie in Einrichtungen und Fahrzeugen des öffentlichen Nahverkehrs der Schutz von Leben, Gesundheit oder Freiheit der sich dort aufhaltenden Menschen als ein besonders wichtiges Interesse gilt. Diese Rechtsgüter sollen die schutzwürdigen Interessen der betroffenen Personen in Zukunft überwiegen.

In der Konsequenz müssten die Datenschutzbeauftragten zukünftig im Rahmen ihrer Entscheidung für bzw. gegen die Videotechnik Sicherheitsbelange stärker berücksichtigen. Dagegen wurde sich seitens der unabhängigen Datenschutzbehörden des Bundes und der Ländern bereits im November 2016 vehement ausgesprochen. In ihrer Entschließung „Videoüberwachungsverbesserungsgesetz zurückziehen!“ (https://s.rlp.de/entschliessungdsk112016) der 92. Datenschutzkonferenz in Kühlungsborn vom 9. November 2016 forderten sie deswegen den Bundesminister des Innern auf, das Videoüberwachungsverbesserungsgesetz zurückzuziehen. Kritisiert wird dabei unter anderem, dass der Gesetzesentwurf nicht deutlich mache, warum eine erleichterte Videoüberwachung mehr Sicherheit gewährleisten soll, als es bereits nach der jetzigen Rechtslage möglich ist. Daneben wird die Abschreckungsgefahr gegenüber Terroristen, die die mediale Aufarbeitung von Anschlägen und die damit einhergehende Verbreitung des Terrors gerade erzielen, bezweifelt. Schließlich wird der präventive Zweck der Videoüberwachung angezweifelt, da das notwendige Live-Monitoring und ein hinterlegtes Eingriffskonzept von den nicht-öffentlichen Stellen in der Regel nicht geleistet werden kann. Besonders kritikwürdig ist die drohende Verlagerung der Gewährleistung öffentlicher Sicherheit auf die nicht-öffentlichen Stellen, obwohl dies die ureigene Aufgabe der Sicherheitsbehörden ist, die dazu auch über die ausreichenden landes- und bundesgesetzlichen Grundlagen verfügen.

Fortwirkung der Problematik im Rahmen der DS-GVO

Auch in der Novellierung des Bundesdatenschutzgesetzes wurde diese unverhältnismäßige Gewichtung von Rechtsgütern übernommen und der § 4 BDSG n.F. geschaffen. Dieser ist aus den gleichen Gesichtspunkten aus datenschutzrechtlicher Sicht weiterhin kritikwürdig und es bestehen hinsichtlich der Konformität mit Europarecht erhebliche Zweifel.

Die Regelung betrifft die Videoüberwachung durch private Verantwortliche und öffentliche Stellen des Bundes gleichermaßen. Die unmittelbar wirksame Datenschutz-Grundverordnung gibt dagegen keinen Spielraum im Rahmen einer Öffnungsklausel für die Schaffung einer solchen Datenverarbeitungsgrundlage für private Verantwortliche. In der Konsequenz müsste im Rahmen des Anwendungsvorrangs

geprüft werden, inwieweit § 4 BDSG n.F. angewendet werden kann. Gelingt eine verordnungskonforme Auslegung? Da die DS-GVO keine solche Abwägungsentscheidung zugunsten der öffentlichen Sicherheit – ohne, dass eine konkrete Gefahr droht – vorsieht, dürften Zweifel begründet sein. Dieses Spannungsverhältnis zu klären wird ein erstes Ziel sein, um ab Wirksamkeit der DS-GVO Rechtssicherheit für Verantwortliche und betroffene Personen zu schaffen.

Dashcam-Einsatz durch Private

Der Einsatz von Dashcams durch Private nimmt immer weiter zu. Die On-Board-Kameras wurden bislang aus datenschutzrechtlicher Sicht durchweg kritisch gesehen. Insbesondere im Fall einer anlasslosen Aufzeichnung des gesamten Verkehrsraums ist der Einsatz in der Regel unzulässig und nicht von § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG gedeckt.

In diesen Fällen ist das Recht der Vielzahl betroffener Personen daran, sich in dem Verkehrsraum aufzuhalten, ohne überwacht zu werden, gegenüber dem Interesse des Dashcambetreibers, potenzielle Beweismittel zu gewinnen, vorrangig. Berücksichtigenswert bei dieser Interessenabwägung ist, dass die betroffenen Personen in der Regel keine Kenntnis von der Videoüberwachung haben und sich ihr damit nicht entziehen können. Zu Lasten des Interesses der Betreiber fällt demgegenüber ins Gewicht, dass dieser anlasslos sämtliche Verkehrsteilnehmer unter einen Generalverdacht stellt. Die Hinweispflichten werden bei dem Einsatz von Dashcams ebenfalls in der Regel nicht erfüllt.

Möglicher datenschutzkonformer Betrieb von Dashcams

Wenn Dashcams technisch dergestalt konfiguriert werden, dass sie lediglich bei einem Aufprall aufzeichnen, kann die datenschutzrechtliche Zulässigkeit dagegen anders zu beurteilen sein. Eine solche Einstellung könnte etwa durch eine Aufnahme im Schleifenmodus (mit einer Aufnahmedauer und Zwischenspeicherung von max. 30 – 60 Sekunden) und der dauerhaften Speicherung ausschließlich bei Auslösung eines sogenannten Unfallsensors sein. In dieser Konstellation erfolgt die Aufnahme nur dann und nur soweit ein Unfallgeschehen vorliegt. Die Dauer der Erfassung von Unbeteiligten ist wesentlich geringer.

Bei einer derartigen Funktionsweise ist im Rahmen der Interessenabwägung ein tatsächliches und nicht ein potentielles Interesse der Verantwortlichen an der Beweissicherung des Unfallgeschehens in die Abwägungsentscheidung einzubeziehen und gegenüber den Interessen der betroffenen Personen, die in einem vergleichsweise geringfügigeren Umfang erfasst werden, abzuwägen. Die Interessenabwägung kann bei einer solchen anlassbezogenen und somit konkreteren Nutzung der Kamera dahingehend ausfallen, dass die berechtigten Interessen des Dashcambetreibers gegenüber denen der betroffenen Personen überwiegen. Jedoch entbindet dies die Betreiber als Verantwortliche nicht davon, weitere datenschutzrechtliche Vorgaben einzuhalten, wie Löschverpflichtungen, das Vorsehen von technischen und organisatorischen Maßnahmen sowie die Sicherstellung der Hinweispflicht nach § 6b Abs. 2 BDSG.

Ausblick auf die Datenschutz-Grundverordnung

Mit der Nutzung von Dashcams geht eine erhebliche und anspruchsvolle datenschutzrechtliche Verantwortlichkeit einher, deren Missachtung sowohl Anordnungen als auch die Verhängung von Geldbußen durch die

Datenschutzaufsichtsbehörden nach sich ziehen kann. Diese Verantwortlichkeit ist mit der ab dem 25. Mai 2018 unter der Datenschutz-Grundverordnung geltenden Rechtslage noch umfangreicher. Die Verantwortlichen treffen dann Dokumentations- und Rechenschaftspflichten hinsichtlich des datenschutzkonformen Einsatzes der Kamera. Außerdem sind sie in der Regel verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, da mit der durch die Kamera verbundenen Datenverarbeitung eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“ verbunden ist, die nach Art. 35 Abs. 3 lit. a DS-GVO eine Datenschutz-Folgenabschätzung zwingend nach sich zieht.

Dieser Verantwortung sollten sich die verantwortlichen Betreiber von Dashcams bewusst sein.

4.11.2 Praxisfälle aus dem Bereich Videoüberwachung

Videoüberwachung vor und in einem Juwelier

Eine der zahlreichen an den LfDI gerichteten Eingaben im Bereich Videoüberwachung betraf eine Überwachungsanlage eines Juweliers. Der Verantwortliche überwache laut der Eingabe sowohl die Geschäftsräume als auch großflächig den Außenbereich samt des Gehweges vor dem Juwelier.

Das Auskunftsersuchen des LfDI an den Verantwortlichen ergab, dass es sich bei den Überwachungskameras an der Außenfassade des Juweliers um Kameraattrappen zu Abschreckungszwecken handelt, die die Auslage und die Schaufenster schützen sollen. Die Kameras in den Geschäftsräumen seien allerdings allesamt in Betrieb. Diese dienten u.a. dazu, nach einem möglichen Einbruch oder Raub die Identifikation von Tätern zu ermöglichen und auf Verlangen der Polizei und Staatsanwaltschaft zur Verfügung zu stellen.

Wenn eine Videoüberwachung dazu eingesetzt wird, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen. Prinzipiell ist hierfür aber eine tatsächliche Gefahrenlage zu fordern. In bestimmten Fällen ist dagegen eine abstrakte Gefährdungslage ausreichend, wenn es sich um eine Fallkonstellation handelt, die nach der Lebenserfahrung typischerweise gefährlich ist. Dies ist z. B. in Geschäften wie Juwelieren der Fall, die wertvolle Ware verkaufen und damit stärker überfallgefährdet sind. Dennoch muss auch hier der Grundsatz der Verhältnismäßigkeit eingehalten werden und die Videoüberwachungsmaßnahme auf das erforderliche Maß beschränkt werden.

Da von Kameraattrappen keine personenbezogenen Daten erhoben, verarbeitet oder genutzt werden, findet das BDSG hierauf keine Anwendung. Kameraattrappen sind für Betroffene häufig nicht von funktionstüchtigen Kameras zu unterscheiden. Für die betroffenen Personen kann der Eindruck entstehen, dass tatsächlich eine Videoüberwachung stattfindet. Dadurch könnten sie sich in gleicher Weise eingeschränkt fühlen wie bei einer Überwachung durch echte Kameras. Von einer Kameraattrappe kann also derselbe Überwachungsdruck wie von einer funktionsfähigen Kamera ausgehen und insofern in das Persönlichkeitsrecht eingegriffen werden. Der Juwelierinhaber wurde darauf aufmerksam gemacht, dass Betroffene zivilrechtliche Unterlassungs- und Abwehransprüche wegen der Verletzung des allgemeinen Persönlichkeitsrechts (vgl. §§ 823, 1004 BGB) geltend machen könnten.

Vor diesem Hintergrund wurde empfohlen, die Kameraattrappen so auszurichten, dass der An-

schein erweckt wird, ein schmaler, maximal ein Meter breiter Streifen vor dem Schaufenster von der Videoüberwachung werde erfasst. Diesen Bereich erachtet auch die Rechtsprechung (Amtsgericht Berlin-Mitte Az. 16 C 427/02 v. 18.12.2003) als zulässig. Voraussetzung ist allerdings, Passanten haben dadurch auch die Möglichkeit, sich dem Überwachungsdruck durch Ausweichen zu entziehen.

Bezüglich der Videoüberwachung der Geschäftsräume wurde darauf hingewiesen, dass die Bereiche der Tresen auch Arbeitsplätze von Beschäftigten darstellen. Es muss gewährleistet sein, dass keine Rundumüberwachung der Mitarbeiter erfolgt, sondern Bereiche vorhanden bleiben müssen, in denen diese sich dem Beobachtungsbereich entziehen können.

Videoüberwachung zum Zwecke der Dokumentation des Baufortschritts auf Baustellen und zum Diebstahlschutz

Vermehrt erhält der LfDI Anfragen von Bauunternehmen oder Bauherren, die den Baufortschritt Ihres Bauvorhabens mittels einer Webcam dokumentieren möchten und in diesem Zusammenhang anfragen, wie eine datenschutzgerechte Ausgestaltung erreicht werden kann.

Die Zulässigkeit der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Geräten, d.h. Videoüberwachung richtet sich auch hier grundsätzlich nach § 6b BDSG. Danach ist die Videoüberwachung nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und wenn schutzwürdige Interessen der betroffenen Personen nicht überwiegen. Wenn öffentlich zugängliche Räume von der geplanten Videoüberwachung betroffen sind, ist diese Maßnahme, nur zu Dokumentationszwecken der Baufortschritte, grundsätzlich nicht zulässig, da hier schutzwürdige Interessen der betroffenen Personen entgegenstehen.

Bei der bloßen Ausrichtung der Kamera auf die Baustelle ist aufgrund des Betretungsverbots davon auszugehen, dass kein öffentlich zugänglicher Raum beobachtet wird, wenn umliegender öffentlich zugänglicher Raum wie Verkehrsraum und insbesondere Nachbargrundstücke von der Beobachtung ausgeschlossen werden.

Sofern kein öffentlich zugänglicher Raum beobachtet wird, beurteilt sich die Zulässigkeit der Videoüberwachung nach § 28 BDSG. Gemäß § 28 Abs. 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung für die Erfüllung von eigenen Geschäftszwecken zulässig, soweit es zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist und wenn schutzwürdige Interessen der betroffenen Personen nicht überwiegen. Baustellenmitarbeiter, Bauleiter und Architekten usw. sind hier besonders als Betroffene von der Videoüberwachung zu betrachten. In die Bewertung der Zulässigkeit einer Überwachungsmaßnahme mit einfließen sollte der Aspekt, dass bei einer Übertragung des Webcam-Bildes in das Internet, eine unbestimmte Vielzahl von Personen weltweit Zugriff auf die Übertragungen haben.

Datenschutzrechtliche Bedenken bestehen gegen eine Baudokumentation mit einer Webcam grundsätzlich nicht, wenn folgende Maßgaben sichergestellt werden:

› Lediglich Übersichtsaufnahmen des Baufortschritts angefertigt werden und somit eine Identifizierung der arbeitenden Personen möglichst ausgeschlossen werden kann. Diesem Aspekt ist mit einer geringen Auflösung der Kameras, deaktivierter Zoom-Möglichkeit

und dem Betrieb der Kameras im Weitwinkelbereich Rechnung zu tragen. Auch intelligente Softwarelösungen zum Auspixeln von Personen sind aus datenschutzrechtlicher Sicht zu begrüßen.

› Öffentlich zugänglicher Raum wie Verkehrsraum, Nachbargrundstücke und Hausfassaden benachbarter Grundstücke von der Erfassung ausgeschlossen werden.

› Die Kamera sollte erst nach Beendigung der Bautätigkeit in Betrieb gesetzt werden, sodass möglichst keine Mitarbeiter mehr erfasst werden.

› Mögliche Betroffene sind im Vorfeld der Überwachung über die Maßnahme zu informieren. Auf den Umstand der Beobachtung und die hierfür Verantwortlichen (Name, Telefonnr.) ist durch geeignete Maßnahmen hinzuweisen (§ 6b Abs. 2 BDSG). Hinweisschilder sind gut wahrnehmbar an allen Zugängen zur überwachten Baustelle anzubringen.

Da selbst bei Übersichtsaufnahmen nicht gänzlich ausgeschlossen werden kann, dass mit vorhandenem Zusatzwissen einzelne Personen identifiziert werden können (z.B. Kranführer xy hat Dienst um 14 Uhr), ist es aus beschäftigtendatenschutzrechtlichen Gesichtspunkten anzuraten, schriftliche Festlegungen (bei Vorhandensein eines Betriebsrats in Form von Betriebsvereinbarungen, andernfalls in Form von Betriebsanweisungen) zum konkreten Zweck der Überwachung zu treffen und auszuschließen, dass eine Leistungs- und Verhaltenskontrolle der Beschäftigten erfolgt. Vermeintliche Einwilligungslösungen kommen bei abhängigen Beschäftigten nicht in Betracht, da diese angesichts des Abhängigkeitsverhältnisses nicht freiwillig in eine Datenverarbeitung einwilligen können.

Als weiteren Zweck wird von den Verantwortlichen für die Baustellen-Überwachung Diebstahlprävention und –aufklärung angegeben. Auf den Baustellen lagert in der Regel wertvolles Baumaterial wie Kabel; zudem auch schweres Baustellengerät. Gerade in Zeiten von hohen Rohstoffpreisen lädt dies Diebe zur Selbstbedienung ein.

Zu diesem Zweck installierte Webcams sollen gerade durch eine hohe Auflösung eine Identifizierung von Tätern sicherstellen. Datenschutzrechtlichen Bedenken lässt sich hier möglicherweise durch eine Begrenzung der Überwachung auf die Nachtzeiten in Verbindung mit einem Bewegungsmelder begegnen. Wie bereits oben im beschäftigtendatenschutzrechtlichen Zusammenhang erwähnt, sind in diesem Fall besonders hohe Anforderungen an klare Regelungen in Betriebsvereinbarungen und –anweisungen zu stellen. Es ist klar und transparent zu regeln, unter welchen Voraussetzungen durch wen Einsicht in die hochauflösenden Aufnahmen genommen werden darf und auf welche Weise dies zu protokollieren ist. Gegebenenfalls lässt sich datenschutzrechtlichen Anforderungen auch durch intelligente Softwarelösungen wie dem automatischen Verpixeln von Gesichtern und Kfz-Kennzeichen und dem Entpixeln nur im Schadensfall mit 2 kryptografischen Schlüsseln zur Gewährleistung eines Vier-Augen-Prinzips Rechnung tragen.

Baustellenüberwachung mittels Webcams (Übertragung des Live-Bildes) in das Internet

Ein in diesem Zusammenhang beim LfDI anhängiges Verfahren behandelt die Webcam-Überwachung von mehreren im Bundesgebiet liegenden Baustellen durch ein Bauunternehmen. Die Übertragung des meist personenscharfen Live-Bildes in das weltweite Netz erfolgt dabei durch einen Dienstleister. Im Hinblick auf

die vom Verantwortlichen angegebenen Zwecke wie Baudokumentation und Diebstahlprävention und –aufklärung ist aus datenschutzrechtlicher Sicht u.a. hoch problematisch, dass keine Trennung der Zwecke hinsichtlich der Ausgestaltung der Videoüberwachung vorgenommen wurde. Im Internet – und damit einem nahezu weltweit unbegrenzten Publikum zugänglich – laufen hochauflösende Bilder mit einer 2-3 sekündlichen Frequenz auf. Speicherungen von Einzelbildern erfolgen 15 minütig. Bemerkenswert ist auch, dass keine Vorabkontrolle (bzw. künftig Datenschutz-Folgenabschätzung) zur Eindämmung der Risiken für die betroffenen Personen vorgenommen wurde. Betriebsvereinbarungen und damit konkrete Regelungen zu beschäftigtendatenschutzrechtlichen Aspekten wie dem Ausschluss der Leistungskontrolle, Zugriffe auf unverpixelte Aufnahmen bei Vorfällen und Berechtigungen wurden bezüglich der Überwachungsmaßnahmen nicht getroffen. Außerdem wird eine nicht ausreichende Maskierung von Straßen und damit öffentlich zugänglicher Bereiche sowie von angrenzenden Privathäusern bemängelt.

Das Verfahren befindet sich noch im Anhörungsstatus des Verantwortlichen und dauert zum Redaktionsschluss noch an.

Personenbezug bei Wärmebildkameras?

Ein externes Datenschutzberatungsbüro ist an den LfDI mit der Frage herangetreten, ob Wärmebildkameras auch vom Anwendungsbereich des § 6b BDSG erfasst seien.

Der LfDI vertritt dabei die Auffassung, dass Wärmebildkameras zwar unter den weit gefassten Begriff der „optisch-elektronischen Einrichtungen“ fallen, eine Subsumtion unter § 6b BDSG daran scheitern wird, dass ein Personenbezug bei derartigen Aufnahmen grundsätzlich verneint werden muss. Anhand des erzeugten Falschfarben-Wärmebildes lassen sich in der Regel keine personenidentifizierenden Merkmale wie etwa die Besonderheiten der Gesichtszüge erkennen.

Begrifflich von Wärmebildkameras abzugrenzen sind hier Kameras mit Infrarotblitz, die oftmals als Wildkameras eingesetzt werden und Nachtsichtkameras. Bei mit solchen Einrichtungen erhobenen Daten wird ein Personenbezug bejaht.

Datenschutzrechtlich relevant kann der Einsatz von Wärmebildkameras im Einzelfall dann werden, wenn mit vorhandenem Zusatzwissen ein Personenbezug hergestellt werden kann, die Daten somit personenbeziehbar sind. Beispiel: Ein Arbeitgeber überwacht zum Objektschutz mittels Wärmebildkamera, ob sein Firmengrundstück in der Nacht betreten wird. Hiervon wird auch das patrouillierende Wachpersonal erfasst. Anhand des Dienstplans könnten die erhobenen Daten einer Person zugeordnet werden. Hier wäre im Einzelfall eine Interessenabwägung erforderlich.

Videoüberwachung von Tankstellen

Im Berichtszeitraum erreichten den LfDI mehrere Eingaben im Zusammenhang mit videoüberwachten Tankstellen. Tankstellen sind heutzutage fast alle mit Videoüberwachungsanlagen ausgestattet. Diese erfassen nicht nur die Zapfsäulen und den Außenbereich, sondern auch den angeschlossenen Tankstellenshop. Die Eingaben bezogen sich insbesondere auf die Überwachung des Bereichs der Sitzgelegenheiten und Stehtresen.

Im Falle der Videoüberwachung von Tankstellen gilt die Besonderheit, dass diese oftmals einem erhöhten Gefährdungspotential durch Überfälle ausgesetzt sind. Hinzu kommt, dass Kunden sich im Regelfall nur kurzfristig zur Ab-

wicklung des Bezahlvorgangs im Laden aufhalten. Die Überwachung bestimmter Ladenbereiche (Eingänge, Bereiche vor dem Tresen etc.) ist demnach in der Regel zulässig. Auch gegen die Überwachung der Zapfsäulenbereiche zur Aufklärung von Benzindiebstählen bestehen regelmäßig keine datenschutzrechtlichen Bedenken. Zu beachten ist allerdings, dass die Überwachung auf ein erforderliches Mindestmaß begrenzt werden muss.

So ist eine lückenlose und dauerhafte Überwachung des Tresens und somit des Arbeitsplatzes des Mitarbeiters wegen des damit einhergehenden ständigen Überwachungsdrucks unzulässig. Hier besteht die Möglichkeit, die Kamera lediglich auf den Bereich vor dem Tresen bzw. von oben auf den Tresen auszurichten. Es muss außerdem ausgeschlossen werden, dass die Videoüberwachung zur Kontrolle der Mitarbeiter eingesetzt wird.

Im Interesse der Kunden ist auch das PIN-Eingabefeld beim bargeldlosen Zahlungsverkehr auszuschließen. Stehtisch- und Sitzbereiche für die Kundschaft sind vom Erfassungsbereich der Kameras auszuschließen, da diese nicht nur zum kurzfristigen Verweilen einladen. Die Videoüberwachung eines Gastbereiches ist in der Regel datenschutzrechtlich unzulässig. Solche Bereiche sollen zum längeren Verweilen, Entspannen und Kommunizieren einladen und damit nicht mit Videokameras überwacht werden. Gerade der Freizeitbereich greift eine Videoüberwachung besonders intensiv in das Persönlichkeitsrecht des Gastes ein, da sie die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gastronomiebesucher erheblich stört.

In den konkreten, aufgrund von Eingaben geprüften, Tankstellen konnten datenschutzrechtliche Bedenken durch Anpassung der Erfassungswinkel der Kameras, Neuausrichtungen oder Abbau ausgeräumt werden. Weitere Beanstandungen gab es bezüglich der Hinweispflicht nach § 6b Abs. 2 BDSG und zu langer Speicherfristen (§ 6b Abs. 5 BDSG).

Videoüberwachung anlässlich der Mainzer Straßenfastnacht

Bei Großveranstaltungen auf öffentlichen Plätzen sehen sich private Veranstalter immer schärferen Sicherheitsauflagen ausgesetzt. Im Vorfeld der Saisoneröffnung der Mainzer Straßenfastnacht hat sich der Veranstaltungsleiter mit der Bitte um datenschutzrechtliche Prüfung des Videoüberwachungskonzeptes an den LfDI gewandt.

Auf dem vorgelegten Lageplan war ersichtlich, dass alle Zugänge zum Veranstaltungsgelände beispielsweise durch einen Sicherheitsdienst kontrolliert werden können und der Zugang beschränkt werden kann.

Im Hinblick auf den verfolgten Zweck der Videoüberwachung (Prüfung der Frequentierung des Platzes) ist aus datenschutzrechtlicher Sicht anzumerken, dass verhältnismäßigere, d.h. weniger in die Persönlichkeitsrechte der betroffenen Personen eingreifende, aber gleichermaßen effektive Mittel zur Verfügung stehen (mildere Mittel). So könnte eine grobe Personenzählung (auch mittels technischer Unterstützung) an allen Zugängen zum Veranstaltungsgelände erfolgen und bei Erreichen der Höchstzahl eine Sperrung des Platzes veranlasst werden. Zudem könnte Sicherheitspersonal durch bloße Beobachtung von einer Erhöhung (z.B. der Bühne) die Lage beobachten und etwa per Funk oder Ähnlichem einen Stopp des Einlasses veranlassen. Steht ein sogenanntes milderes Mittel zur Verfügung, wäre eine Videoüberwachung nicht zulässig. Diese Erwägungen sind im Sicherheitskonzept zu berücksichtigen.

Datenschutzrechtliche Bedenken bestehen nach Berücksichtigung der o.g. Ausführungen gegen eine Videoüberwachung als flankierende Maßnahme grundsätzlich nicht, wenn Sie folgende Punkte beachten:

› Die Videoüberwachung ist auf das erforderliche Maß zu beschränken. D.h. die Videoüberwachung sollte lediglich auf eine Beobachtung in Echtzeit (Monitoring) beschränkt werden und es sollten keine personenbezogenen und personenbeziehbaren Bilder erhoben werden. Dies ist durch eine geringe Auflösung der Kameras, deaktivierte Zoom-Möglichkeit und einen Betrieb der Kameras im Weitwinkelbereich sicherzustellen. Bloße Übersichtsaufnahmen des Geländes sind ausreichend.

› Es ist auszuschließen, dass die Kameras auf Anwohnerhäuser gerichtet sind und beispielweise Balkone oder Fenster miterfasst werden können.

› Auf den Umstand der Beobachtung und den hierfür Verantwortlichen (Name, Telefonnr.) ist durch geeignete Maßnahmen hinzuweisen (§ 6b Abs. 2 BDSG). Hinweisschilder sind gut wahrnehmbar an allen Zugängen zum überwachten Gelände anzubringen.

› Abschließend ist zu beachten, dass der mit der Videobeobachtung gegebenenfalls verfolgte Zweck, unmittelbar auf Vorfälle reagieren zu können, nur bei ständiger Beobachtung der Kameraaufnahmen gewährleistet ist.

Versteckte Kamera im Fahrstuhl eines Miethauses

Ein Petent zeigte an, dass seitens des Hauseigentümers Kameras im Erdgeschoss und Keller eines Miethauses installiert wurden. Nach einiger Zeit entdeckte er auch eine versteckte Kamera, die sich im Fahrstuhl des Gebäudes hinter einer Lampe befand.

Zwar handelt es sich beim Innenbereich eines Mietgebäudes in der Regel um nicht-öffentlich zugängliche Räume, mit der Folge, dass § 6b BDSG als Rechtsgrundlage mit seinen Voraussetzungen keine Anwendung findet. Befinden sich jedoch Einrichtungen wie Arztpraxen, Kanzleien oder Ähnliches mit offenem Publikumsverkehr im Gebäude, kann es sich hier zumindest während der Öffnungszeiten um einen öffentlich zugänglichen Raum handeln. Derartige Einrichtungen waren jedoch nicht vorhanden. Die Videoüberwachung ist allerdings nach § 28 BDSG zu beurteilen, wonach ähnlich Voraussetzungen gelten wie in den Fällen des § 6b BDSG.

Nach Maßgabe des § 28 Abs. 1 Abs. 1 Nr. 2 BDSG dürfen personenbezogenen Daten – hier: Bilddaten – zur Wahrnehmung berechtigter Interessen nur dann verarbeitet werden, soweit es erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen der betroffenen Personen am Ausschluss einer Videoüberwachung überwiegen.

Der verantwortliche Hauseigentümer wurde im Rahmen eines Auskunftsersuchens gem. § 38 Abs. 3 BDSG um Stellungnahme zum Sachverhalt aufgefordert. Dieser verwies auf eine beauftragte Hausverwaltung als Verantwortliche. Eine versteckte Kamera im Fahrstuhl war dieser nicht bekannt. Bei den übrigen Kameras handele es sich um Attrappen zu Abschreckungszwecken, da es bereits Manipulationsversuche am Fahrstuhl und verschiedene Vandalismusvorfälle gab.

Im nicht öffentlich zugänglichen Raum und insbesondere im Mietverhältnis ist zu berücksichtigen, dass die Privatsphäre der Mieter eine größere Bedeutung als im öffentlich zugänglichen Raum hat. Der Überwachungsdruck wird

hier stärker wahrgenommen und der Eingriff wiegt schwerer. Die personenscharfe Überwachung kann zulässig sein, wenn sichergestellt werden soll, dass Täter, die die Funktionsfähigkeit manipulieren, überführt werden. Dafür genügt allerdings eine Ausrichtung lediglich auf den Fahrstuhl. Die Überwachung sollte auch nur vorrübergehend erfolgen. Eine heimliche Videoüberwachung ist im Übrigen unzulässig.

Im konkreten Fall ist die Zulässigkeit der Attrappen zivilrechtlich zu beurteilen. So erweckt auch das Anbringen von Kameraattrappen bei Personen, die diese zur Kenntnis nehmen, regelmäßig den Eindruck, dass sie tatsächlich videoüberwacht werden. Da die fehlende Funktionsfähigkeit der Kamera von außen nicht erkennbar ist, - so sagt die Rechtsprechung (Landgericht Bonn, Urteil vom 16.11.2004- 8 S 139/04) – kann ein Überwachungsdruck hervorgerufen werden, der für betroffene Personen eine Beeinträchtigung des Persönlichkeitsrechts darstellen und möglicherweise zivilrechtliche Abwehransprüche auslösen kann. Diese könnten von betroffenen Personen im Klageweg durchgesetzt werden.

Die versteckte Kamera im Fahrstuhl wurde zwischenzeitlich entfernt. Der Verantwortliche, der die Kamera dort installierte, ist nicht bekannt.

Durchgangspassage als öffentlich zugänglicher Bereich

Durch eine Eingabe wurde der LfDI auf die Videoüberwachung einer Durchgangspassage aufmerksam. Dabei stellte sich die Frage, ob bei einer Durchgangspassage in einem Gebäude, die zwei Parallelstraßen miteinander verbindet, der § 6b BDSG, der die Beobachtung des öffentlich zugänglichen Bereichs regelt, überhaupt anwendbar ist. Dies zweifelte zumindest die vom Privateigentümer des Gebäudes beauftragte Hausverwaltung an, die mit zahlreichen Videokameras die Passage rundum überwachten. Es handele sich schließlich um ein Privatgrundstück.

Dass es sich bei der Passage um ein Privatgrundstück handelt, ist datenschutzrechtlich zunächst nicht von Belang. Bei dem Objekt handelt es sich um eine gemischt genutzte Einrichtung mit Gewerbeeinheiten. Die Durchgangspassage ist nicht baulich abgegrenzt und kann grundsätzlich von Jedermann betreten werden. Die im von Ihnen verwalteten Objekt vorhandenen Ladengeschäfte, Büros und in der Passage vorhandenen Schaufenster führen zu einem regen Publikumsverkehr. Es ist hier somit vielmehr davon auszugehen, dass die Passage betreten werden soll.

Zudem erreichen Anlieger ihre Wohneinheiten durch eine Eingangstür über die Passage. Ob der überwachte Bereich Privateigentum ist oder nicht, ist für die Bewertung, ob es sich um öffentlich zugänglichen Raum im datenschutzrechtlichen Sinne handelt, nicht erheblich. Relevant ist allein die durch den Berechtigten eröffnete tatsächliche Nutzungsmöglichkeit durch die Allgemeinheit, zumindest durch einen unbestimmten oder nur nach allgemeinen, von jedermann erfüllbaren Merkmalen bestimmten Personenkreis.

Die Durchgangspassage ist demnach als öffentlich zugänglicher Raum i.S.d. § 6b BDSG zu bewerten und nur im Rahmen dessen Voraussetzungen zulässig.

Als Anlass der Überwachung wurden regelmäßige Verunreinigungen der Passage sowie Einbruchversuche angeführt. Die Überwachung erfolge zum Zwecke der Abschreckung und der Vermeidung von Schäden. Es hat in diesem Zusammenhang eine Interessenabwägung mit Kunden, Passanten und Mietern zu erfolgen,

die von der Videoüberwachung betroffen sein könnten.

Aus datenschutzrechtlicher Sicht bestehen Bedenken im Hinblick auf die Verhältnismäßigkeit der dauerhaften Videoüberwachung der öffentlich zugänglichen Durchgangspassage. Im Rahmen der Erforderlichkeit ist zu prüfen, ob die genannten Zwecke durch kein anderes, ebenfalls geeignetes, aber weniger in das informationelle Selbstbestimmungsrecht der betroffenen Personen eingreifende Mittel erreicht werden können. Aus hiesiger Sicht kann eine Abschreckungswirkung beispielsweise auch mit dem Anbringen von Kameraattrappen erzielt werden, was sich als milderes Mittel erweisen würde. Der Zweckerreichung dienlich wäre auch die Beauftragung eines Wachdienstes oder eine generelle bauliche Zugangsbeschränkung, sodass nur ein bestimmter Personenkreis Zugang zum Objekt erhält.

In zeitlicher Hinsicht ist ein permanentes Anfertigen von Videoaufzeichnungen nicht verhältnismäßig. Insbesondere die permanente Überwachung während der üblichen Geschäftszeiten der vorhandenen Ladengeschäfte ist nicht durch § 6b Abs. 1 Nr. 3 BDSG gedeckt. Zu diesen Zeiten ist Personal zur Kontrolle der Durchgangspassage vorhanden. Auch eine Beschränkung der Beobachtung bzw. der Videoaufzeichnungen auf die Nachtzeiten wäre ein unverhältnismäßig starker Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Personen. Eine derartige Überwachung des sozialen Lebens besonders für die Mieter des Objekts kann nicht mit aufgetretenen Verschmutzungen gerechtfertigt werden. Insofern überwiegen die schutzwürdigen Interessen der Mieter, Passanten und Besucher als Betroffene.

Die Rundum-Überwachung wurde aufgrund der Anordnung des LfDI durch den Verantwortlichen eingestellt.

Videoüberwachung durch die allgemeinen Ordnungsbehörden

Städte und Gemeinden setzen immer häufiger Videoüberwachungstechniken ein, um öffentliche Einrichtungen zu schützen und Straßen und Plätze zu überwachen. Die Einsatzbereiche sind so vielfältig wie die technischen Möglichkeiten der Durchführung.

Auch eine Vielzahl von Volks- und Straßenfesten in Rheinland-Pfalz wird mittlerweile videoüberwacht.

Dabei ist der Zweck der Videoüberwachung in Form einer Live-Beobachtung in Echtzeit (Monitoring) oder mit einer Aufzeichnungsfunktion entscheidend für die Anordnungskompetenz der Videoüberwachung im öffentlichen Bereich. Der LfDI verzeichnete in der Vergangenheit vermehrt Anfragen von kommunalen Ordnungsbehörden, die zur Verhinderung von Straftaten und zur Strafverfolgung eine Videoüberwachung im Rahmen eines Umzugs oder eines Volksfestes beabsichtigten.

Für die Videoüberwachung öffentlich zugänglicher Räume ist dies vor allem § 34 Landesdatenschutzgesetz (LDSG). Für sonstige Bereiche kommen die §§ 12 bis 14 LDSG in Betracht. Die allgemeinen Ordnungsbehörden sind in bestimmten Fällen ebenfalls dazu befugt, diese Technik zur Überwachung öffentlich zugänglicher Räume einzusetzen (§ 27 Abs. 1 Polizei- und Ordnungsbehördengesetz (POG)), soweit dies im Einzelfall zur Erfüllung einer Aufgabe nach § 1 Abs. 1 Satz 1 und 3 und Abs. 2 und 5 POG erforderlich ist. Nach § 1 Abs. 1 Satz 1 POG haben die allgemeinen Ordnungsbehörden und die Polizei die Aufgabe, Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren. Soweit im Rahmen der Gefahrenabwehr auch Straftaten zu verhüten sind, stellt § 1 Abs. 1 Satz 3 POG klar, dass diese Aufgabe

ausschließlich der Polizei übertragen ist.

Nach § 27 Abs. 3 POG kann die Polizei an den in § 10 Abs. 1 Satz 2 Nr. 1 genannten Orten und in den in § 10 Abs. 1 Satz 2 Nr. 2 genannten Orten sowie in deren unmittelbarer Nähe personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen erheben, soweit Tatsachen die Annahme rechtfertigen, dass Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden.

Bei den in § 10 Abs. 1 Satz 2 Nr. 1 POG genannten Orten handelt es sich um sog. gefährliche Orte, von denen aufgrund tatsächlicher Anhaltspunkte insbesondere anzunehmen ist, dass Personen dort Straftaten verabreden, vorbereiten oder verüben. Orte im Sinne des § 10 Abs. 1 Satz 2 Nr. 2 POG sind sog. gefährdete Orte, d. h. Orte, bei denen Hinweise auf eine Gefährdung durch die Begehung oder Androhung von Straftaten vorliegen.

Während nach § 27 Abs. 1 Satz 2 Nr. 1 POG Videoaufzeichnungen nur zur Abwehr einer im Einzelfall bestehenden konkreten Gefahr zulässig sind, erlaubt § 27 Abs. 3 POG Videoaufzeichnungen bereits im Vorfeld konkreter Gefahren. Dem durch Videoaufzeichnungen berührten Grundrecht auf informationelle Selbstbestimmung wird nur dann hinreichend Rechnung getragen, wenn sich der Anwendungsbereich der Vorschrift auf „Kriminalitätsbrennpunkte“, also auf Orte, an denen sich die Kriminalitätsbelastung deutlich von der an anderen Orten abhebt, beschränkt. Ferner muss aufgrund konkreter Anhaltspunkte die Annahme gerechtfertigt sein, dass am fraglichen Ort in Zukunft weitere Straftaten begangen werden und dass die Videoüberwachung zu deren Bekämpfung erforderlich ist (vgl. VGH Baden-Württemberg, Urteil v. 21.07.2003, 1 S 377/02).

Nach § 27 Abs. 1 Satz 2 Nr. 1 POG können sowohl die Polizei als auch die allgemeinen Ordnungsbehörden im Rahmen ihrer Aufgabenerfüllung Videoaufzeichnungen zur Abwehr einer (konkreten) Gefahr anfertigen. Wie sich aus § 1 Abs. 1 Satz 3 POG ergibt, obliegt die Aufgabe der Straftatenverhütung ausschließlich der Polizei, wobei nicht nur Aufgaben gemeint sind, die auf unspezifische Kriminalitätsvorbeugung gerichtet sind, sondern ebenso auch die Verhinderung konkret drohender Delikte. Ist Ziel einer gefahrenabwehrrechtlichen Videoaufzeichnung die Verhütung drohender Straftaten, so ist allein die Polizei berechtigt, entsprechende Maßnahmen durchzuführen. Sie kann Videoaufzeichnungen entweder zur Abwehr einer konkret drohenden Straftat auf § 27 Abs. 1 Satz 2 Nr. 1 POG oder aber im Vorfeld konkreter Gefahren an Kriminalitätsbrennpunkten auf § 27 Abs. 3 POG stützen. Den allgemeinen Ordnungsbehörden verbleibt eine Befugnis zur Videoaufzeichnung nur dann, wenn es um die Abwehr sonstiger, also nicht in der Begehung von Straftaten bestehender (konkreter) Gefahrenlagen geht. Dies wäre der Fall, wenn es um die Abwehr von Gefahren geht, die in der Begehung von Ordnungswidrigkeiten bestehen.

Vor diesem Hintergrund hat der LfDI im Rahmen seiner datenschutzrechtlichen Prüfung entsprechende Anfragen von allgemeinen Ordnungsbehörden in Dahn und Kaiserslautern mit Hinweis auf den angegebenen Zweck der Videoüberwachung als unzulässig angesehen und auf mildere Mittel verwiesen.

5. GESUNDHEIT

5.1 Digitalisierung im Gesundheitswesen

5.1.1 Ausgangslage

Mit der Digitalisierung im Gesundheitswesen kommt eine durchgreifende Veränderung der bisherigen Arbeitsprozesse im Gesundheitsbereich in Gang, die vielfältige Chancen für eine bessere und nachhaltigere medizinische Versorgung der Menschen birgt (vgl. bereits 24. Tb., Tz. III.5.2.1 zu intelligenten Assistenzsystemen und 25. Tb., Tz. III.5.4 zur Telematik im Gesundheitswesen). Insbesondere können Versorgungswege effizienter, schneller und kostengünstiger gestaltet und fachlich unterstützt werden. Auch ist zu vermuten, dass der Einsatz von Big Data für die biomedizinische und pharmazeutische Forschung einschließlich der Entwicklung neuartiger und verbesserter Behandlungsmethoden ein enormes Potential enthält. Auf Seiten der Patientinnen und Patienten besteht mit der zunehmenden Digitalisierung des Gesundheitswesens die Gelegenheit, stärker in die eigene Behandlung eingebunden zu werden und sich zugleich mit der wachsenden Verfügbarkeit von Informationen auch aktiver an dem Genesungsprozess zu beteiligen. Im Idealfalle können somit alle Akteure im Gesundheitswesen von der Digitalisierung profitieren: Leistungserbringer, Kostenträger, Patientinnen und Patienten, Gesundheitswirtschaft und die medizinische Forschung.

Diesen Chancen stehen aus der Sicht des Datenschutzes diverse Risiken gegenüber. So besteht mit der zunehmenden technologischen Vernetzung die Gefahr, dass die Vertraulichkeit der Heilbehandlung nicht länger garantiert werden kann. Sicherheitslücken der eingesetzten Technik, aber auch Bedienungsfehler der Anwender können gravierende Auswirkungen für den Einzelnen oder die Funktionsfähigkeit ganzer Einrichtungen haben. Neben datenschutzrechtlichen stellen sich auch ethische Fragen, wenn sich medizinische Behandlungen künftig im Wesentlichen auf die Auswertung gesammelter Messwerte und abstrakter Standards reduzieren, ohne das Individuum noch gebührend in den Blick zu nehmen. Ohnehin wird das Risiko der Bildung von Persönlichkeitsprofilen mit der Nutzung digitaler Technik auch im Gesundheitsbereich deutlich ansteigen. Aufgrund der hohen wirtschaftlichen Bedeutung von Gesundheitsdaten insbesondere für Industrie und Forschung besteht zudem die Gefahr, dass künftig verstärkt solche Informationen ohne Wissen der Betroffenen und Ärztinnen und Ärzte abgesaugt und möglicherweise durch Dritte verwertet werden. Das Risiko hierfür tragen bislang die Betroffenen selbst, da sie mit ihrer Einwilligung den Einsatz telematischer Anwendungen legitimieren, ohne die daraus resultierenden Gefährdungen erkennen zu können. Gleichwohl bleibt den Patientinnen und Patienten keine andere Wahl, es sei denn, sie verzichten auf die mit den Anwendungen erhofften gesundheitlichen Vorteile. Schließlich ist zu befürchten, dass mit einer zunehmenden Verfügbarkeit digitaler Gesundheitsdaten die Gemeinschaft der Krankenversicherten entsolidarisiert und Gesundheit als wirtschaftlich verwertbares Gut – wie z.B. durch bessere Vertragskonditionen – belohnt, kranke Menschen dagegen als reiner Kostenfaktor diskriminiert werden. Auch auf dem Arbeitsmarkt könnten vergleichbare Entwicklungen drohen.

5.1.2 Forderungen aus der Sicht des Datenschutzes

Im April 2016 verabschiedete die 91. Datenschutzkonferenz auf ihrer Sitzung in Schwerin eine Entschließung zum effektiven Schutz

sensibler Gesundheitsdaten in Wearables und Gesundheits-Apps https://s.rlp.de/dsk042016. In dem Papier werden die hierbei aus Datenschutzsicht bestehenden grundlegenden Aspekte zusammengefasst und zugleich der Gesetzgeber aufgefordert, ein Tätigwerden zu prüfen. Geboten ist nach Auffassung der Datenschutzkonferenz insbesondere die Entwicklung datenschutzfreundlicher Technologien (privacy by design/privacy by default). Mit der Nutzung von Wearables und Gesundheits-Apps zusammenhängende Datenweitergaben an Dritte sollten für die Betroffenen sofort erkennbar sein und klaren rechtlichen Vorgaben unterworfen werden. Die Einwilligung wird nur dann als tragfähige Legitimation einer Datenverarbeitung anerkannt, wenn sie freiwillig ist und nicht auf einem erheblichen Verhandlungsungleichgewicht basiert. Verbindliche gesetzliche Standards zur Datensicherheit können nicht durch Einwilligungen abbedungen werden. Schließlich verweist die Datenschutzkonferenz auf eine Mitverantwortlichkeit der Vertreiber von Wearables und Gesundheits-Apps für deren datenschutzkonforme Ausgestaltung.

Die in der Entschließung der 91. Datenschutzkonferenz zunächst für den Einsatz von Wearables und Gesundheits-Apps formulierten Anforderungen gelten im Wesentlichen für alle Bereiche des Gesundheitswesens, die von der Digitalisierung erfasst werden. Teilweise kann dabei eine Differenzierung zwischen den jeweiligen Nutzungszwecken digitaler Produkte sinnvoll sein. So stehen z.B. bei Anwendungen im sog. Lifestyle-Bereich zumindest auch die Verbraucherinnen und Verbraucher selbst in der Verantwortung, durch eigene Aufklärung und den Verzicht auf unsichere oder intransparente Produkte zum Schutz ihrer Gesundheitsdaten beizutragen. Dies ist bei einem Einsatz digitaler Anwendungen z.B. im Rahmen einer medizinischen Behandlung anders: hier müssen die Patientinnen und Patienten darauf vertrauen können, dass die eingesetzten Geräte und Anwendungen einem definierten Datenschutz- und Datensicherheitsstandard entsprechen. Denn im Zweifel würden sie zugunsten ihrer Genesung auch Einbußen an dem Schutzniveau der sie betreffenden Daten hinnehmen.Dies darf jedoch nicht ausgenutzt werden. Dementsprechend sollte der professionelle Einsatz digitaler Technik rechtlichen Vorgaben (z.B. im Berufsrecht oder im Medizinprodukterecht) unterliegen, die zwingend die Einhaltung eines datenschutzrechtlichen Qualitätsstandards verlangen.

Darüber hinaus muss die Frage der datenschutzrechtlichen Verantwortlichkeit für den Einsatz digitaler Anwendungen im Gesundheitsbereich geklärt werden. Dies ist sowohl für die Umsetzung der beschriebenen Vorgaben als auch für die Wahrnehmung der Betroffenenrechte elementar. In Betracht kommen je nach Einsatzszenario Hersteller, Anbieter, Vertreiber der einzelnen Produkte, Mediziner und Krankenversicherungen. Die Europäische Datenschutz-Grundverordnung bietet mit dem neuen Instrument der gemeinsamen Verantwortlichkeit nach Art. 26 nunmehr eine gute Möglichkeit, die gerade mit der Digitalisierung im Gesundheitswesen einhergehenden Kooperationen und differenzierten Rollenzuordnungen datenschutzrechtlich passend abzubilden.

Abgesehen von dem Ende 2015 verabschiedeten E-Health-Gesetz, das im Wesentlichen den Ausbau der Elektronischen Gesundheitskarte vorantreiben wollte, fehlt es bislang an einem klaren gesetzgeberischen Signal, obwohl die Thematik nicht nur von den staatlichen Datenschutzbeauftragten, sondern auch seitens der Verbraucherschutzministerkonferenz aufgegriffen wurde (vgl. Beschluss zu TOP 34/35 der 13. VMK vom 28.04.2017 https://www.verbraucherschutzministerkonferenz.de/Beschluesse.

html). Die Datenschutzkonferenz hat daher im November 2017 in ihrem grundlegenden Forderungskatalog (https://s.rlp.de/entschliessungdsk1120172) für die neue Legislaturperiode auf Bundesebene verlangt, bei der Digitalisierung des Gesundheitswesens generell das Recht auf Schutz personenbezogener Daten der Patientinnen und Patienten und Versicherten gesetzlich wirksam zu sichern. Dabei müsse das Vertrauensverhältnis zwischen Patientinnen und Patienten und ihren Behandelnden effektiv geschützt werden. Unentbehrlich sei deshalb, vor der Nutzung neuer technischer Anwendungen im Gesundheitsbereich einen Datenschutz- und Datensicherheitsstandard festzulegen, der den Anforderungen der im Mai 2018 wirksam werdenden Europäischen Datenschutz-Grundverordnung genügt. Zugleich müsse sichergestellt werden, dass die Ausgestaltung der im Gesundheitswesen verwendeten telematischen Anwendungen auch tatsächlich diesen Standards entspreche. Im Zusammenhang mit dem Einsatz sog. Big-Data-Anwendungen fordert die Datenschutzkonferenz spezielle rechtliche Regelungen, die eine Reidentifizierung und unerlaubte Zusammenführung von Daten, das Anlegen von Datenprofilen zu einer Person sowie den Handel mit Gesundheitsdaten verbieten und unter Strafe stellen. Schließlich fordert die Datenschutzkonferenz, zumindest bei dem Einsatz neuer technischer Anwendungen in der Regelversorgung für eine angemessene Transparenz aus Nutzersicht zu sorgen.

Im weiteren Prozess der Digitalisierung hält der LfDI ein aktives und strukturiertes Vorgehen der Datenschutzbeauftragten für geboten. Dabei lassen sich konkrete Handlungsfelder identifizieren:

› Sichtung der datenschutzrelevanten Anwendungsszenarien bei der Digitalisierung im Gesundheitsbereich (z.B. Gesundheits-Apps, Telemedizinische Fachanwendungen, Cloud Computing, Elektronische Patientenakte, intelligente Assistenzsysteme (AAL), Big Data)

› Festlegung der aus Datenschutzsicht gebotenen rechtlichen und technischen Standards (z.B. Klärung der datenschutzrechtlichen Verantwortlichkeit, Präzisierung von privacy by design und privacy by default im konkreten Anwendungszusammenhang)

› Schaffung des zum Schutz von Patientendaten erforderlichen rechtlichen Rahmens (z.B. im Berufsrecht, im Medizinprodukterecht, im Zivilrecht)

› Bildung und Sensibilisierung aller Akteure im Umgang mit digitaler Technik (z.B. Vermittlung von Medienkompetenz, Datenschutzschulung)

› Bereitstellung praktischer Hilfen für die Anwendenden zur Verbesserung von Transparenz (z.B. Gütesiegel, Zertifizierung)

Da im Zusammenhang mit der Digitalisierung des Gesundheitswesens nicht nur Aspekte des Datenschutzes, sondern u.a. auch verbraucherschutzrechtliche und fachliche Belange betroffen sind, sollte eine erfolgreiche E-Health-Strategie auf das interdisziplinäre Zusammenwirken aller hiervon betroffenen Akteure ausgerichtet sein.

5.1.3. Aktivitäten

Auf Initiative des LfDI hat sich im Dezember 2017 eine Arbeitsgruppe des Arbeitskreises Gesundheit und Soziales der Datenschutzkonferenz zur Digitalisierung im Gesundheitswesen konstituiert. Ziel ist es, unter Federführung der BfDI eine gemeinsame Strategie der staatlichen Datenschutzaufsichtsbehörden im Umgang mit den vielfältigen Digitalisierungslö-

sungen im Gesundheitsbereich zu entwickeln. Zugleich sollen sowohl konkrete Anforderungen zur Sicherstellung des Datenschutzes in den verschiedenen Anwendungsszenarien sowie praxisorientierte Lösungsvorschläge formuliert werden.

Auf Landesebene hat der LfDI im Jahr 2017 mit zwei Veranstaltungen zur Digitalisierung im Gesundheitswesen (https://s.rlp.de/digitalisierunggesundheit) dazu beigetragen, die öffentliche Aufmerksamkeit auf die Thematik zu richten. Mit der Teilnahme an dem von der Landesregierung im September 2017 initiierten „Runden Tisch E-Health" werden die Anliegen des Datenschutzes zugleich in die Gesamtstrategie des Landes zur Begleitung und Gestaltung des Digitalisierungsprozesses eingebracht. Zusammen mit der Verbraucherzentrale Rheinland-Pfalz und Vertretern der Ärzteschaft wird der LfDI schließlich versuchen, konkrete Maßnahmen wie beispielsweise die Entwicklung tragfähiger Konzepte für Gütesiegel bei Gesundheits-Apps oder die Bereitstellung datenschutzgerechter Messengerdienste für den ärztlichen Alltag anzustoßen. Schließlich beteiligte sich der LfDI im Dezember 2017 zum ersten Mal an der Ausbildung von Medizinerinnen und Medizinern im Zusammenhang mit dem an der Universitätsmedizin Mainz entwickelten „Curriculum 4.0 Medizin im digitalen Zeitalter". Das bundesweit vielbeachtete und ausgezeichnete Projekt hat das Ziel, künftigen Ärztinnen und Ärzten die für einen Einsatz der neuen Kommunikations- und Kooperationsformen notwendigen zusätzlichen Kompetenzen und Qualifikationen zu vermitteln. Diesen Ansatz unterstützt der LfDI ausdrücklich. Denn für einen angemessenen Schutz von Patientendaten spielen auch im digitalen Zeitalter die Ärztinnen und Ärzte eine entscheidende Rolle.

5.1.4 Ausblick

Mit der Ende 2017 veröffentlichten Stellungnahme des Deutschen Ethikrats zum Thema „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung" (https://s.rlp.de/bigdatagesundheit) wird letztendlich eine gesamtgesellschaftliche Auseinandersetzung mit der Digitalisierung im Gesundheitswesen gefordert. Es bleibt zu hoffen, dass diese stattfindet und zu konstruktiven und einvernehmlichen Ergebnissen führt. Ob und ggf. in welcher Weise dabei das Datenschutzrecht weiterentwickelt oder neu gestaltet werden muss, wird sich zeigen. Der LfDI ist bereit, sich an dem Prozess einer gemeinsamen Konzeption von Big Data und darüber hinaus zu beteiligen.

5.2 Fragebogen zur Schuleingangsuntersuchung

In Rheinland-Pfalz wie in anderen Bundesländern müssen sich Kinder, die zur Einschulung angemeldet werden, einer amtsärztlichen Untersuchung unterziehen. Dies ist gesetzlich so vorgesehen. Mit der sog. „Schuleingangsuntersuchung" soll der individuelle Entwicklungsstand des Kindes und ein möglicher Förderbedarf im Vorfeld der Einschulung festgestellt werden. Die Eltern haben aufgrund der Teilnahmepflicht keine Möglichkeit, sich der Untersuchung durch das Gesundheitsamt zu entziehen. Es ist das einzige Mal, dass eine homogene Altersgruppe aus der Bevölkerung vollständig ärztlich begutachtet und deren Gesundheitszustand festgestellt wird. Demzufolge sollen die aus den Untersuchungen gewonnenen Erkenntnisse auch für den Zweck der Gesundheitsberichterstattung genutzt werden.

Zur Vorbereitung der Schuleingangsuntersuchung versenden die Gesundheitsämter im

Vorfeld Fragebögen an die Eltern, in denen Angaben zur Anamnese des Kindes, aber auch zur Lebenssituation und dem häuslichen Umfeld erhoben werden. Soweit die Fragen der amtsärztlichen Begutachtung des Kindes dienen, besteht eine gesetzliche Antwortpflicht, bei allen anderen Fragen ist die Beantwortung den Eltern freigestellt. Hierauf wird in dem seitens des Landes entwickelten und den Kommunen zur Verfügung gestellten Musterfragebogen, der inhaltlich mit dem LfDI abgestimmt wurde, ausdrücklich hingewiesen.

Im Berichtszeitraum erfuhr der LfDI, dass ein rheinland-pfälzisches Gesundheitsamt einen gegenüber dem Mustervordruck um drei Fragen ausgeweiteten Fragebogen an ca. 1.500 Eltern künftiger Grundschülerinnen und -schüler versandt hatte. Darin wurden die Sorgeberechtigten ergänzend um Angaben zum Medienkonsum und zum Freizeitverhalten der Kinder und zur telefonischen Erreichbarkeit der Eltern gebeten. In dem Begleitschreiben wurde der Eindruck erweckt, dass auch diese Fragen verpflichtend zu beantworten seien. Auf Bitten von Eltern prüfte der LfDI die datenschutzrechtliche Zulässigkeit des Vordrucks.

Das Vorgehen des Gesundheitsamtes war im Ergebnis nicht von den Vorgaben des Datenschutzes gedeckt. So bestand entgegen der in dem Fragebogen und dem dazu versandten Anschreiben enthaltenen Aussagen eindeutig keine rechtliche Verpflichtung der Eltern, auf die ergänzend aufgenommenen Fragen zu antworten. Informationen zu deren Verwendungszweck fehlten völlig. Mit der Verwendung des Landeswappens auf dem Vordruck war zudem nicht erkennbar, dass der ursprüngliche seitens des Landes erarbeitete Musterfragebogen durch die Kreisverwaltung abgeändert wurde. In Gesprächen mit der Kreisverwaltung stellte sich zudem heraus, dass das Gesundheitsamt den behördlichen Datenschutzbeauftragten bei der Ergänzung des Vordrucks nicht eingebunden hatte.

In Abstimmung mit dem für die Durchführung der Schuleingangsuntersuchungen federführenden Fachministerium hat der LfDI mit der betroffenen Kreisverwaltung Kontakt aufgenommen und um Klärung gebeten. Die Kreisverwaltung räumte ihr Versäumnis ein und unterband den weiteren Einsatz der Fragebögen. Eine Neufassung des Vordrucks für künftige Schuleingangsuntersuchungen soll unter Hinzuziehung des behördlichen Datenschutzbeauftragten und des LfDI zeitnah erfolgen.

6. SOZIALES

6.1 Kompliziert, aber machbar: Datenschutzkonformes Vorgehen des Jugendamtes bei einem Verdacht auf Kindeswohlgefährdung

Mit der Frage, wie die datenschutzrechtlichen Vorgaben im Bereich der öffentlichen Jugendhilfe im Behördenalltag eingehalten werden können, wird der LfDI seit Jahren konfrontiert. Viele Sachverhalte erreichen den ihn durch Eingaben betroffener Bürgerinnen und Bürger. Dabei stellt sich immer wieder heraus, dass die Beachtung des informationellen Selbstbestimmungsrechts durch Jugendämter in der Praxis in jedem Einzelfall eine Herausforderung zu sein scheint, die bedauerlicherweise nicht immer gelingt. In einem besonders eklatanten Fall kam es im Berichtszeitraum nun sogar zu einer förmlichen Beanstandung.

In dem zugrunde liegenden Sachverhalt war eine vierköpfige Familie Gegenstand einer anonymen Anzeige. Darin wurde vorgetragen, dass in der Familie ein Drogen- und Alkoholproblem bestehen würde, das sich auch auf die dortigen Kinder auswirke. Dem Jugendamt war die Familie bislang nicht bekannt. Insbesondere fehlten Erkenntnisse, die auf eine Gefährdung der Kinder oder ein bestehendes Aggressionspotential der Eltern hindeuteten. Dennoch wandte sich das Jugendamt aufgrund des Hinweises sofort an eine Kindertagesstätte und diverse Grundschulen im Umkreis des Wohnortes der Familie, ohne zuvor mit den Betroffenen direkt Kontakt aufzunehmen. Zumindest gegenüber der Kindertagesstätte wurde der vollständige Inhalt der anonymen Anzeige offenbart.

Datenschutzrechtlich warf das Vorgehen des Jugendamtes einige Fragen auf. Bedenken bestanden sowohl hinsichtlich der unterbliebenen Kontaktaufnahme mit der Familie als auch in Bezug auf die sofortige Recherche bei der Kindertagesstätte und den Schulen und der damit einhergehenden Übermittlung der Verdachtsinhalte. Maßgeblich für die Klärung der datenschutzrechtlichen Zulässigkeit sind die Regelungen des Sozialgesetzbuchs zur Datenverarbeitung im Zusammenhang mit einer befürchteten Kindeswohlgefährdung, insbesondere § 8a SGB VIII.

§ 8a Abs. 1 SGB VIII

(1) Werden dem Jugendamt gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so hat es das Gefährdungsrisiko im Zusammenwirken mehrerer Fachkräfte einzuschätzen. Soweit der wirksame Schutz dieses Kindes oder dieses Jugendlichen nicht in Frage gestellt wird, hat das Jugendamt die Erziehungsberechtigten sowie das Kind oder den Jugendlichen in die Gefährdungseinschätzung einzubeziehen und, sofern dies nach fachlicher Einschätzung erforderlich ist, sich dabei einen unmittelbaren Eindruck von dem Kind und von seiner persönlichen Umgebung zu verschaffen. Hält das Jugendamt zur Abwendung der Gefährdung die Gewährung von Hilfen für geeignet und notwendig, so hat es diese den Erziehungsberechtigten anzubieten.

Eine Erhebung von Sozialdaten ohne Einbeziehung der Erziehungsberechtigten ist nur zulässig, wenn konkrete Anhaltspunkte dafür vorliegen, dass eine unmittelbare Kontaktaufnahme des Jugendamtes mit den Eltern zum Zwecke der Gefährdungseinschätzung den wirksamen Schutz des Kindes in Frage stellen würde und die zu erhebenden Daten der Erfüllung des Schutzauftrags nach § 8a SGB VIII dienen (vgl. § 62 Abs. 3 Nr. 2d SGB VIII i.V.m. § 8a Abs. 1 Satz 2 SGB VIII).

Im konkreten Fall lagen diese Voraussetzungen nicht vor: Entgegen der Auffassung des Jugendamtes war aufgrund der bislang fehlenden Erkenntnisse über die Familie nicht zu befürchten, dass eine Kontaktaufnahme mit den Eltern den Schutz der Kinder gefährden würde. Nach dem heranzuziehenden materiellen Recht darf die Tatsache, dass dem Jugendamt keine Informationen zu der Familie vorlagen, nicht zu deren Nachteil verwendet werden. Denn es ist durchaus üblich und kein Indiz drohender Kindeswohlgefährdungen, dass nicht alle in einem Zuständigkeitsbereich eines Jugendamtes ansässigen Familien diesem bekannt sind.

Es war deshalb rechtlich fehlerhaft, wegen nicht vorhandener Erkenntnisse über die betroffene Familie auf den in § 8a Abs. 1 Satz 2 SGB VIII geforderten direkten Kontakt mit den Erziehungsberechtigten zur Gefährdungseinschätzung zu verzichten. Damit verletzte das Jugendamt den gesetzlich verlangten Schutz der von einer Anzeige wegen drohender Kindeswohlgefährdung betroffenen Sorgeberechtigten.

Mit dem in § 8a Abs. 1 SGB VIII vorgesehenen abgestuften Vorgehen hat der Gesetzgeber einen Ausgleich zwischen den bei einer drohenden Kindeswohlgefährdung widerstreitenden Interessen des betroffenen Kindes (Schutz vor drohender Gefährdung) und der Eltern bzw. Sorgeberechtigten (Schutz vor falschen Verdächtigungen und damit einhergehender Stigmatisierung) gefunden, der ausnahmslos von den Jugendämtern beachtet werden muss. Der Versuchung, zum Schutz von Kindern letztendlich alles tun und insbesondere sich über gesetzliche Vorgaben und Rechte Betroffener hinwegsetzen zu dürfen, muss klar und konsequent widerstanden werden.

Der LfDI hat das Vorgehen des Jugendamtes aufgrund der klaren rechtlichen Vorgaben, die missachtet wurden, und der für die Betroffenen damit verbundenen stigmatisierenden Auswirkungen formell beanstandet. Zugleich wurde die Kreisverwaltung gebeten, künftig ein datenschutzkonformes Vorgehen des Jugendamtes bei der Aufklärung von Anzeigen über drohende Kindeswohlgefährdungen sicherzustellen.

6.2 Bereitstellung von Jugendamtsakten für eine Organisationsuntersuchung durch ein privates Wirtschaftsunternehmen

Die geplante Organisationsuntersuchung in einem rheinland-pfälzischen Jugendamt durch ein privates Wirtschaftsunternehmen warf die Frage auf, ob und ggf. in welchem Umfang Fallakten mit personenbezogenen Inhalten den Prüfern zur Verfügung gestellt werden dürfen.

Zur datenschutzrechtlichen Zulässigkeit der Bereitstellung von Akten eines Jugendamtes zum Zwecke der Rechnungsprüfung hat sich der LfDI in der Vergangenheit wiederholt geäußert (vgl. 17. Tb., Tz. 11.3.1). Dabei wurde die Auffassung vertreten, dass der Gesetzgeber nach den Regelungen der §§ 35 Abs. 1 Satz 4 SGB I, 67c Abs. 3 Satz 1 und 69 Abs. 5 SGB X eine Übermittlung von Sozialdaten an die Rechnungsprüfungsbehörden (insbesondere Rechnungsprüfungsamt, Landesrechnungshof) zur Überprüfung der Wirtschaftlichkeit der Sozialverwaltung grundsätzlich für zulässig erachtet, soweit die in den Akten enthaltenen Daten für eine konkrete Prüfung erforderlich sind. Dies gilt angesichts § 61 Abs. 1 SGB VIII auch für den Bereich der öffentlichen Jugendhilfe. Lediglich die Übermittlung anvertrauter Daten im Sinne von § 65 SGB VIII unterliegt besonderen Anforderungen und ist nur ausnahmsweise zulässig.

Vor diesem gesetzlichen Hintergrund kommt im Rahmen von Organisationsuntersuchungen im Bereich der öffentlichen Jugendhilfe die Bereitstellung von Sozialdaten für private Stellen eher nicht in Betracht. Zwar können auch private Stellen zur Durchführung einer der Aufgaben nach § 67c Abs. 3 Satz 1 SGB X beauftragt werden. Allerdings lässt § 69 Abs. 5 SGB X eine Datenübermittlung nur zu, wenn sie für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe und der anderen Stellen, auf die § 67c Abs. 3 Satz 1 SGB X Anwendung findet, erforderlich ist. Voraussetzung ist somit, dass die Bereitstellung der Sozialdaten für die Erfüllung einer gesetzlichen Aufgabe des Empfängers erfolgt. Dies ist jedoch nicht der Fall, wenn private Unternehmen mit der Durchführung von Organisationsuntersuchungen im Jugendamt beauftragt werden. Dementsprechend wäre es datenschutzrechtlich nicht zulässig, den externen Prüfern vollständige Fallakten des Jugendamtes zu überlassen. Neben der Option einer individuell erteilten Einwilligung durch die Betroffenen selbst, die allerdings wenig praktikabel erscheint und darüber hinaus im Bereich der Jugendhilfe zumindest Fragen nach der Wirksamkeit einer derartigen Einwilligung aufwirft, kommt im Falle von Organisationsuntersuchungen durch private Stellen daher vorrangig die Bereitstellung anonymisierter Akten in Betracht.

6.3 Speicherung von Kontoauszügen bei der Beantragung von Sozialleistungen

Die datenschutzrechtliche Zulässigkeit der Vorlage von Kontoauszügen im Zusammenhang mit der Beantragung von Sozialleistungen, insbesondere der Grundsicherung für Arbeitsuchende, hat in der Vergangenheit den LfDI immer wieder beschäftigt. Sowohl bei der Gewährung von Grundsicherungsleistungen nach dem Sozialgesetzbuch II als auch von Sozialhilfeleistungen nach dem Sozialgesetzbuch XII verlangen die Leistungsträger von den Antragstellenden die Vorlage von Kontoauszügen zum Nachweis der individuellen Hilfebedürftigkeit. Diese auf die Mitwirkungspflichten der Leistungsempfänger gestützte Anforderung erfolgt sowohl bei der erstmaligen Antragstellung als auch bei Folgeanträgen.

Nach der Rechtsprechung des Bundessozialgerichts (Urteil vom 19. September 2008, Az. B 14 AS 45/07 R) ist das Vorlageverlangen als Datenerhebung zulässig, soweit von den Antragstellenden die Kontoauszüge der letzten drei Monate vor Antragstellung erbeten werden. Dies gilt sowohl für den Erst- als auch für weitere Folgeanträge. Bislang nicht von der Rechtsprechung des Bundessozialgerichts erfasst ist dagegen die Frage, ob und ggf. wie lange die Leistungsträger befugt sind, die ihnen vorgelegten Kontoauszüge zu speichern. Im Berichtszeitraum wandten sich wiederholt Betroffene an den LfDI und baten um Klärung dieser Frage, da nach ihrer Erfahrung rheinland-pfälzische Sozialbehörden verbreitet die vorgelegten Auszüge dauerhaft in ihren Leistungsakten aufbewahrten, obwohl der LfDI dies bislang, soweit keine Abweichungen von den ursprünglichen Antragsangaben ersichtlich waren, als datenschutzrechtlich bedenklich bewertet hatte.

Im Rahmen der Sachaufklärung bestätigte sich der Eindruck, dass die Leistungsträger trotz der eindeutigen Handlungsempfehlung des LfDI die Kontoauszüge auch in Fällen ohne weitere Auffälligkeiten nicht nur vorübergehend, sondern dauerhaft zu ihren Akten nahmen. Grund hierfür waren die in diesem Zusammenhang von Seiten des Landesrechnungshofs angeführten Belange der Rechnungsprüfung. Gegenüber dem LfDI bestätigte der Landesrechnungshof diese Bewertung. Der entscheidungserhebliche Sachverhalt sei zumindest im Hinblick auf

den Erstantrag nur mithilfe der vorgelegten Kontoauszüge nachvollziehbar und damit für die Rechnungsprüfung vollständig dokumentiert.

Zur Vermeidung gegensätzlicher Handlungsvorgaben und im Interesse der betroffenen Sozialverwaltungen hat der LfDI seine früheren Bedenken gegen eine dauerhafte Speicherung der im Rahmen eines Erstantrags vorgelegten Kontoauszüge zurückgestellt und toleriert künftig deren Aufnahme in die Leistungsakte. Demgegenüber hält er in Bezug auf Folgeanträge an seiner bisherigen Rechtsauffassung fest. Die routinemäßige Speicherung der vorgelegten Auszugskopien in den Leistungsakten begegnet in diesen Fällen auch weiterhin datenschutzrechtlichen Bedenken, sofern nicht im Einzelfall die Speicherung z.B. wegen bestehender Unstimmigkeiten mit den bisherigen Antragsangaben sachlich begründet ist.

Unabhängig davon sind in jedem Fall die Leistungsträger verpflichtet, alle vorhandenen Spielräume des technisch-organisatorischen Datenschutzes bei der Speicherung der Kontoauszüge auszuschöpfen. Hierzu gehören beispielsweise eingeschränkte Zugangsmöglichkeiten zu den vorgehaltenen Auszugskopien sowie die Verankerung moderater Speicherfristen. Es empfiehlt sich deshalb, zur Festlegung einer datenschutzkonformen Vorgehensweise die Datenschutzbeauftragten vor Ort einzubinden.

6.4 Mitgliederwerbung in der Gesetzlichen Krankenversicherung

Die Gratwanderung zwischen noch rechtlich zugelassener Werbung um neue Mitglieder und der Verletzung des informationellen Selbstbestimmungsrechts ist im Bereich der Gesetzlichen Krankenversicherungen für die Akteure seit je her eine Herausforderung, die leider nicht immer gelingt. Dies ist umso erstaunlicher, da es klare datenschutzrechtliche Vorgaben zum Umgang mit personenbezogenen Daten zum Zwecke der Mitgliederwerbung gibt und die Aufsichtsbehörden wiederholt und seit langem auf die Grenzen des Zulässigen hinweisen (vgl. u.a. 25. Tb., Tz. III.6.1.1; 36. Tb. der LfD Bremen, Tz. 7.3; 22. Tb. des LfD Bayern, Tz. 14.1.4).

Im Berichtszeitraum wurde dem LfDI erneut ein Fall der unzulässigen Datenverarbeitung einer Krankenversicherung zum Zwecke der Mitgliederwerbung zugetragen, der zu einer formellen Beanstandung führte. Es lag folgender Sachverhalt zugrunde:

Ausgangspunkt war die seitens einer gesetzlichen Krankenkasse im Jahre 2017 geplante Erhöhung des kassenindividuellen Zusatzbeitrags. In einem persönlich adressierten und postalisch versendeten Informationsschreiben unterrichtete die Krankenkasse damals ihre Mitglieder über die beabsichtigte Beitragserhöhung. Nach dem Erhalt des Schreibens suchte ein bei der Krankenkasse Versicherter das Kundencenter einer anderen Krankenversicherung auf, um sich über die dortigen Versicherungsleistungen und Beitragskonditionen beraten zu lassen. Das von ihm in diesem Zusammenhang vorgezeigte Informationsschreiben seiner Krankenkasse, das u.a. den Namen des Versicherten und seine Anschrift sowie Angaben zur Identität und Erreichbarkeit des Kundenberaters enthielt, wurde mit seiner formlos und ohne weitere Zweckbestimmung eingeholten Einwilligung vor Ort kopiert. Das Kundencenter leitete die angefertigte Kopie ungeschwärzt im Rahmen der Marktbeobachtung an die Direktion der Krankenversicherung weiter. Der mittlerweile mit der Angelegenheit befasste Vertriebsbereich der Versicherung informierte nun per E-Mail individuell diverse Arbeitgeber über

die geplante Erhöhung des Zusatzbeitrags bei dem Konkurrenzunternehmen und die im Falle eines Kassenwechsels zu erwartende Ersparnis für Neukunden ab einem bestimmten Durchschnittseinkommen. Der E-Mail war als Anhang die in dem Beratungsgespräch erstellte Kopie mit den darin enthaltenen persönlichen Daten zu dem Versicherten und dessen Kundenbetreuer beigefügt. Ein aufmerksamer Arbeitgeber, der von der Krankenversicherung kontaktiert worden war, bat den LfDI um Klärung der Zulässigkeit dieses Vorgehens.

Im Ergebnis qualifizierte der LfDI das Vorgehen der Krankenversicherung als Verstoß gegen datenschutzrechtliche Vorgaben. Weder die mit der Anfertigung einer Kopie des personalisierten Informationsschreibens verbundene Erhebung noch die mit der Versendung der Kopie an einzelne Arbeitgeber einhergehende Übermittlung von Sozialdaten waren von den Regelungen des Sozialdatenschutzes gedeckt:

§ 284 Abs. 4 SGB V bestimmt den Rahmen der zum Zwecke der Mitgliederwerbung durch Krankenkassen zulässigen Datenerhebung. Diese ist hiernach nur zulässig, wenn die Daten allgemein zugänglich sind oder sich eine Erhebungsbefugnis aus § 67a SGB X ergibt.

Die für Gesetzliche Krankenversicherungen im Zusammenhang mit der Mitgliederwerbung zu beachtende datenschutzrechtliche Regelung des § 284 Abs. 4 SGB V lautet:

(4) Zur Gewinnung von Mitgliedern dürfen die Krankenkassen Daten erheben, verarbeiten und nutzen, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. (…) Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten, ist sie unzulässig. Die Daten sind zu löschen, sobald sie für die Zwecke nach Satz 1 nicht mehr benötigt werden. Im Übrigen gelten für die Datenerhebung, Verarbeitung und Nutzung die Vorschriften des Ersten und Zehnten Buches.

§ 67a Abs. 1 Satz 1 SGB X lautet:

Das Erheben von Sozialdaten durch in § 35 des Ersten Buches genannte Stellen ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist.

Im zu bewertenden Sachverhalt war keiner dieser beiden Alternativen gegeben. Insbesondere lagen nicht die Voraussetzungen des § 67a Abs. 1 SGB X vor. Denn zweifellos war die Kenntnis der erhobenen Angaben – Name und Anschrift des von der Krankenversicherung Beratenen sowie Identität und Erreichbarkeitsdaten des Kundenbetreuers seiner Krankenkasse – nicht zur Aufgabenerfüllung der Krankenversicherung erforderlich. Das Beratungsgespräch hatte einen unverbindlichen Charakter und diente nicht der direkten Vertragsanbahnung. Zugleich konnte aber auch die von dem Versicherten gegebene Einwilligung nicht als wirksame Legitimation der Datenerhebung gewertet werden. Denn unabhängig von der Frage, ob eine Einwilligung im Bereich der Gesetzlichen Krankenversicherung überhaupt als Erhebungsbefugnis in Frage kommt, wenn die Kenntnis der Daten eindeutig keinen Nutzen für die Aufgabenerfüllung der erhebenden Stelle besitzen, entsprach im konkreten Fall die eingeholte Erklärung eindeutig nicht den Anforderungen an eine wirksame Einwilligung im Sinne von § 67b Abs. 2 Satz 1 SGB X. Insbesondere fehlte es an einem Hinweis auf die beabsichtigte Verwendung der angefertigten Kopie des Informationsschreibens.

§ 67b Abs. 2 Satz 1 SGB X lautet:

Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Aus den gleichen Gründen fehlte es auch einer datenschutzrechtlichen Befugnis der Krankenversicherung zur Übermittlung der in der angefertigten Kopie enthaltenen Sozialdaten an die von ihr kontaktierten Arbeitgeber. Aufgrund der besonderen Schwere des Datenschutzverstoßes, die regelmäßig mit einem Bruch des Sozialgeheimnisses verbunden ist, der Offensichtlichkeit der Rechtsverletzung und dem in keiner Weise bestehenden Bedarf der Krankenversicherung an den unberechtigt erhobenen und weitergegebenen Sozialdaten zu Zwecken der Mitgliederwerbung kam der LfDI nicht umhin, das Vorgehen formell zu beanstanden. Inzwischen hat die betroffene Krankenkasse mitgeteilt, dass sie die durch den LfDI getroffene rechtliche Bewertung der Angelegenheit teile und diverse Maßnahmen zur Vermeidung vergleichbarer Vorfälle in der Zukunft getroffen worden seien.

7. SCHULDATENSCHUTZ UND WISSENSCHAFT

7.1 Schuldatenschutz

7.1.1 Datenschutz bei Lernplattformen

Die Datenschutzaufsichtsbehörden haben im April 2016 eine ausführliche Orientierungshilfe für Online-Lernplattformen im Schulunterricht veröffentlicht (Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht - Stand April 2016; https://s.rlp.de/dsk042016)

Gleichwohl sind in der konkreten Umsetzung landesspezifische Besonderheiten und Absprachen mit den jeweiligen Aufsichtsbehörden zu berücksichtigen. Nachfolgend werden die für die Schulen in Rheinland-Pfalz maßgeblichen Punkte zum Datenschutz bei Lernplattformen in Form einer Checkliste zusammengefasst, welche die Grundlage für die Beratungs- und Kontrolltätigkeit des LfDI auch schon im Hinblick auf die Europäische Datenschutz-Grundverordnugn bilden.

1. Allgemeines:

› Erfolgt der Betrieb einer Lernplattform nicht durch die Schule selbst, sondern im Auftrag, so ist dies im Rahmen einer Auftragsverarbeitung mit dem Anbieter vertraglich zu regeln.

› Unterrichtung der Betroffenen über den Einsatz der Lernplattform: Soweit keine Regelungen zur Verbindlichkeit (verpflichtender Bestandteil des Unterrichts) erlassen worden sind, ist die Nutzung nur auf freiwilliger Basis zulässig.

2. Verpflichtungen der Schule ggf. unter Einbeziehung des/der schulischen Datenschutzbeauftragten:

› Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten

› Datenschutz-Folgenabschätzung durchführen

3. Benutzerkonten:

› Individuelles Benutzerkonto für jede/n Schüler/in anlegen.

› Bei der Anlage eines Nutzerkontos für Schülerinnen und Schüler sind nur die für die Nutzung erforderlichen Daten zu erfassen. Eine private E-Mail-Adresse darf nur auf freiwilliger Basis erhoben werden.

4. Maßnahmen zum Schutz vor unbefugtem Zugriff treffen:

› Verschlüsselung der Datenübertragung zwischen Server und Nutzerin und Nutzer sicherstellen.

› Richtige Zuordnung zu einer bestimmten Klasse oder zu einem Kurs beachten; kein Zugriff auf klassen- bzw. kursfremde Inhalte.

› Bei Fortführen eines Kurses als Folgekurs mit neuen Teilnehmern müssen verbleibende Inhalte gelöscht/anonymisiert werden (Forenbeiträge, Wikis, etc.).

5. In einer Nutzerordnung Detailfragen regeln:

› Rollen- und Berechtigungskonzept erarbeiten:

  › Wer hat welchen Zugriff (ändernd/lesend) auf welche Daten?

  › Genaue Rollen vorsehen u.a. für: Schulleitung, Klassenlehrerin bzw. -lehrer, Administratorin bzw. Administrator, Eltern, Schülerin bzw. Schüler, Externe, Austauschschülerin bzw. -schüler, Praktikantin bzw. Praktikant.

› Protokolldaten:

  › Verbot der Überwachung von Aktivitäten der Schülerinnen und Schüler durch Lehrkraft festlegen (Ausnahme: Dies ist pädagogische Aufgabe im Rahmen einer Leistungsmessung).

  › Verbot von allgemeinen Verhaltens- und Leistungskontrollen in Bezug auf die Lehrkraft durch Schulleitung in die Nutzungsordnung oder in Dienstvereinbarung mit dem Personalrat aufnehmen.

› Löschungsfristen festlegen (Vorschlag: Ende des laufenden Schuljahrs, ansonsten bei Schulwechsel oder Verlassen der Schule).

6. Unterrichtung der Betroffenen (Schülerin bzw. Schüler, Eltern, Lehrkräfte) über:

› Zugriffsrechte

› Auswertungsmöglichkeiten

› Einsichtsrechte

› Löschfristen

7.1.2 Elektronisches Klassenbuch

Die Schulordnungen enthalten in aller Regel nur rudimentäre Bestimmungen zum Datenschutz bei Klassenbüchern (vgl. § 89 Abs. 6 Übergreifende Schulordnung). Auch hatte der Gesetzgeber bei der Formulierung der Regelung offenkundig die herkömmliche Papier-

form der Klassenbücher vor Augen. Dies führt dazu, dass viele Datenschutzfragen, die mit dem Führen eines elektronischen Klassenbuchs in Zusammenhang stehen, nicht beantwortet werden.

Die nachfolgenden Ausführungen basieren auf den Erkenntnissen, die der LfDI im Rahmen örtlicher Feststellungen zur Software „WebUntis“ in einzelnen Schulen getroffen hat. Eine abschließende datenschutzrechtliche Bewertung des Verfahrens ist damit ebenso wenig verbunden wie eine Zertifizierung. Maßgeblich sind stets die tatsächlichen Verhältnisse vor Ort und die konkrete Ausgestaltung im Kontext zur schulischen IT-Ausstattung insgesamt.

Bei „WebUntis“ handelt es sich um eine cloudbasierte Software des österreichischen Herstellers Untis GmbH, mit deren Hilfe die Papierversion des herkömmlichen Klassenbuchs vollständig abgeschafft werden kann. Insoweit ist hierfür ein Vertrag zur Verarbeitung von personenbezogenen Daten im Auftrag abzuschließen. Außerdem sind die mit der Softwarebetreuung befassten Beschäftigten des Dienstleisters auf das Datengeheimnis zu verpflichten.

Die Software bietet beispielsweise auch die Möglichkeit, Noten einzutragen. Dies ist jedoch nach § 89 Abs. 6 der Übergreifenden Schulordnung nicht zulässig. Nach dieser Bestimmung dürfen in Klassen- und Kursbücher nur eingetragen werden:

1. Namen und Geburtsdatum der Schülerinnen und Schüler,

2. Teilnahme an Schulveranstaltungen,

3. Vermerk über unentschuldigtes und entschuldigtes Fernbleiben und über Beurlaubungen,

4. erzieherische Einwirkungen gemäß § 96 Abs. 1,

5. Namen und Anschrift der Eltern,

6. Angaben zur Herstellung des Kontakts in Notfällen.

Diese Aufzählung ist abschließend. Weitere Daten dürfen im Klassen- oder Kursbuch nicht aufgenommen werden.

Je nach Softwareausgestaltung können in den Klassenräumen Laptops zur Eintragung durch die Lehrkräfte eingerichtet werden, die ausschließlich für WebUntis genutzt werden. Die Lehrkraft kann dann zu Beginn des Unterrichts etwa die Anwesenheit und im Laufe der Stunde Einträge, z.B. erzieherische Einwirkungen („Tadel“) sowie Hausaufgaben und Lehrstoff eintragen. Dabei können mehrere Schülerinnen oder Schüler gleichzeitig ausgewählt und mit demselben Eintrag versehen werden (beispielsweise bei gemeinsamer Verspätung). Zudem können Lehrkräfte über einen Zugriff von zuhause aus im Krankheitsfall Arbeitsaufträge an die vertretende Lehrkraft direkt in die entsprechende Stunde eintragen.

Die Software sieht auch Zugriffsrechte der Eltern vor, was in dieser Form beim herkömmlichen Klassenbuch nicht zulässig war. Andererseits haben Eltern nach den Bestimmungen der Schulordnungen zumindest einen Auskunftsanspruch über die ihr Kind betreffenden Daten (z.B. § 8 Abs. 3 Satz 3 Übergreifende Schulordnung). Wie die Schule diesen Auskunftsanspruch erfüllt, liegt in ihrem pflichtgemäßen Ermessen. Insofern kommt auch die Einräumung eines Zugriffs auf das Elektronische Klassenbuch vom Grundsatz her in Frage. Allerdings ist der Zugriff hierbei strikt auf die Daten des eigenen Kindes zu beschränken. Dies gilt insbesondere im Falle eines „Tadels“ bei meh-

reren Schülerinnen und Schülern. Da es sich bei dem Auskunftsrecht der Eltern um ein Recht und nicht um eine Verpflichtung handelt, ist die Schule daran gehindert, die Protokolldaten auszuwerten, um Eltern aufzufordern, sich regelmäßig einzuloggen, wie dies bei einer Schule kurz nach Einführung des elektronischen Klassenbuchs der Fall war.

Die Software verfügt auch über eine Nachrichtenfunktion, die eine Weiterleitung der Nachrichten auf die hinterlegte E-Mailadresse bietet. Soweit Schulen planen, z.B. nach drei vergessenen Hausaufgaben Elternbriefe über das System abzuwickeln, ist hierbei zu bedenken, dass in der Kommunikation mit den Eltern personenbezogene Daten per E-Mail nur verschlüsselt übermittelt werden dürfen. Alternativ kann die Benachrichtigung der Eltern per E-Mail über WebUntis lediglich auf das Vorliegen einer Nachricht hinweisen, selbst jedoch keine personenbezogenen Daten enthalten. Die Versendung von Nachrichten per E-Mail, die lediglich allgemeine Informationen enthalten (etwa Unterrichtsausfälle; Einladung zum Tag der Offenen Tür), ist dagegen unproblematisch.

Bei Eintritt der Volljährigkeit der Schülerinnen und Schüler muss sowohl der Zugang der Erziehungsberechtigten als auch die Unterrichtung der Eltern per E-Mail gelöscht oder inaktiv geschaltet werden.

Die bzw. der schulische Datenschutzbeauftragte sollte im Rahmen der Vorabkontrolle bzw. der Datenschutz-Folgenabschätzung den Umfang der gespeicherten Daten und die vorgesehenen Auswertungsmöglichkeiten prüfen. Außerdem ist eine Verfahrensbeschreibung zu erstellen und in das Verzeichnis von Verarbeitungstätigkeiten vor Ort aufzunehmen. Die Eltern sollten über die Einführung des elektronischen Klassenbuchs und der damit in Zusammenhang stehenden Informationsvorgänge unterrichtet werden. Sofern hierbei private E-Mail-Anschriften der Eltern bzw. Schülerinnen und Schüler erfasst werden sollen, ist dies nur auf freiwilliger Basis möglich.

In einer Dienstanweisung sollten insbesondere folgende Fragen des technisch-organisatorischen Datenschutzes geregelt werden:

› Definition des Zwecks des Verfahrens

› verschlüsselter Zugriff auf das Webportal

› automatischer Logout nach wenigen Minuten Inaktivität, insbesondere bei mobilen Endgeräten

› Verwendung von sicheren Passwörtern, wenn über Apps auf das elektronische Klassenbuch zugegriffen wird; kein Schreibzugriff auf das Klassenbuch via App

› Regelungen zum dienstlichen Einsatz privater Endgeräte

› Zweifaktor-Authentifizierung bei der Anmeldung

› Erstellen eines Rollenberechtigungskonzeptes; wer darf auf welche Daten lesend/schreibend zugreifen? Welche Auswertungen sind durch welche Personen zulässig? Sind die Auswertungen anonym oder personenbezogen? Genaue Rollen vorsehen u.a. für: Schulleitung, Klassenlehrerin bzw. -lehrer, Administratorin bzw. Administrator, Eltern, Schülerin bzw. Schüler, Austauschschülerin bzw. -schüler, Praktikantin bzw. Praktikant

› Einmalpasswort zur Erstanmeldung (per Brief mit Rückantwortzettel und Hinweisen zu den eingestellten Passwortrichtlinien)

› Protokollierung der Nutzeraktivitäten; Beteiligung der Personalvertretung (Abschluss einer Dienstvereinbarung)

› Backup: Exporte von unverschlüsselten Datensätzen auf beweglichen Datenträgern sichern, die an einem gesicherten Ort (z.B. Safe) deponiert werden

› Erarbeitung eines Löschkonzepts unter Beachtung vorgeschriebener Löschfristen.

7.1.3 Foto- und Filmaufnahmen in der Kita

Im Zuge der Verbreitung von Smartphones und Tablets müssen sich auch Kitas mehr und mehr mit Fragen rund um den Datenschutz beschäftigen. Häufig geht es dabei um das Recht am eigenen Bild, seien es Fotos von Kindern, die kitaintern ausgehängt, in die Portfolios aufgenommen oder auf der Kita-Homepage eingestellt werden. Auch der Umgang mit Eltern, die stolz die Aktivitäten ihrer Kinder dokumentieren und den Verwandten in aller Welt schicken möchten, stellt Erzieherinnen und Erzieher vor die Notwendigkeit datenschutzrechtlicher Bewertungen. Kita-Leitungen fragen häufig beim LfDI nach, wie sich eine Kita verhalten soll, wenn Eltern auf Kita-Festen filmen und diese Videos auf YouTube oder anderen Kanälen veröffentlichen. Einige Eltern meinen sogar, mit Hilfe von Drohnen Aufnahmen über dem Kita-Gelände fertigen zu müssen.

Die Kita ist im Rahmen ihres Hausrechtes berechtigt, das Fotografieren und Filmen von Kindern bei Veranstaltungen zu regeln, d.h. auch zu untersagen. Diese Regelungen sollten aus Sicht des LfDI zum Gegenstand des Aufnahmevertrages mit den Eltern gemacht werden. In Bezug auf Drohnen regelt die neue Drohnen-Verordnung vom 30. März 2017 ein grundsätzliches Betriebsverbot über Wohngrundstücken.

Auch wenn kein ausdrückliches Verbot von Fotos und Videos durch die Kita erfolgt ist, dürfen Eltern bei Kita-Veranstaltungen ihre Aufnahmen nur veröffentlichen, wenn das Ereignis selbst und nicht einzelne Kinder, Eltern oder Erzieherinnen und Erzieher im Vordergrund der Aufnahmen stehen (§§ 22, 23 KunstUrhG). Eine unbefugte Veröffentlichung kann ein strafbares Verhalten nach § 33 KunstUrhG darstellen. Auch hier empfiehlt der LfDI im Aufnahmevertrag darauf hinzuweisen, dass Fotos und Filme, die auch andere Personen zeigen, nicht ohne Einwilligung der Betroffenen in sozialen Netzwerken veröffentlicht werden dürfen.

Als Vorgehensweise kann zwischen Kita und Eltern auch vereinbart werden, dass die Einrichtung selbst Fotos und Videos fertigt und an die Eltern weitergibt. Im Aufnahmevertrag sollte darauf hingewiesen werden, dass die Fotos bzw. Videos dann nur für den Zweck des gegenseitigen Austauschs („privater Gebrauch“) weitergegeben werden und eine Veröffentlichung in sozialen Medien durch die Eltern ohne Einwilligung der Betroffenen nicht zulässig ist.

Der LfDI hat in zahlreichen Fortbildungen Erzieherinnen und Erzieher in Kitas zum Datenschutz geschult. Gemeinsam mit dem Bildungsministerium wurde ein Flyer erstellt, der an die Kitas verteilt wurde und aufgrund der großen Nachfrage nachgedruckt werden musste. Dieser gibt in komprimierter Form praktische Tipps für den datenschutzgerechten Alltag in der Kita. Der Flyer ist online abrufbar unter https://s.rlp.de/dskita.

Ergänzend hierzu sollen in einem zweiten Schritt Mustertexte (z.B. für Einwilligungserklärungen oder Aufnahmeverträge) auf dem Kita-Server hinterlegt werden.

7.1.4 Nutzung von MS-Office 365 und anderen Cloud-Diensten durch Schulen

Mit der Safe-Harbor-Entscheidung hat der Europäische Gerichtshof am 6. Oktober 2015 Datenübermittlungen in die USA die rechtliche Grundlage entzogen. Er kippte das Safe-Harbor-Abkommen (vgl. …), das seit 2000 bestand und die Grundlage des transatlantischen Datentransfers für viele europäische Unternehmen bildete. In den USA würden Daten von EU-Bürgerinnen und Bürgern gesammelt, ohne dass sie vor dem Zugriff US-amerikanischer Sicherheitsbehörden ausreichend geschützt seien, urteilte das Gericht. Die Bestimmungen des PATRIOT Act erlauben es nämlich US-Behörden, ohne richterliche Anordnung auf die Server von US-Unternehmen zuzugreifen; auch ausländische Töchter sind nach dem Gesetz verpflichtet, den Zugriff auf ihre Server zu gewähren und zwar auch dann, wenn lokale Gesetze dem entgegenstehen. Nach dem Urteil eines New Yorker Bundesgerichts vom 25. April 2014 sind US-amerikanische Unternehmen gegenüber US-Sicherheitsbehörden auch dann zur Herausgabe der Daten verpflichtet, wenn die Daten im Ausland gespeichert sind.

Am 2. Februar 2016 gab die Europäische Kommission bekannt, sie habe sich mit der US-amerikanischen Regierung auf eine Nachfolgeregelung geeinigt, die den Namen EU-US Privacy Shield trage. Ob diese Regelungen den Anforderungen des Europäischen Gerichtshofs entsprechen, wird von Datenschützern jedoch bezweifelt.

› Wenn Schulen US-amerikanische Cloud-Anbieter nutzen möchten, muss daher die US-amerikanische Praxis des Datensammelns und des unkontrollierten Zugriffs durch staatliche Stellen ausgeschlossen sein.

› Die von Microsoft angebotenen bzw. unterstützten Ausprägungen von Office365 unterscheiden sich nach Art und Umfang der genutzten Cloud-Funktionen, so dass die datenschutzrechtliche Bewertung vom jeweiligen Einsatzszenario abhängt.

› Wenn Office365 in der Variante betrieben wird, bei der die Microsoft Office- und Server-Anwendungen sowie die Daten lokal auf einer eigenen IT-Struktur vorgehalten werden („On-Premise“), ergeben sich die geschilderten Probleme nicht.

› Möglich ist auch ein Hybridbetrieb, bei dem die Office-Anwendungen als „Software-as-a Service“ aus der Cloud bezogen werden, die Datenspeicherung jedoch lokal erfolgt. Auch hier werden die Daten unter alleiniger Kontrolle der verantwortlichen Stelle verarbeitet.

› Soweit lediglich Speicherplatz in der Cloud für die Ablage von Daten bzw. Dokumenten genutzt und Zugriffe auf personenbezogene Daten durch eine eigene zusätzliche Inhaltsverschlüsselung ausgeschlossen werden, bestehen keine datenschutzrechtlichen Bedenken. Dies kann aber auch ohne Nutzung außereuropäischer Anbieter, insbesondere im Wege eines sicheren Datenaustauschs über den BSCW-Server des Pädagogischen Landesinstituts erfolgen.

› Möglich ist weiterhin der Betrieb von Office365 in Form einer „Private-Cloud“ innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums durch einen Dienstleister, bei dem die Gefahr einer Herausgabe von Daten auf Anweisung einer außereuropäischen Muttergesellschaft nicht besteht. Mit dem ab 2017 angebotenen Modell „Microsoft Deutschland Cloud“ bietet Microsoft eine Datenverarbeitung ausschließlich in deutschen Rechenzentren an und sieht

T-Systems als Treuhänder der Daten vor. Voraussetzung ist der Abschluss eines Vertrages zur Auftragsdatenverarbeitung, der den Vorgaben aus § 4 LDSG bzw. künftig der Datenschutz-Grundverordnung entspricht. Darüber hinaus muss aus datenschutzrechtlicher Sicht ein Zugriff auf die in der Cloud gespeicherten personenbezogenen Daten durch Microsoft ausgeschlossen sein. Aus technisch-organisatorischer Sicht waren hier insbesondere die Rolle des Treuhänders, die Frage der Zugriffsberechtigungen sowie die Ausgestaltung von Servern und Modulen klärungsbedürftig. Der Hessische Datenschutzbeauftragte hat in einer Pressemitteilung vom 22. August 2017 den Einsatz von Office 365 im schulischen Konzept als Deutschland-Cloud-Modell unter bestimmten Voraussetzungen als datenschutzrechtlich akzeptabel bewertet: https://www.datenschutz.hessen.de/ds12.htm

Der LfDI schließt sich dieser Auffassung an.

Wenn losgelöst von den dargestellten Szenarien Cloud-Lösungen außereuropäischer Anbieter genutzt werden sollen, bei denen die Daten der Nutzerinnen und Nutzer durch den Anbieter verarbeitet bzw. gespeichert werden (z.B. Google Classroom, MS Office365 Education) ist dies aus Datenschutzsicht nur möglich, wenn die folgenden Voraussetzungen berücksichtigt werden:

› Die Verwendung pseudonymer Benutzerzugänge (Accounts) für Lehrkräfte, Schülerinnen und Schüler, die durch die jeweilige Bildungseinrichtung erstellt bzw. verwaltet und an die Teilnehmer vergeben werden.

› Die Trennung privater und schulischer Nutzung; die im Rahmen der schulische Nutzung eingerichteten Accounts dürfen nicht für private Zwecke genutzt werden.

› Keine Speicherung personenbezogener Daten bzw. Dokumente in der Cloud. Statt des Klarnamens ist daher ein Pseudonym zu verwenden. Allerdings ist bei der Pseudonymisierung zu beachten, dass keine „sprechenden Pseudonyme“, wie beispielsweise der Vorname einer Schülerin oder eines Schülers, verwendet wird. Auch dürfen die in der Cloud eingestellten Dokumente (z.B. Arbeitsblätter) keine Namen der Schülerinnen und Schüler enthalten.

› Insbesondere ist bei der Nutzung von Google-Classroom zu beachten, dass der Pseudonymisierungsprozess von den Schülerinnen und Schülern korrekt eingehalten wird. Dies bedeutet, dass kein Einloggen mit dem Account für private E-Mail-Nutzung oder eine Verknüpfung mit privaten anderweitigen Google-Accounts, beispielsweise von Google-Mail oder Youtube erfolgt. Weiterhin sollten die Accounts durch die Bildungseinrichtung erstellt und verwaltet und sodann an die Teilnehmerinnen und Teilnehmer vergeben werden. Angesichts der von Google genutzten Tracking-Mechanismen (Cookies, Device-IDs, etc.) besteht grundsätzlich die Gefahr, dass bereits durch die einmalige Nutzung unter einem vorhandenen persönlichen Google-Account das jeweilige Pseudonym gegenüber Google aufgehoben wird. Von daher sollen die Schülerinnen und Schüler Nutzungshinweise erhalten und allgemein über die Gefährdungen ihrer Privatsphäre im Rahmen der Nutzung von Google-Diensten informiert werden.

Von Bedeutung ist schließlich die Tatsache, dass sich die Anbieter entsprechender Lösungen zum Teil in den Nutzungsbedingungen die Anzeige von Werbung vorbehalten. Mit Blick auf das grundsätzliche Werbeverbot an Schulen und das Verbot der Weitergabe von Schüler- bzw. Elterndaten für Werbezwecke (vgl. § 103 Übergreifende Schulordnung) ergeben sich weitere klärungsbedürftige Fragen. Hier

muss geprüft werden, ob der jeweilige Anbieter die Werbefreiheit des genutzten Dienstes sicherstellt oder zusichert, dass Nutzungsdaten nicht für Werbezwecke verwendet werden.

7.1.5 Nutzung von WhatsApp im schulischen Kontext

Laut Jim-Studie 2017 nutzen derzeit 94 Prozent der Zwölf- bis 19-Jährigen WhatsApp; selbstverständlich können auch Lehrkräfte Facebook und WhatsApp für private Zwecke nutzen und hier auch mit Jugendlichen „befreundet" oder anders vernetzt sein; beispielsweise wenn beide ähnliche Hobbies haben oder in demselben Verein Sport treiben. Dies entspricht im Übrigen auch den Allgemeinen Geschäftsbedingungen von WhatsApp, die lediglich eine private Nutzung der Chats vorsehen.

Lehrkräften ist es in Rheinland-Pfalz aber untersagt, sich für die schulische Kommunikation auf Facebook oder WhatsApp mit Schülerinnen und Schülern zu vernetzen, indem beispielsweise Freundschaftsanfragen an Schülerinnen und Schüler gestellt werden oder auf WhatsApp eine gemeinsame Gruppe für die schulische Kommunikation mit Eltern oder Schülerinnen und Schülern eingerichtet wird.

Zur schulischen Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern steht den Schulen u.a. eine landeseigene, kostenfreie, auf Moodle basierende Lernplattform zur Verfügung: http://lernenonline.bildung-rp.de. Diese gewährleistet die Datensicherheit durch die Verwendung eines landeseigenen Servers.

Sofern eine Lehrkraft es als notwendig erachtet, über Messenger mit Eltern und Schülerinnen und Schülern zu kommunizieren, kommen nur europäische Anbieter, die eine Ende-zu-Ende-Verschlüsselung anbieten, in Betracht (z. B. Pidgin/OTR, Signal 2.0, SIMSme, Chiffry, oder Threema).

Hierbei ist allerdings stets das Distanzgebot zu beachten: Das zwischen den Lehrkräften und Schülerinnen und Schülern einer Schule bestehende Obhutsverhältnis verpflichtet Lehrkräfte nach den Bestimmungen im Schulgesetz zu einem „verantwortungsvollen und vertrauensvollen Umgang mit Nähe und Distanz" (§§ 1 Abs. 5, 25 Abs. 3 SchulG).

Der LfDI hat zu diesen und anderen Fragen des schulischen Datenschutzes gemeinsam mit dem Bildungsministerium einen Flyer herausgegebenen, der 2017 veröffentlicht wurde http://s.rlp.de/schuldatenschutz2017.

7.2 Wissenschaft

7.2.1 Datenschutzrechtliche Prüfung wissenschaftlicher Forschungsvorhaben

Bereits in den Datenschutzberichten 2012/2013 (vgl. 24. Tb., Tz. III-6.2.1) und 2014/2015 (25. Tb., Tz. III-7.2.1) hatte der LfDI über die stetig steigende Zahl der im Zusammenhang mit § 67 Abs. 6 SchulG zur datenschutzrechtlichen Bewertung eingereichten Vorhaben berichtet.

Nun wurde die bereits vor geraumer Zeit gemeinsam mit der Aufsichts- und Dienstleistungsdirektion als Schulbehörde und dem Wissenschaftsministerium abgestimmte Verfahrensänderung bei der datenschutzrechtlichen Prüfung wissenschaftlicher Untersuchungen an Schulen endlich zum Schuljahr 2017/2018 in die Praxis umgesetzt.

Zu diesem Zweck wurde den rheinland-pfälzischen Hochschulen eine Generalgenehmigung

für die Durchführung wissenschaftlicher Untersuchungen in Schulen erteilt. Anhand einer vom LfDI zu Verfügung gestellten „Checkliste“ sollen die Verantwortlichen in die Lage versetzt werden, weitgehend eigenständig zu prüfen, ob eine geplante wissenschaftliche Untersuchung den datenschutzrechtlichen Vorgaben Rechnung trägt. Eine Beteiligung des LfDI ist nur noch in Zweifelsfällen vorgesehen.

Die Verfahrensänderung greift offenbar, da gerade im Hinblick auf die Prüfung wissenschaftlicher Untersuchungen im Rahmen von Qualifikationsmaßnahmen (z.B. Bachelor-, Master-, Examensarbeiten) seit einigen Monaten eine Entlastung spürbar ist. Dies ist zu begrüßen, da die freiwerdenden personellen Kapazitäten bei Maßnahmen zur Vorbereitung auf die Europäische Datenschutz-Grundverordnung dringend benötigt werden.

7.2.2 Die Einwilligung - datenschutzrechtliches Spannungsfeld bei Biobanken

Erstmalig und dann gleich zweifach wurde die Bitte an den LfDI gerichtet, im Rahmen der Änderung bzw. der Fortführung einer Biobank beratend mitzuwirken.

Eine Biobank kann als langfristige Sammlung von menschlichem Körpermaterial und dazugehörigen Gesundheitsdaten für die medizinische Forschung beschrieben werden. Aufgrund dieser Kombination können Biobanken für eine Vielzahl von Auswertungsmöglichkeiten und Forschungsprojekten zur Verfügung stehen. Sinn und Zweck ist es, dass neu und unvorhersehbar auftretende Fragestellungen anhand eines solchen Informationsvorrates beforscht werden können.

Somit musste sich der LfDI auch mit der Frage auseinandersetzen, welche Anforderungen an eine wirksame Einwilligung als Grundlage für die Verarbeitung der o.g. personenbezogenen Daten zu stellen sind.

Von den Datenschutzaufsichtsbehörden wird teilweise eine informierte Einwilligung, auch sog. informed consent, favorisiert. Dies bedeutet, dass Spendende oder Patienteninnen und Patient oder Probandinnen und Probanden über den möglichst bestimmten Zweck der Verarbeitung und Empfängerkreis aufzuklären sind. Dabei wird in diesem Zusammenhang auch ins Feld geführt, dass Biomaterial prinzipiell nicht (absolut) anonymisierbar ist, da es über identifizierte Referenzproben immer einer bestimmten Person zuordenbar bleibt und sowohl Gesundheitsdaten als auch genetische Informationen eines besonderen Schutzes bedürfen.

Dem wird aus dem Kreis der Wissenschaft entgegengehalten, dass die in einem informed consent enthaltenen Begrenzungen von Nutzungszweck, -dauer und konkreten Nutzerinnen und Nutzern dem Sinn und Ziel einer Biobank entgegenstehen. Gleichzeitig wird auf den hohen Stellenwert von Biobanken in der Grundlagenforschung, der klinischen Forschung und bei der Fortentwicklung der personalisierten Medizin verwiesen. Die Wissenschaftlerinnen und Wissenschaftler möchten daher mit einer breit bzw. umfassender angelegten Einwilligung, auch sog. broad consent, arbeiten, die auch im Zeitpunkt der Einwilligungserklärung noch unspezifische Forschungszwecke erfasst, weil Forschung auf innovative Erkenntnisse angelegt ist.

Aber welchen Inhalt muss eine Einwilligung umfassen, um wirksam zu sein?

Die ab dem 25. Mai 2018 gültige EU-DS-GVO formuliert in Art. 6 Abs. 1 lit.a folgendermaßen:

Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt.

Und wie ist in dem Zusammenhang ErwGr. 33 zur Europäischen Datenschutz-Grundverordnung zu interpretieren?

Hier wird das Problem angesprochen, dass oftmals der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden kann. Daher sollte es betroffenen Personen unter gewissen Rahmenbedingungen erlaubt sein, ihre Einwilligung für bestimmte Bereiche, wie z.B. die Krebsforschung, wissenschaftlicher Forschung oder Teile von Forschungsprojekten zu geben.

Aus diesem Erwägungsgrund wird die Möglichkeit für den sog. broad consent abgeleitet, also dass sich betroffene Personen damit einverstanden erklären können, dass ihre Forschungsdaten auch über ein aktuelles Forschungsprojekt hinaus genutzt werden können.

Wie können das Recht auf informationelle Selbstbestimmung der Spendenden und die Wissenschaftsfreiheit in diesem Spannungsfeld in Ausgleich gebracht werden und wie könnte eine tragbare Formulierung einer ausführlichen und gleichzeitig verständlichen Information lauten?

Der Arbeitskreis Medizinischer Ethik-Kommissionen für Information und Einwilligungserklärung hat einen Mustertext entwickelt. Ein Austausch mit dem Arbeitskreis Wissenschaft und Forschung der Datenschutzaufsichtsbehörden wurde begonnen.

Diskutiert wird auch eine optional gestaltete Einwilligung, sodass gesondert der Weitergabe von Daten an ausländische Forschungseinrichtungen oder Industriepartner zugestimmt werden oder eine Begrenzung auf bestimmte Indikationsgebiete vorgenommen werden kann. Weiterhin wird erörtert, die Einwilligung mit Sicherungsmechanismen zu ergänzen, beispielhaft kann hier das „5-Säulen-Konzept“ des Deutschen Ethikrates genannt werden.

Das heterogene Meinungs- und Regelungsbild gilt es unter Ausgleich der zu berücksichtigenden Interessen zu harmonisieren und dabei die verschiedenen Ansätze von Biobanken zu berücksichtigen.

7.2.3 Forschungsdatenzentrum (FDZ) der Statistischen Landesämter – Erweiterung des regionalen Standortes Bad Ems

Die Statistischen Ämter der Länder betreiben seit 2002 ein gemeinsames Forschungsdatenzentrum (FDZ) mit regionalen Standorten in den jeweiligen Statistischen Landesämtern. Ziel und Aufgabe des Forschungsdatenzentrums ist es, Mikrodatenbestände der amtlichen Statistik über geregelte Zugangswege unter Einhaltung von unterschiedlichen Stufen der Anonymität für die wissenschaftliche Forschung bereitzustellen (§ 3a Abs. 2 BStatG). Dabei hängt der Informationsgehalt der Mikrodaten für die wissenschaftliche Nutzung von dem Grad der Anonymität ab.

Das Statistische Landesamt Rheinland-Pfalz ist mit dem regionalen Standort Bad Ems an diesem Forschungsdatenzentrum beteiligt. Dieser regionale Standort soll um einen externen Gastwissenschaftlerarbeitsplatz (GWAP) an der Universität Trier erweitert werden, weil Bad Ems abseits von großen Hochschulen oder wirtschafts- und sozialwissenschaftlichen For-

schungseinrichtungen liegt.

Wegen der zu gewährleistenden Geheimhaltung (§ 16 Abs. 6 S. 1 Nr. 2 BStatG) wurde der LfDI um Prüfung und Bewertung des überarbeiteten Informationssicherheitskonzeptes für den regionalen Standort sowie des Betriebskonzeptes für den externen GWAP gebeten, mit dem ausführliche Maßnahmen für die Zutritts-, Raum- und Sicherheitskontrolle des abgeschotteten GWAP außerhalb der Räumlichkeiten des Statistischen Landesamtes beschrieben werden.

Insbesondere weil am externen GWAP keine lokale Bereitstellung von Daten erfolgt und keine Kommunikations- oder Recherchemöglichkeiten für eine Nutzerin bzw. einen Nutzer bestehen, lautete das Prüfungsergebnis, dass die vorgesehenen Vorkehrungen zur Wahrung der Geheimhaltung geeignet sind. Weiterhin wurden Anmerkungen des LfDI u.a. zur Erforderlichkeit der Videoüberwachung des externen GWAP zum Vorteil der Wissenschaftlerinnen und Wissenschaftler berücksichtigt.

8. MEDIENBILDUNG

8.1. Bildungsaktivitäten des LfDI

8.1.1 Multiplikatorenschulungen

Mit dem Ziel, Aspekte des schulischen Datenschutzes für die im Bildungsbereich tätigen Personengruppen (wie z.B. Lehrerinnen und Lehrer, Systemadministratorinnen und -administratoren und Medienberaterinnen und -berater) näher zu bringen, wurde im Berichtszeitraum eine Vielzahl unterschiedlicher Schulungen und Informationsveranstaltungen durchgeführt.

Ein wichtiges Instrument der digitalen Fortbildungen für Lehrkräfte ist hierbei die jährlich durch das Pädagogische Landesinstitut durchgeführte iMedia. Der LfDI beteiligt sich regelmäßig mit verschiedenen Workshops zu den Themen:

- Schulischer Datenschutz für Lehrerinnen und Lehrer
- Datentracking im Internet
- Smartphones – Spione in der Hosentasche
- Big Data und das Internet der Dinge.

Weiterhin wurden Lehrkräfte und schulische Medienberaterinnen und -berater bei Studientagen bzw. Netzwerktagungen hinsichtlich des Umgangs mit privaten Endgeräten und der Nutzung cloudbasierter Dienste geschult.

8.1.2 Weiterentwicklung des Schülerworkshop-Projekts

Im Berichtszeitraum wurden an rheinland-pfälzischen Schulen im Jahr 2016 insgesamt 451 Workshops und im Jahr 2017 fast 500 Workshops durchgeführt https://s.rlp.de/Htz9i. Seit Beginn des Projektes im Jahr 2010 wurden damit weit über 100.000 Schülerinnen und Schüler im Bereich der digitalen Bildung fit gemacht. Die Datenschutz-Workshops des LfDI sind inzwischen wichtiger Bestandteil der Landesstrategie „Medienkompetenz macht Schule"; dies haben Ministerpräsidentin Malu Dreyer und Bildungsministerin Dr. Stefanie Hubig in ihren Festreden bei der Jubiläumsveranstaltung im September 2017 anlässlich 10 Jahre „Medienkompetenz macht Schule" deutlich gemacht.

Sowohl Inhalte als auch konzeptionelle Annäherung an die Zielgruppe unterliegen hier einem dynamischen Wandel, welcher mit der technischen Ausstattung und dem Nutzungsverhalten der Kinder und Jugendlichen einhergeht. Während noch vor einigen Jahren erst mit dem Wechsel an die weiterführenden Schulen Kinder mit Smartphones ausgestattet wurden, hat sich dieser Zeitpunkt in der Zwischenzeit deutlich nach vorn verlagert. Daten- und Medienkompetenzförderung muss dementsprechend bereits in der Grundschule beginnen. Daher wurden 125 Grundschulen neu in das Programm „Medienkompetenz macht Schule" aufgenommen. Auch der LfDI musste sich diesen Veränderungen anpassen: So werden die Workshops an Grundschulen künftig bereits ab der dritten Klasse angeboten und zeitlich von zwei auf vier Schulstunden verdoppelt. Die hierbei entwickelten Konzepte und Methoden wurden von den medienpädagogischen Fachkräften des LfDI entwickelt; sie wurden auf dem OMEGA-Server des Landes auch für den Medienkomp@ss und sonstige Lehrmethoden für alle Lehrkräfte im Land zur Verfügung gestellt und zwischenzeitlich auch an andere Datenschutzaufsichtsbehörden weitergegeben.

Zur besseren Ergebnissicherung der Workshops wurde ein Flyer („Spickzettel") für die Schülerinnen und Schüler entwickelt https://s.rlp.de/youngdataspickzettel.

Er enthält wichtige Tipps zur Smartphone- und Internetnutzung sowie eine Zusammenstellung wichtiger Links zum Nachlesen.

In Kooperation mit dem Verbraucherschutzministerium und der Verbraucherzentrale Rheinland-Pfalz e.V. wurde das Schülerworkshop-Projekt nunmehr auf Fortbildungsangebote speziell für Familien erweitert. Das neue Vortragsangebot beinhaltet Themen zu Verbraucher- und Datenschutzrisiken in der digitalen Welt.

Die Vorträge sind kostenfrei und können von den Familieneinrichtungen im Land gebucht werden. Das Vortragsangebot umfasst acht Themenmodule, die je nach Interesse frei wählbar sind. Schwerpunkte sind beispielsweise Online-Spiele und Werbung im Internet, Soziale Netzwerke, Urheber- und Persönlichkeitsrechte, Datenspuren im Internet oder BigData sowie das Internet der Dinge. Geschulte Referentinnen und Referenten der Verbraucherzentrale Rheinland-Pfalz e.V. oder des LfDI halten die Vorträge. Weitere Informationen hierzu unter: https://s.rlp.de/datenschutzverbrauchervortrag

8.1.3 Weitere Kooperationen im Bildungsbereich

Der LfDI war mittlerweile zum vierten Mal mit einer großen Zahl seiner Mitarbeiterinnen und Mitarbeiter beim Tag des Datenschutzes der Hochschule der Polizei, um gemeinsam mit den

Dozentinnen und Dozenten der Hochschule den 400 Studierenden des Bachelorstudiengangs ein breites Spektrum an Themen nahezubringen. Das Veranstaltungsformat besteht aus einem Einführungsvortrag des LfDI, einer Reihe von themenorientierten Workshops und einer abschließenden Podiumsdiskussion von Polizei, Studierenden und Datenschützern. Aber auch der zweite Aufgabenbereich des LfDI – die Informationsfreiheit – wird den Polizeianwärterinnen und -anwärtern in den Workshops anhand von Beispielen aus der Anwendungspraxis nahegebracht. Das thematische Spektrum der Workshops reicht vom „Verhaltensknigge" in sozialen Netzwerken über polizeiliche Ermittlungsstrategien im Internet bis hin zu den Auswirkungen der Snowden-Enthüllungen auf die Online-Kommunikation und den bestehenden Möglichkeiten, Datenspuren und die Ausforschung des eigenen Nutzungsverhaltens zu vermeiden.

Mit dem Landessportbund wurden Möglichkeiten zur Sensibilisierung von Sportvereinen und Verbänden insbesondere bei der Veröffentlichung von Fotos auf der Vereinshomepage erörtert. Im Rahmen einer mit dem LfDI abgestimmten Postkartenaktion konnten bei einer Veranstaltung des Sportbundes ca. 350 teilnehmende Kursleiterinnen und -leiter und Trainerinnen und Trainer ihre Kenntnis zum Thema im Wege eines Selbsttests überprüfen.

Mit jugendschutz.net als Kompetenzzentrum von Bund und Ländern für den Jugendschutz im Internet wurden weitere Kooperationsmöglichkeiten ausgelotet. Hier ging es beispielsweise um die Anforderungen, die mit der Europäischen Datenschutz-Grundverordnung im Hinblick auf die Einwilligung von Kindern (vgl. Art. 8 DS-GVO) zu beachten sind. Schwerpunkt des Gedankenaustauschs war aber der Datenschutz bei Spiele-Apps: Mit app-geprüft. net hat jugendschutz.net ein neues Informationsangebot für Eltern und pädagogische Fachkräfte entwickelt, das auf einen Blick wichtige Informationen über Kinder-Apps bietet. Die Seite bewertet mit einem Ampelsystem beliebte Apps auf ihre Eignung für Kinder und zeigt mögliche Risiken, wie In-App-Käufe, Werbung und Schwachstellen im Datenschutz auf. Ergänzend hierzu bietet das mobilfähige Angebot kompass-social.media Jugendlichen Orientierung bei beliebten Online-Diensten wie Instagram, Snapchat und YouTube. Auch hier werden Sicherheitseinstellungen, Meldefunktionen und Datenschutz mit einem Ampelsystem bewertet. Beide Entwicklungen wurden auf der Homepage des LfDI bzw. auf www.youngdata.de verlinkt https://s.rlp.de/schulemedienkompetenz. Darüber hinaus ist eine Zusammenarbeit beim technischen Datenschutz beabsichtigt; hier soll es insbesondere um die Prüfung des sog. Datensendeverhaltens von Spiele-Apps gehen, also der Frage, welche Daten der Kinder (unbemerkt) an den Anbieter weitergeleitet werden.

Durch die Abordnung zweier medienpädagogischer Fachkräfte zum LfDI konnte die enge Kooperation mit medien+bildung.com, einer Tochtergesellschaft der Landeszentrale für Medien und Kommunikation, im Bildungsbereich verstetigt werden. Die Mitarbeit der medienpädagogischen Fachkräfte ist mittlerweile bei den vielseitigen Bildungsaktivitäten des LfDI nicht mehr wegzudenken. Nur so war es möglich, das erste Webinar zum Schuldatenschutz für Lehrkräfte und sonstige im Bildungsbereich Tätige durchzuführen https://s.rlp.de/websds.

Auch in anderen Ländern ist man dem Beispiel aus Rheinland-Pfalz gefolgt und hat Lehrkräfte zu den Datenschutzaufsichtsbehörden abgeordnet, um die Aufklärungsverpflichtungen, die sich nicht zuletzt unmittelbar aus der Europäischen Datenschutz-Grundverordnung ergeben (vgl. Art. 57 Abs. 1 lit. b DS-GVO), auch in pädagogischer Hinsicht zu erfüllen. Ebenfalls

hat sich die Beschäftigung einer FSJ-Kraft bewährt, die von den pädagogischen Fachkräften der Dienststelle betreut wird. Durch die Übernahme von Aufgaben bei der Pflege der gemeinsamen Jugendseite der Datenschutzaufsichtsbehörden des Bundes und der Länder www.youngdata.de und der Organisation des Schülerworkshop-Projektes des LfDI konnten die FSJ-Kräfte zu einer erheblichen Entlastung der sonstigen im Bildungsbereich tätigen Mitarbeiterinnen und Mitarbeitern beitragen. Umgekehrt konnte der LfDI den FSJ-Kräften entscheidende Impulse für deren berufliche Weiterentwicklung geben.

8.2. Digitale Bildung

Mit dem Beschluss der KMK aus dem Jahr 2012 („Medienbildung in der Schule“) sollte eine umfassende Medienkompetenz als Pflichtaufgabe schulischer Bildung nachhaltig verankert werden. „Medienbildung gehört zum Bildungsauftrag der Schule, denn Medienkompetenz ist neben Lesen, Rechnen und Schreiben eine weitere wichtige Kulturtechnik geworden“ heißt es dort. In dem unter Beteiligung der Datenschutzbeauftragten entstandenen Papier beschäftigte sich die KMK erstmals mit der digitalen Bildung und forderte u.a. die Verankerung der Medienbildung in den Lehr- und Bildungsplänen der Länder sowie eine diesen Bedürfnissen entsprechende Lehreraus- und -fortbildung.

Zu einer Evaluation der Umsetzung der hier formulierten Forderungen ist es jedoch nie gekommen, obwohl Studien längst belegen, dass Deutschland bei der digitalen Bildung im internationalen Vergleich regelmäßig auf den hinteren Rängen zu finden ist (z.B. International Computer and Information Literacy Study „ICLIS-Studie“ aus dem Jahr 2014). Die Aktuelle JIM-Studie 2017 zeigt, dass nur sieben Prozent der Schülerinnen und Schüler täglich in der Schule online arbeiten. Gut die Hälfte der Schülerinnen und Schüler gibt an, allenfalls einmal im Monat oder noch seltener in der Schule mit dem Internet zu lernen.

Mit der im Jahr 2016 vorgestellten Strategie „Bildung der digitalen Welt“ unternimmt die KMK den Versuch, die Verbindlichkeit ihrer bildungspolitischen Forderungen zu erhöhen. Die Länder verpflichten sich in dem Beschluss, dass alle Schülerinnen und Schüler, die zum Schuljahr 2018/2019 in die Grundschule eingeschult werden oder in die Sekundarstufe I eintreten, bis zum Ende der Pflichtschulzeit bestimmte, näher definierte digitale Kompetenzen erwerben können. Bis 2021 soll jede Schülerin und jeder Schüler, wenn es aus pädagogischer Sicht im Unterrichtsverlauf sinnvoll ist, eine digitale Lernumgebung und einen Zugang zum Internet haben. Alle Lehrkräfte – so heißt es dort - müssen selbst über eine allgemeine Medienkompetenz verfügen und in ihren fachlichen Zuständigkeiten zu „Medienexperten“ werden; entsprechende Kompetenzen sollen in der fachspezifische Lehrerbildung für alle Lehrämter verbindlich festgelegt werden.

Das Strategiepapier enthält darüber hinaus viele wichtige Handlungsfelder, etwa zum Einsatz digitaler Lernumgebungen und Schulverwaltungssoftware, zur Schulhausvernetzung mit WLAN, zur Nutzung (privater) mobiler Endgeräte, zur Cloudnutzung, zu ID-Management-Systemen sowie zur Zusammenarbeit mit den Datenschutzaufsichtsbehörden.

Auf Landesebene ist Rheinland-Pfalz mit dem Regierungsprogramm „Medienkompetenz macht Schule“ vergleichsweise gut aufgestellt https://medienkompetenz.bildung-rp.de/. Rund 65.000 Lehrkräfte haben in den letzten zehn Jahren an Fortbildungsangeboten zum Einsatz digitaler Medien im Unterricht teilgenommen,

über 2.900 Jugendmedienschutzberaterinnen und -berater wurden qualifiziert und über 2.400 Schülerinnen und Schüler als Medienscouts ausgebildet. Mit einer Fördersumme von annähernd 22 Millionen Euro wurden 580 der weiterführenden Schulen im Rahmen des Landesprogramms mit knapp 13.000 Notebooks und Tablets sowie mit mehr als 1.500 interaktiven Whiteboards zusätzlich ausgestattet. Das Landesprogram wurde zum Schuljahr 2017/2018 auch auf den Primarbereich mit insgesamt 250 Grundschulen ausgeweitet.

Mit Hilfe des „Medienkomp@sses“ können digitale Kompetenzen der rheinland-pfälzischen Schülerinnen und Schüler in den Grund- und weiterführende Schulen dokumentiert und zertifiziert werden, die sich weitgehend mit den im Strategiepapier der KMK formulierten Kompetenzen decken.

Gleichwohl bleibt in Sachen Erhöhung der Verbindlichkeit der KMK-Forderungen auch im Land noch einiges zu tun. Hierfür bietet die Digitalisierungsoffensive der Landesregierung den richtigen Rahmen. Der LfDI hat zur Digitalstrategie der Landesregierung seine Datenschutzforderungen im Bildungskontext formuliert und in verschiedenen Workshops an der Umsetzung mitgearbeitet. Im Übrigen wurden konkrete Datenschutzfragen der digitalen Bildung, soweit diese Rechtsfragen oder datenschutztechnische Aspekte betrafen, gemeinsam mit dem Bildungsministerium erörtert und bewertet. Vieles davon ist in den Flyer zum schulischen Datenschutz mit eingeflossen: https://s.rlp.de/sdsflyer

Das Wirksamwerden der Europäischen Datenschutz-Grundverordnung sowie die in der KMK-Strategie genannten Handlungsfelder werden auch weiterhin eine enge Abstimmung mit dem Bildungsministerium erforderlich machen.

9. KOMMUNALES, MELDEWESEN UND STATISTIK

9.1 Kommunales

9.1.1 Kommunales Datenschutzmanagement – Projekt „Datenschutz update in der Kommunalverwaltung“

Die Wahrung des 1983 durch das Volkszählungsurteil des Bundesverfassungsgerichts geschaffenen Grundrechts auf informationelle Selbstbestimmung ist verfassungsrechtlich geboten. Dementsprechend haben die Verwaltungen von Bund, Ländern und Kommunen im Rahmen des Gesetzesvollzugs die Vorgaben des Datenschutzes zu beachten. Hierbei kommt einem funktionierenden Datenschutzmanagement in den Verwaltungen und insbesondere der Funktion der behördlichen Datenschutzbeauftragten eine zentrale Bedeutung zu.

Ungeachtet dessen stellte der LfDI in der Vergangenheit im Rahmen seiner Beratungs- und Prüfungstätigkeit wiederholt fest, dass die Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben in der Landes- und Kommunalverwaltung im Praxisalltag nicht immer in vollem Umfang gewährleistet werden konnte. Verantwortlich hierfür waren nach Überzeugung des LfDI nicht nur individuelle Mängel bei der Rechtsanwendung, sondern auch strukturelle Defizite beim Datenschutzmanagement innerhalb der Verwaltungen, insbesondere die fehlende oder zu späte Einbindung der behördlichen Datenschutzbeauftragten in datenschutzrelevante Arbeitsprozesse und deren ungenügende Ausstattung mit den zu ihrer Aufgabenerfüllung erforderlichen Zeitressourcen. Trotz der Bedeutung der Funktion der Datenschutzbeauftragten war deren Tätigkeit

im Regelfall weder im Stellenplan der Verwaltungen enthalten noch wurde der Aufgabenumfang quantitativ bemessen. Es überrascht daher nicht, dass bei derartigen Rahmenbedingungen ein beachtliches Verbesserungspotential zur Stärkung des Datenschutzes zu vermuten war.

Da aus Sicht des LfDI den Kommunalverwaltungen aufgrund der Vielzahl der dort zu erfüllenden Sachaufgaben eine besondere Bedeutung zur Sicherstellung des Datenschutzes zukommt, initiierte er im Herbst 2016 ein Projekt zur strukturierten Aufarbeitung der dargestellten Defizite („Datenschutz-update in der Kommunalverwaltung"). Ziel war es, gemeinsam mit vier ausgewählten Kommunalverwaltungen aus unterschiedlichen Bereichen (Landkreis, kreisfreie Stadt, große kreisangehörige Stadt, Verbandsgemeinde) die wesentlichen Hürden bei der Beachtung des Datenschutzes im Verwaltungsalltag zu identifizieren und darauf aufbauend praktikable und inhaltlich abgestimmte Empfehlungen zur Stärkung des Datenschutzes und zur Verbesserung des Datenschutzmanagements zu entwickeln. Durch die Einbindung der in Größe und Aufgabenspektrum unterschiedlichen Kommunalverwaltungen war bereits im Projektkonzept gewährleistet, daraus resultierende Unterschiede im kommunalen Datenschutzmanagement von Anfang an zu berücksichtigen und ggf. darauf basierende differenzierte Empfehlungen treffen zu können. Schließlich sprach für die Durchführung des Projekts auch die Tatsache, dass mit den erwarteten Hilfestellungen zur Verbesserung des kommunalen Datenschutzmanagements bereits frühzeitig ein Beitrag zur Vorbereitung der Verwaltungen auf die Anforderungen der Europäischen Datenschutz-Grundverordnung geleistet werden konnte, die im Mai 2018 wirksam werden wird.

Mit einer Fachveranstaltung im Juni 2017 und der Vorlage von Best-Practice-Empfehlungen zur Stärkung des Datenschutzes in der Kommunalverwaltung (https://s.rlp.de/datenschutz-kommunalverwaltung) konnte der LfDI das von ihm initiierte Projekt erfolgreich beenden. Die erarbeiteten Empfehlungen zeigen den Kommunalverwaltungen insbesondere Wege auf, wie sie die regelmäßig bei ihnen geschaffene Funktionen des Datenschutzbeauftragten besser nutzen und in die Verwaltungsabläufe einbinden können. Zugleich enthalten die Papiere auf die Praxis ausgerichtete Überlegungen, wie die zur Wahrung von Datenschutz und Datensicherheit in der Verwaltung benötigten personellen Ressourcen angemessen quantifiziert werden können. Hierzu dient insbesondere der in dem Projekt gemeinsam erarbeitete und bundesweit wohl erstmalige Vorschlag zur Stellenbemessung und Stellenbewertung kommunaler Datenschutzbeauftragter.

Die Best-Practice-Empfehlungen des LfDI zur Stärkung des Datenschutzes in der Kommunalverwaltung befassen sich mit folgenden Inhalten:

1. Rahmenbedingungen für die Ausübung der Funktion der/des Datenschutzbeauftragten

2. Kriterien für die Auswahl einer/eines Datenschutzbeauftragten

3. Unterstützung der/des Datenschutzbeauftragten bei der Aufgabenwahrnehmung

4. Qualitätsmerkmale für die Tätigkeit der/des Datenschutzbeauftragten

5. Kommunikation und Netzwerkarbeit

6. Nachhaltigkeit des Datenschutzes in der Kommunalverwaltung

In den einzelnen Bereichen werden abstrakt verschiedene Handlungsziele formuliert, die zur Gewährleistung eines angemessenen Datenschutzniveaus erreicht werden sollten. Daran anknüpfend enthalten die Empfehlungen konkrete Praxisbeispiele, die den Verwaltungen einzelne Schritte auf diesem Weg aufzeigen. Es bleibt selbstverständlich in der Verantwortlichkeit jeder Kommunalverwaltung und der dort tätigen Datenschutzbeauftragten zu entscheiden, ob und ggf. welche der beschriebenen Ziele mit welchen Methoden erreicht werden sollen.

Neben dem Hauptpapier wurden in einigen Bereichen noch zusätzliche erläuternde oder vertiefende Papiere erarbeitet, die als Anlagen den Best-Practice-Empfehlungen beigefügt sind. Im Einzelnen handelt es sich um:

› Papier zur Stellenbemessung und Stellenbewertung der Funktion der kommunalen Datenschutzbeauftragten

› Orientierungshilfe zu den Aufgaben der behördlichen Datenschutzbeauftragten in der rheinland-pfälzischen Kommunalverwaltung

› Papier zu den Kooperationsmöglichkeiten von Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen bei der Ausübung der Funktion der Datenschutzbeauftragten

› Papier zum Anforderungsprofil für kommunale Datenschutzbeauftragte

› Übersicht zum „Starterkit“ für neue Datenschutzbeauftragte

Die Best-Practice-Empfehlungen basieren auf dem zum Zeitpunkt ihrer Veröffentlichung geltenden Rechtsrahmen. Der LfDI wird die Papiere bis zum Wirksamwerden der Europäischen Datenschutz-Grundverordnung im Mai 2018 an die neue Rechtslage anpassen.

Dem LfDI war es von Anfang an ein wichtiges Anliegen, sowohl die kommunalen Spitzenverbände als auch die Landesregierung sowie den Landesrechnungshof in das Projekt einzubinden. Dementsprechend würdigten bei der öffentlichen Vorstellung der Best-Practice-Empfehlungen im Juni 2017 auch das Innenministerium sowie ein Vertreter der kommunalen Spitzenverbände die Projektarbeit ausdrücklich. Im Herbst 2017 kam es zudem zu einem ersten Gespräch des LfDI mit dem Landesrechnungshof, um eine einvernehmliche Position zu den für ein angemessenes Datenschutzmanagement in den Kommunen erforderlichen Rahmenbedingungen zu erreichen.

Angesichts der im Mai 2018 wirksam werdenden Europäischen Datenschutz-Grundverordnung, die die Verwaltungen als Ganzes zur Sicherstellung von Datenschutz und Datensicherheit verpflichtet, sind die vorgelegten Empfehlungen eine wichtige Grundlage für die Kommunalverwaltungen, sich auf die anstehende Rechtsänderungen vorzubereiten. Vor dem Hintergrund, dass Datenschutz unbestritten weiterhin Grundrechtsschutz ist und dessen Sicherstellung gerade von den Verwaltungen zu Recht eingefordert wird, ist der LfDI zuversichtlich, dass sich das mit den Empfehlungen verbundene Anliegen erfüllt.

9.1.2 Entsorgung von Altakten im Fußballstadion

Zuschauer eines Fußballspieles verstreuten aus Altakten einer Kommunalverwaltung teils komplett erhaltene, teils nachlässig zerrissene Seiten als Konfetti. Darauf waren personenbezogene Daten von Bürgerinnen und Bürgern gut lesbar.

Dazu konnte es kommen, weil die zuvor nach Ablauf der Aufbewahrungsfrist zur Vernichtung aussortierten Akten in Müllsäcken ohne Kennzeichnung als schutzbedürftiger Papiermüll nicht ausreichend gesichert zwischengelagert wurden. Dadurch konnte ein Mitarbeiter der Verwaltung eine größere Menge Altpapier an sich nehmen, um sie als Wurfmaterial im Stadion zu verwenden. Die datenschutzrechtliche Relevanz des Inhaltes der Papiere wurde von dem Mitarbeiter nicht erkannt.

Somit wurden personenbezogene Daten nach Ablauf der Aufbewahrungsfrist (§ 19 Abs. 2 LDSG) ohne Grundlage bzw. Erlaubnis Dritten – insbesondere den Zuschauern des Fußballspieles - gegenüber in sonstiger Weise offenbart, weil technisch-organisatorische Vorgaben, die verhindern, dass Unbefugte auf diese Daten zugreifen können, missachtet und zumindest nicht ausreichend geregelt und dokumentiert waren. So fehlte auch ein schriftlicher Vertrag zwischen der Kommune als Auftraggeberin und einem externen Dienstleister für die Aktenvernichtung.

Der LfDI hat gegenüber der Kommune eine Beanstandung, d.h. eine förmliche Missbilligung von Datenschutzverstößen ausgesprochen. Die Verwaltung hat Maßnahmen zur Verbesserung der Abläufe – u.a. dezentrale, datenschutzkonforme Entsorgung von Papiermüll – und zur weiteren Sensibilisierung der Beschäftigten in Datenschutzfragen ergriffen.

Die Ursachen dieses Vorfalls bestätigen zentrale Aussagen der Best Practice-Empfehlungen (vgl. „Kommunalprojekt unter I.....) des LfDI zur Stärkung des kommunalen Datenschutzmanagement.

Als weitere Konsequenz aus diesem Vorfall und auch im Hinblick auf die Anforderungen der Europäischen Datenschutz-Grundverordnung hat sich die Kommunalverwaltung auch dazu entschlossen, im Stellenplan eine Stabsstelle mit 50 Prozent Zeitanteil einer Vollzeitstelle auszuweisen. Dieser Stabsstelle werden die Aufgaben des behördlichen Datenschutzbeauftragten und des Informationssicherheitsbeauftragten übertragen.

Auch dieser Entschluss ist ganz im Sinne der o.g. Empfehlungen.

9.1.3 Regionaltreffen mit den behördlichen Datenschutzbeauftragten

Die Treffen mit den behördlichen Datenschutzbeauftragten sollen es dem LfDI einerseits ermöglichen, diesen Personenkreis zeitnah mit datenschutzrechtlichen Anliegen ansprechen zu können. Anderseits dienen sie dem Gedankenaustausch zwischen LfDI und behördlichen Datenschutzbeauftragten sowie auch untereinander, sodass jeder vom Wissen und Können der anderen profitieren kann.

Seit 2007 hatte die Dienststelle des LfDI die behördlichen Datenschutzbeauftragten der Kommunen einmal jährlich zu einer Tagung eingeladen, die den o.g. Zwecken diente. Auf Anregung verschiedener behördlicher Datenschutzbeauftragter hin hat sich der LfDI für die Zeit ab 2017 dazu entschieden, anstelle der einmaligen jährlichen Tagung mehrere regionale Tagungen pro Jahr anzubieten. Mit der Verkürzung des Anfahrtsweges bzw. der Auswahl unter mehreren Terminen sollen noch mehr behördliche Datenschutzbeauftragte über die einzelnen Treffen in unterschiedlichen Regionen von Rheinland-Pfalz erreicht und auch weitere Beschäftigte aus den Kommunalverwaltungen für die Treffen interessiert und damit für den Datenschutz sensibilisiert werden.

Die Veranstaltungen fanden statt im Januar 2017 in Bad Neuenahr-Ahrweiler, Kreisverwaltung Ahrweiler, im April 2017 in Mainz, Kommunale Datenzentrale der Landeshauptstadt Mainz, und im November 2017 in Landstuhl bei der dort ansässigen Verbandsgemeindeverwaltung. Allen Kommunalverwaltungen an dieser Stelle nochmals herzlichen Dank für die Gastfreundschaft und die damit verbundene Unterstützung des LfDI.

Als Ziel wurden 100 Teilnehmerinnen und Teilnehmer an den drei Treffen ausgegeben. Diese Zahl wurde leicht übertroffen und erfreulicherweise auch mehr als zwei Dutzend Kommunalverwaltungen erreicht, die noch nie oder seit 2007 nur einmal mit einem Vertreter an den Tagungen teilgenommen haben. Das inhaltliche Feedback, das die Referentin und zwei Referenten des LfDI von den Veranstaltungen jeweils mitnahmen, gestaltet sich positiv. Zudem wird das neue Format auch intensiver zur Diskussion und zum Austausch genutzt.

Allerdings gibt es immer noch zahlreiche Kommunalverwaltungen, insbesondere Verbandsgemeindeverwaltungen, die noch auf keiner der Tagungen vertreten waren. Die Gründe hierfür wurden vom LfDI bislang noch nicht ermittelt. Denkbar ist, dass diese öffentlichen Stellen den jeweiligen behördlichen Datenschutzbeauftragten nicht ausreichend bei der Erfüllung seiner Aufgaben unterstützen (§ 11 Abs. 5 S. 1 LDSG), mit anderen Worten ihm nicht den benötigten Anteil an der wöchentlichen Arbeitszeit für die Erledigung der Aufgaben des Datenschutzbeauftragten zur Verfügung stellen bzw. einräumen. Zu dem Umfang des Personalbedarfs hat sich der LfDI in seinen Best-Practice-Empfehlungen zum Datenschutz in der Kommunalverwaltung geäußert (vgl. …).

Die Reihe an Informationsveranstaltungen wird daher auch 2018 fortgesetzt werden. Thematisch wird der Schwerpunkt dieser Regionaltreffen aus gegebenem Anlass noch stärker auf Informationen zur Anwendung der Europäischen Datenschutz-Grundverordnung liegen.

9.1.4 Rats- und Bürgerinformationssystem

Sitzungsvorlagen aus den Fachbereichen einer Verwaltung zur Vorbereitung der Mandatsträgerinnen und -träger auf eine Sitzung bzw. für eine Beschlussfassung während einer Sitzung enthalten mitunter personenbezogene Daten, d.h. Einzelangaben über persönliche oder sachliche Verhältnisse einer identifizierten oder identifizierbaren natürlichen Person.

Der Name und das Geburtsdatum sind eine Person direkt identifizierende Daten. Bei einer Flurstücksnummer, einer Anschrift, einem Kfz-Kennzeichen, einem Bildnis oder einem Orthofoto kann die betroffene Person mit Zusatzwissen indirekt identifiziert werden. Auch eine Verknüpfung mehrerer sog. personenbeziehbarer Daten wie z.B. Staatsangehörigkeit, Alter, Körpergröße oder Geschlecht kann zur Identifizierung einer Person führen.

9.1.4.1. Ratsinformationssystem für die Mandatsträgerinnen und -träger

Hier soll anhand verschiedener Sachverhalte im Kontext einer öffentlichen Sitzung beispielhaft dargestellt werden, von welchen personenbezogenen Daten die Kenntnisnahme durch Mandatsträgerinnen und -träger zur Erledigung der übertragenen Aufgaben erforderlich ist; mit anderen Worten, welche personenbezogenen Daten in Sitzungsvorlagen aus den Fachbereichen zur Vorbereitung auf eine Sitzung bzw. für eine Beschlussfassung während einer Sitzung aus datenschutzrechtlicher Sicht enthalten sein dürfen, aber gleichzeitig sachgerecht

entschieden werden kann. Bei schwierigen Entscheidungsgegenständen oder Angelegenheiten von größerer Bedeutung geschieht eine Information bereits im Vorfeld einer Sitzung durch schriftliche Vorlagen. Bei einfachen Sachverhalten kann eine mündliche Erläuterung oder Verlesen der Vorlage während der Sitzung ausreichend sein.

Diese Vorgaben werden auch in der Datenschutz-Grundverordnung getroffen. Gemäß Art. 5 Abs. 1 lit. c DS-GVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"). Weiterhin ist die Verarbeitung solcher Daten gemäß Art. 6 Abs. 1 lit. e DS-GVO u.a. dann zulässig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Überhaupt gilt für Sitzungen kommunaler Gremien das „Mündlichkeitsprinzip", d.h. es besteht keine Rechtspflicht zur Übersendung bzw. Bereitstellung von Unterlagen zur Vorbereitung auf eine Gremiensitzung. Daraus kann als Faustregel abgeleitet werden, dass je sensibler die für die Beratung eines Tagesordnungspunktes benötigten Informationen sind, diese desto stärker räumlich einzuengen sind. Im Zweifel kommt nur ein mündlicher Sachvortrag in Betracht, ergänzt durch eine schriftliche, jedoch im Sitzungsraum verbleibende Tischvorlage.

Dieser Grundsatz darf auch bei der Erstellung von Vorlagen sowie der Bereitstellung ergänzender Unterlagen für in nicht-öffentlicher Sitzung beratene Angelegenheiten nicht außer Acht gelassen werden. Findet beispielsweise zur Besetzung einer Stelle unter den Bewerbern eine Vorauswahl durch das Personalamt und den Personalrat statt, dürfte für die Beratung und Entscheidung im Personalausschuss die Bereitstellung eines Besetzungsberichts an die Mitglieder des Ausschusses genügen.

Zu den in die engere Auswahl genommenen Bewerberinnen und Bewerbern könnte ergänzend insbesondere noch der Lebenslauf zur Vorbereitung auf eine Sitzung zur Verfügung gestellt werden. Die Offenbarung darüber hinausgehender Informationen, wie Zeugnisse jeglicher Art, zu Bewerberinnen und Bewerbern kann wegen der kritisch zu sehenden Freiwilligkeit grundsätzlich nicht auf deren Einwilligung gestützt werden.

9.1.4.2. Einwendungen von Bürgerinnen und Bürgern zu einem Bebauungsplanentwurf und Öffentlichkeits-beteiligung

Bauleitpläne sind ihrer Natur nach von der Gemeindevertretung in öffentlicher Sitzung zu beraten und zu beschließen. Bei der Aufstellung von Bauleitplänen sind die öffentlichen und privaten Belange gegen- und untereinander gerecht abzuwägen (§ 1 Abs. 7 BauGB). In Verbindung dazu regelt § 4a Abs. 1 BauGB als vorrangigen Zweck der Öffentlichkeits- und Behördenbeteiligung, dass die von der Planung berührten Belange vollständig ermittelt und zutreffend bewertet werden.

Deshalb lässt es sich zur Feststellung der Betroffenheit einer Bürgerin bzw. eines Bürgers von der Planung oder zur Gewichtung einer geäußerten Anregung oder Einwendung mitunter nicht vermeiden, dass Stellungnahmen aus der Öffentlichkeitsbeteiligung den Mandatsträgern personenbezogen vorgelegt werden.

Auch wenn der Gesetzgeber mit § 3 BauGB die grundsätzliche Entscheidung über den Vorrang der Bürgerbeteiligung vor dem Daten-

schutz getroffen hat, ist eine pauschale oder zwangsläufige Nennung des Namens sowie des Wohnortes eines Einwenders ohne vorherige Interessenabwägung aber unzulässig. Eine Einwendung darf nur dann personenbezogen vorgelegt werden, wenn die Belange der Öffentlichkeitsbeteiligung die Erfordernisse des Datenschutzes überwiegen.

Die aus einem Bebauungsplanentwurf ersichtlichen Flurstücknummern als personenbeziehbare Daten hinsichtlich der Grundstückseigentümer sind unkritisch bzw. dürfen offengelegt werden.

9.1.4.3. Abweichung von textlichen Festsetzungen eines Bebauungsplanes

In der Sitzungsvorlage dürfen im Rahmen des Sachverhalts neben dem Namen des Bebauungsplanes auch Flurstücknummer und Anschrift zum Grundstück genannt werden. Da ggf. die Umgebungsbebauung in die Beurteilung des Antrages einbezogen werden muss, handelt es sich um für die Entscheidung des Gremiums relevante Umstände. Die Angabe des Namens der Eigentümerinnen und Eigentümern bzw. Antragstellenden ist dagegen grundsätzlich nicht notwendig.

9.1.4.4. Einwohnerfragestunde

Nach der Mustergeschäftsordnung für Gemeinderäte sollen Anfragen für eine Einwohnerfragestunde der Bürgermeisterin oder dem Bürgermeister grundsätzlich rechtzeitig vor der Sitzung schriftlich zugeleitet werden, damit eine entsprechende Vorbereitung zur sachgerechten Beantwortung erfolgen kann. Damit ist nicht ausgeschlossen, dass auch die Mandatsträgerinnen und -träger zur Vorbereitung auf die Sitzung solche Anfragen als Sitzungsvorlage erhalten. Denn die Fraktionen sind berechtigt, zur Antwort der Bürgermeisterin oder des Bürgermeisters Stellung zu nehmen.

Fraglich ist nun, welche Daten zur Person der Bürgerin bzw. des Bürgers in diesem Zusammenhang notwendigerweise in der Sitzungsvorlage zur Erfüllung der gesetzlich vorgesehenen Aufgabe zu nennen sind.

Zweck der Fragestunde ist nicht eine Diskussion des Bürgers mit dem Gremium oder dem Bürgermeister, sondern die Beantwortung von Fragen oder die Entgegennahme von Anregungen und Vorschlägen. Deshalb sollte aus datenschutzrechtlicher Sicht zur Vorbereitung auf die Erledigung einer Anfrage im Rahmen der Einwohnerfragestunde grundsätzlich ein Hinweis wie z.B. „Frage aus der Bürgerschaft“ genügen.

9.1.5 Bürgerinformationssystem

Bei der Bereitstellung von Informationen aus der Gremienarbeit im Internet handelt es sich - wenn personenbezogene Daten enthalten sind - um eine Offenlegung auch an nicht-öffentliche Stellen, da auf diesen Teil des Systems weltweit von einem unbestimmten Personenkreis zugegriffen werden kann. Die Voraussetzungen allgemeiner und spezieller datenschutzrechtlicher Regelungen liegen häufig nicht vor, weil die Aufgabenerfüllung der Kommune eine beliebige Datenweitergabe nicht erfordert, auch wenn damit die Transparenz im kommunalen Verwaltungshandeln weiter gefördert werden soll.

Denn das Kommunalverfassungsrecht sieht regelmäßig nur eine lokal begrenzte Öffentlichkeit vor. Dagegen erreicht der Verbreitungsgrad der Informationen im Medium Internet

einen deutlich höheren Umfang als dies bei einer Veröffentlichung z.B. in einem Amtsblatt, einer regionalen Tageszeitung oder im Verlauf einer öffentlichen Gremiensitzung der Fall ist. Bei dieser weltweiten Übermittlung von Daten sind die Vervielfältigungsmöglichkeiten, Suchmaschinen und die nicht endliche Datenverarbeitung im Internet zu berücksichtigen.

Mit Hilfe von Suchmaschinen wird eine elektronische Auffindbarkeit möglich, die es erlaubt, sämtliche zu den betroffenen Personen vorhandenen Angaben zu sammeln und – losgelöst vom ursprünglichen Informationszweck – zur Erstellung eines Persönlichkeitsprofils zu nutzen. Über die Archivfunktion von Suchmaschinen sind die Daten häufig auch dann noch abrufbar, wenn die Angaben aus dem Internet-Angebot der Verwaltung bereits entfernt oder geändert wurden. Im Gegensatz zu einer Veröffentlichung über ein herkömmliches Medium ist darin eine andere Qualitätsstufe des Eingriffs in das Recht auf informationelle Selbstbestimmung zu sehen.

Die Einholung von Einwilligungen der Betroffenen ist teilweise wenig praktikabel, weshalb vor der Veröffentlichung von Dokumenten im Internet das Augenmerk besonders auf dem Grundsatz der Datenminimierung liegen muss und ggf. alle personenbezogenen Daten aus den Vorlagen bzw. Niederschriften zu entfernen oder zu anonymisieren sind.

9.1.5.1. Einwendungen von Bürgerinnen und Bürgern zu einem Bebauungsplanentwurf

Der Gesetzgeber hat zwar mit § 3 BauGB die grundsätzliche Entscheidung zum Vorrang der Bürgerbeteiligung vor dem Datenschutz zugunsten einer Transparenz der gemeindlichen Verwaltungstätigkeit getroffen.

Aus der personenbezogenen Beratung von Einwendungen in öffentlicher Sitzung ergibt sich jedoch nicht die Zulässigkeit einer personenbezogenen Veröffentlichung im Internet. § 4a Abs. 4 Satz 1 und Satz 2 BauGB, der die Einstellung gewisser Inhalte in das Internet vorsieht, erfasst diese Daten nicht.

Für eine bloße Information der Bürgerinnen und Bürger, in welcher Weise das Gremium über die Anregungen und Einwendungen beschlossen hat, ist es nicht erforderlich, diese unter Angabe von Name und Anschrift der Einwenderin oder des Einwenders bekannt zu machen.

Eine Veröffentlichungsbefugnis von (auch digitalisierten und georeferenzierten) Bebauungsplänen ist wegen der darin enthaltenen personenbeziehbaren Flurstücknummern in § 10a Abs. 2 BauGB zu sehen.

9.1.5.2. Sitzungsniederschrift

Die Veröffentlichung der Niederschrift mit dem gesetzlichen Mindestinhalt (§ 41 Abs. 1 Satz 2 GemO) ist zulässig.

Die Veröffentlichung einer Sitzungsniederschrift im Internet stellt aber dann eine Datenübermittlung i.S. des Datenschutzrechts dar, wenn davon auch personenbezogene Daten betroffen sind.

§ 41 Abs. 5 GemO sieht vor, dass die Verwaltung die Einwohnerinnen und Einwohner über die Ergebnisse der Ratssitzungen in geeigneter Form unterrichten soll. Dies kann aber nur innerhalb dem von § 35 Abs. 1 GemO vorgegebenen Rahmen erfolgen. Zudem bezieht sich diese Pflicht der Verwaltung nach der dazu ergangenen Verwaltungsvorschrift nur auf den sachlichen Inhalt der für die Einwohnerinnen

und Einwohner wichtigen Ratsbeschlüsse (z. B. Beschlüsse über Satzungen, Bauleitpläne, Erhebung oder Änderung von Abgaben, Planung wichtiger Bauvorhaben). Vielmehr ist die Veröffentlichung des Wortlauts der Sitzungsniederschrift in der Regel als Mittel zur Unterrichtung der Einwohner ungeeignet.

Zur Erfüllung dieser Aufgabe durch die Kommune ist es jedenfalls nicht erforderlich, personenbezogene Daten zu verarbeiten. Mit anderen Worten, eine Fassung der Niederschrift, mit der die Pflicht zur Veröffentlichung aus § 41 Abs. 5 GemO erfüllt werden soll, muss grundsätzlich so formuliert sein, dass keine personenbezogenen Daten aufgeführt werden.

Auch wenn über den gesetzlichen Mindestinhalt hinaus auf der Grundlage einer Mehrheitsentscheidung mit § 26 Abs. 1 der Mustergeschäftsordnung auch die Namen von unentschuldigt fehlenden Mandatsträgerinnen und -trägern protokolliert werden dürfen, sollte auf diese Information bei der Veröffentlichung im Internet wegen der grundsätzlich möglichen Profilbildung verzichtet werden.

Laut § 26 Abs. 1 Satz 2 Nr. 9 der Mustergeschäftsordnung muss die Niederschrift beispielsweise auch den Verlauf einer Einwohnerfragestunde wiedergeben. Dabei ist zu berücksichtigen, dass zwar eine anonyme Fragestellung vom Gesetz nicht vorgesehen ist, wenn eine Einwohnerin oder ein Einwohner während der Einwohnerfragestunde selbst und unmittelbar das zur Sprache bringt, was sie oder ihn in eigener Person oder als Mitglied der örtlichen Gemeinschaft berührt, d.h. sie oder er nennt den Namen und dieser kann vom Schriftführer auch protokolliert werden.

Der Name darf in der Fassung der Niederschrift für das Internet aber nicht enthalten sein, weil dies im Hinblick auf den genannten Zweck einer Veröffentlichung nicht erforderlich ist.

Überhaupt ist schon die Führung der Niederschrift als Ergebnisprotokoll durch die Grundsätze der Sparsamkeit und Wirtschaftlichkeit geboten. Auch deshalb sollte davon abgesehen werden, Wortprotokolle und Protokollierungen des Abstimmungsverhaltens einzelner Mandatsträgerinnen und -träger zu erstellen und im Internet zu veröffentlichen.

Schließlich kann sich eine Verwaltung auch nicht auf § 41 Abs. 4 GemO stützen, da diese Vorschrift lediglich ein Einsichtsrecht der Einwohnerinnen und Einwohner in die Niederschrift öffentlicher Sitzungen eröffnet und gerade keine Befugnis der Verwaltung, diese zu veröffentlichen.

9.1.5.3. Stellenplan

§ 97 Abs. 1 Satz 1 GemO schreibt vor, dass der Entwurf der Haushaltssatzung mit dem Haushaltsplan und seinen Anlagen nach Zuleitung an den Gemeinderat bis zur Beschlussfassung zur Einsichtnahme durch die Einwohner verfügbar zu halten ist. Laut der Gesetzesbegründung bleibt es der Gemeinde überlassen, ob sie den Entwurf in herkömmlicher Weise als Druckwerk auslegt, im Internet verfügbar macht oder in sonstiger Weise ihren Einwohnern zur Einsichtnahme zur Verfügung stellt.

Ein Bestandteil des Haushaltsplanes ist der Stellenplan (§ 96 Abs. 4 Nr. 4 GemO). Wenn darin auch zumindest personenbeziehbare Angaben zu Teilzeit, Altersteilzeit, Entgeltgruppe, Dienstunfähigkeit, Elternzeit, Besuch des Angestelltenlehrganges o.ä. mit Abwesenheit in Zusammenhang stehende Informationen enthalten sind, sollten im Hinblick auf die eingangs getätigten Ausführungen zum Verbreitungsgrad von Informationen im Internet und dem

Grundsatz der Datensparsamkeit Vorkehrungen zum Schutz solcher Informationen getroffen werden und ggf. der Stellenplan nicht oder nur in einer angepassten Fassung im Internet veröffentlicht werden.

Im Übrigen enthält die Gesetzesbegründung zu § 97 Abs. 1 GemO keine Hinweise darauf, dass für eine bürgerfreundliche und transparente Gestaltung des Aufstellungsverfahrens des gemeindlichen Haushalts die genannten Dokumente für die Einsichtnahme durch Einwohnerinnen und Einwohner verfügbar zu halten sind.

9.1.6 Bekanntmachung der Tagesordnung des Bauausschusses

Bauherren stellten einen Antrag auf Zustimmung zur Abweichung von den textlichen Festsetzungen des geltenden Bebauungsplanes bezüglich der Errichtung eines Gara¬gendaches an ihrem Wohnhaus. In der der lokalen bzw. über die Online-Ausgabe des Amtsblat¬tes bekanntgemachten Tagesordnung für die öffentliche Sitzung des Planungs- und Bauausschusses der Gemeinde wurde zusätzlich zur Flurstücknummer auch die Wohnanschrift und somit personenbezogene Daten der Bauherren genannt. Diese Vorgehensweise haben sie gegenüber dem LfDI problematisiert.

Die Verwaltung führte dazu u.a. aus, dass Flurstücknummer, Straße und Hausnummer in der Einladung genannt wurden, weil diese Angaben bei der Beurteilung des Antrages eine Rolle spielen. Bei den Entscheidungen über Einvernehmenserteilungen oder Abweichungsanträge seien immer auch die Umgebungsbebauung und die Auswirkungen des zu beurteilenden Vorhabens auf die Nachbargrundstücke zu berücksichtigen. Deren Eigentümer könnten über die Anschrift in der Einladung unschwer erkennen, um welches Bauvorhaben es sich handele. Die Nennung der Flurstücknummer sei nicht ausreichend, da diese kaum bekannt sei.

Gemäß § 34 Abs. 6 Satz 1 GemO ist die Tagesordnung für die Sitzung eines Gremiums öffentlich bekannt zu machen. Ziel der Regelung ist es u.a., den Bürgerinnen und Bürgern der jeweiligen Kommune zum Zweck der demokratischen Kontrolle und Teilhabe Einblick in die Tätigkeit kommunaler Vertretungskörperschaften zu gewähren.

Der LfDI vertritt den Standpunkt, dass es zur Erledigung dieser Aufgabe grundsätzlich nicht erforderlich ist, personenbezogene Daten zur weiteren Konkretisierung eines Tagesordnungspunktes zu übermitteln. Erforderlichkeit heißt, dass die Kenntnisnahme bestimmter personenbezogener Daten unabdingbar sein muss, damit die Mandatsträgerin bzw. der Mandatsträger die ihr bzw. ihm übertragenen Aufgaben erfüllen bzw. die Bürgerinnen und Bürger an den kommunalen Entscheidungsprozessen entsprechend teilhaben können. Dem Grunde nach hat also eine Entscheidung im Einzelfall zu erfolgen.

Im Hinblick auf den Zweck, den die Tagesordnung zu erfüllen hat, muss ein Punkt so spezifiziert werden, dass die Eingeladenen sich auf die Behandlung der Beratungsgegenstände hinreichend einstellen können. Unter Beachtung des Grundsatzes der Erforderlichkeit genügt es, wenn Antragsgegenstand und Name des Bebauungsplanes genannt werden. Die Mitglieder eines Gremiums erhalten weitere Informationen von der Verwaltung über interne Beschlussvorlagen. Antragstellende müssen daher nicht damit rechnen, dass ihre volle Anschrift der Öffentlichkeit zugänglich gemacht wird.

Zumal Mandatsträgerinnen und Mandatsträger auch in nicht-öffentlicher Sitzung von perso-

nenbezogenen Daten grundsätzlich nur in dem Maß Kenntnis erhalten dürfen, wie es zur abschließenden Beratung eines Tagesordnungspunktes erforderlich ist.

Wegen der grundsätzlichen Bedeutung wurde auch das zuständige Ministerium eingebunden. Es führt dazu aus, dass die Tagesordnung, die den Ratsmitgliedern nach § 34 Abs. 2 Satz 1 GemO mit der Einladung zu übersenden ist, nicht wörtlich mit der nach § 34 Abs. 6 GemO zu veröffentlichenden Tagesordnung übereinstimmen müsse, sondern konkreter gefasst sein könne.

§ 34 Abs. 6 GemO (bei Ausschusssitzungen i.V.m. § 46 Abs. 5 Satz 1 GemO) diene dem Grundsatz der Sitzungsöffentlichkeit nach § 35 Abs. 1 GemO. Erforderlich sei daher die öffentliche Bekanntmachung einer hinreichend aussagekräftigen Tagesordnung. Insbesondere zum Schutz personenbezogener Daten habe der Gesetzgeber die Möglichkeit eröffnet, eine weniger detaillierte Tagesordnung zu veröffentlichen, ohne dabei den Grundsatz der Sitzungsöffentlichkeit zu beeinträchtigen.

Außerdem hätten die Regelungen über die Tagesordnung von Gremiensitzungen keine nachbarschützende Wirkung. Schließlich diene § 34 Abs. 2 Satz 1 GemO der Information und Vorbereitung der Ratsmitglieder, damit diese in der Sitzung nicht mit unvorhergesehenen Beratungsgegenständen konfrontiert würden. Eine erforderliche detailliertere Information könne über entsprechende Sitzungsunterlagen erfolgen.

Konkret führt das Ministerium aus, dass bei der Einvernehmenserteilung der Gemeinde nach § 36 Abs. 1 BauGB in der Regel die Benennung des Bebauungsplans, bei Anträgen nach § 31 BauGB und bei Anträgen bzgl. des unbeplanten Innenbereichs nach § 34 BauGB die Nennung des Straßennamens (und zwar unabhängig von der Länge der Straße) genüge. Ein konkrete Betroffenheit müsse eine einzelne Person nicht aus der nach § 34 Abs. 6 GemO öffentlich bekanntzumachenden Tagesordnung für eine Gemeinderats- oder Ausschusssitzung über die Angabe von Flurstücks- oder Hausnummer ableiten können.

Die Verwaltung hat sich dem von Ministerium und LfDI vertretenen Standpunkt angeschlossen.

9.2 Meldewesen

9.2.1 Bundesmeldegesetz und die Anpassung auf Landesebene

Mit dem Bundesmeldegesetz sind die Online-Abrufmöglichkeiten durch andere öffentliche Stellen gegenüber der bisherigen (landesrechtlichen) Regelung erweitert worden. So ist mit § 38 Abs. 1 BMG die Zulässigkeit einer bundesweiten „einfachen Behördenauskunft“ eingeführt worden. Der Datensatz, der dabei zum länderübergreifenden Abruf zur Verfügung steht, besteht aus folgenden Informationen: Familienname, frühere Namen, Vornamen, Ordensname, Künstlername, Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch der Staat, Doktorgrad, derzeitige Anschriften oder Wegzugsanschrift sowie Sterbedatum und Sterbeort. Ebenfalls wurde die Zulässigkeit bundesweiter Abfragen durch Sicherheitsbehörden mit einem erweiterten Datenkatalog eingeführt. § 38 Abs. 3 BMG verpflichtet die Meldebehörden, Daten für Sicherheitsbehörden und sonstige durch Bundes- und Landesrecht bestimmte öffentliche Stellen „rund um die Uhr“ zum Abruf bereitzuhalten (§ 39 Abs. 3 BMG).

Damit ist nicht nur der Kreis der abrufberechtigten Personen und Stellen exponentiell angestiegen und für die Betroffenen unüberschaubar erweitert worden, sondern auch die Möglichkeit obsolet geworden, auf Landesebene Online-Abrufe regional einzuschränken. Jedwede landesrechtliche Erweiterung der bereits bundesrechtlich bestehenden Abrufmöglichkeiten bedarf daher einer eingehenden Prüfung nach dem Grundsatz der Verhältnismäßigkeit.

Eine datenschutzrechtliche Bewertung der landesrechtlichen Regelungen hat dabei zu berücksichtigen, dass das Missbrauchspotenzial mit der Erweiterung des Datenkataloges und der abrufberechtigten Personen und Stellen in erheblichem Umfang noch weiter ansteigen wird. Wie die Protokollauswertungen in der Vergangenheit (vgl. 21. Tb., Tz. 4.2), Eingaben beim LfDI und aktuelle Rechtsprechung (Massenhafte Abrufe von Meldedaten durch Bürgeramtsmitarbeiterin - Landesarbeitsgericht Berlin-Brandenburg, Urteil vom 13 April 2017, Az. 10 Sa 154/17) belegen, werden Abfragen aus dem Melderegister in einem nicht unerheblichen Umfang auch für private Zwecke und aus Neugier vorgenommen. Auch eine hundertprozentige Protokollierung kann dies nicht verhindern. Denn entsprechende Verstöße sind - mit Ausnahme unberechtigter Abfragen in Bezug auf Prominente - kaum zu erkennen.

In Rheinland-Pfalz soll eine neue Meldedatenverordnung die bundesrechtlichen Vorgaben für das behördliche Abrufverfahren im Land umsetzen und dabei die Bedarfe der öffentlichen Stellen im Land berücksichtigen. In dem Verordnungsentwurf sind landesweite automatisierte Abrufe und regelmäßige Datenübermittlungen vorgesehen. Bei den Online-Abrufen soll der Datenkatalog des § 38 Abs. 1 BMG für landesinterne Abrufe „zur Feststellung der Identität“ sogar noch erweitert werden, nämlich um frühere Anschriften, Ein- und Auszugsdaten, gesetzliche Vertreter (Familienname, Vorname, Doktorgrad, derzeitige Anschriften, Haupt -und Nebenwohnung, Geburtsdatum, Sterbedatum, bedingte Sperrvermerke) und die De-Mail-Adresse.

Parallel hierzu soll auf der Basis von § 37 Abs. 2 BMG in Form einer „Musterdienstanweisung“ für den automatisierten Abruf von Meldedaten „innerhalb der Verwaltungseinheit“ Rahmenbedingungen für Zugriffe auf den lokalen Datenbestand der jeweiligen Meldebehörde geschaffen werden.

In beiden Entwürfen ist der Online-Abruf des sog. melderechtlichen Familienverbandes vorgesehen. Durch „Verknüpfung von Datensätzen“ wird festgestellt, welche Personen einem melderechtlichen Familienverband angehören, der sodann auch für den automatisierten Abruf zur Verfügung gestellt werden soll. Zu dem Verband gehören Ehegatte, Lebenspartner, minderjährige Kinder sowie deren Eltern(teile) und gesetzliche Vertreter (einschließlich Betreuer) sowie die vertretenen Personen. Die Tatsache der Zugehörigkeit zu einem Familienverband ist in dieser Form im Bundesmeldegesetz nicht vorgesehen, sondern wurde landesrechtlich über das Ausführungsgesetz zum Bundesmeldegesetz als speicherfähiges Datum aufgenommen. Als Begründung wurde ausgeführt, dass es sich bei der Tatsache der Zugehörigkeit zu einem Familienverband um eine Information handele, die „vielfach“ für die Bearbeitung von einzelnen durch Rechtsvorschrift übertragenen Aufgaben benötigt werde.

Der LfDI hat gegenüber dem Innenministerium seine teilweisen erheblichen datenschutzrechtlichen Bedenken bzgl. der vorliegenden Entwürfe zum Ausdruck gebracht.

Diese betreffen insbesondere die Geeignet-

heit, Erforderlichkeit und Verhältnismäßigkeit einer Online-Abrufmöglichkeit des melderechtlichen Familienverbandes durch die Vielzahl der insoweit berechtigten Stellen sowie die Erweiterung des übermittlungsfähigen Datenkatalogs für öffentlich-rechtliche Religionsgesellschaften und den Südwestrundfunk.

Mit Blick auf die Europäische Datenschutz-Grundverordnung stellen sich weitere Fragen, z.B.

ob die „einfache Behördenauskunft“ nach § 38 Abs. 1 BMG im Hinblick auf die Zweckbindung (vgl. Art. 5 Abs. 1 DS-GVO „festgelegte, eindeutige und legitime Zwecke“) als mit der Europäischen Datenschutz-Grundverordnung vereinbar angesehen werden kann,

ob die programmgesteuerte Bildung des melderechtlichen Familienverbandes mit dem Verbot automatisierter Einzelentscheidungen nach Art. 22 DS-GVO zu vereinbaren ist und

ob und wie den Unterrichtungsverpflichtungen beim automatisierten Abruf nach Art. 14 Abs. 1 bis 4 DS-GVO durch die abrufberechtigten Stellen entsprochen werden kann.

Angesichts der Bedeutung der melderechtlichen Abrufe für die ca. vier Millionen Einwohnerinnen und Einwohner in Rheinland-Pfalz wird sich der LfDI mit den Datenschutzaufsichtsbehörden des Bundes und der Länder abstimmen und seine Position gegenüber dem Innenministerium auch weiterhin im Sinne des Datenschutzes für die Bürgerinnen und Bürger im Land vertreten.

9.2.2 Datenübermittlung an Ortsvorsteherinnen und –vorsteher durch das Bürgeramt

Der LfDI vertritt in Übereinstimmung mit dem Innenministerium zur Weitergabe von Meldedaten an Ortsvorsteherinnen und -vorsteher folgende Rechtsauffassung:

Die Zulässigkeit einer Weitergabe von Meldedaten der Bürgerinnen und Bürger an Ortsvorsteherinnen und -vorsteher hängt davon ab, ob die zuletzt genannten gem. § 76 Abs. 2 Satz 2 GemO von der Bürgermeisterin bzw. dem Bürgermeister oder den zuständigen Beigeordneten beauftragt worden sind, Repräsentationsaufgaben, wie die Gratulation zu Jubiläen, oder sonstige Aufgaben wahrzunehmen. Nur dann kann die Weitergabe der Meldedaten für deren Aufgabenerfüllung erforderlich sein.

Eine Dienstordnung ist insofern nicht ausreichend. Sofern diese Anforderung erfüllt ist, kommt eine Übermittlung von Meldedaten nach Maßgabe des § 34 Abs. 1 und 2 BMG auf Ersuchen der Ortsvorsteherin bzw. des Ortsvorstehers in Betracht. Dies schließt regelmäßige Datenübermittlungen ohne Ersuchen aus. Weiterhin ist zu beachten, dass der Wortlaut der genannten Bestimmung eine Datenweitergabe ins Ermessen des Bürgeramtes bzw.eldeamtes stellt („Die Meldebehörde darf…“) und darüber hinaus gem. § 8 BMG schutzwürdige Interessen der betroffenen Personen dabei nicht beeinträchtigt werden dürfen. Dies wäre etwa dann der Fall, wenn Daten von Personen betroffen wären, für die eine Auskunftssperre eingetragen ist oder die der Übermittlung von Meldedaten für Jubiläumszwecke widersprochen haben.

Es wäre aus datenschutzrechtlicher Sicht jedenfalls nicht zu beanstanden, wenn das Bürgeramt bzw. Meldeamt Ortsvorsteherinnen und -vorstehern bei Vorliegen der o.g. Voraussetzungen Meldedaten zur Verfügung stellt, damit diese beispielsweise Neubürgerinnen und -bürger begrüßen, zu Seniorennachmitta-

10. JUSTIZ

10.1 Datenschutz in Justizvollzugsanstalten

10.1.1 Gefangeneneinkauf

Im Berichtszeitraum haben den LfDI mehrere Eingaben von in den Justizvollzugsanstalten des Landes Rheinland-Pfalz inhaftierten Personen erreicht.

Es wurden u.a. datenschutzrechtliche Verstöße bei der Durchführung der Gefangeneneinkäufe dargelegt, insbesondere die namentliche Benennung der Gefangenen bei Verteilung der getätigten Einkäufe in Anwesenheit des externen Einkaufspersonals.

Gemäß § 10 Abs. 1 und 2 Nr. 2 lit. c LJVollzDSG dürfen personenbezogene Daten von Justizvollzugsbehörden zwar übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, wobei eine solche Übermittlung regelmäßig dann erforderlich ist, wenn sie dazu dient, Gefangenen den Einkauf zu ermöglichen. Allerdings sind die Daten dabei gemäß § 12 Abs. 2 LJVollzDSG zwingend zu pseudonymisieren, wobei grundsätzlich die Gefangenennummer zu verwenden ist.

Die betroffenen Justizvollzugsanstalten wurden infolge der Eingaben vom LfDI sodann zur Stellungnahme zum jeweiligen Sachvortrag des Petenten aufgefordert. Diese schilderten vielfach ein datenschutzkonformes Vorgehen beim Gefangeneneinkauf durch das Verwenden von Einkaufsscheinen, die lediglich die Gefangennummer als personenbeziehbares Datum enthielten.

Bei der Verteilung des Einkaufs kam es allerdings zumindest einmal zu einer namentlichen Benennung eines Gefangenen. Dies ist nach Aussage der Anstaltsleitung erfolgt, weil der Gefangene trotz mehrfacher Nennung der Buchungsnummer nicht reagiert habe. Der LfDI ist der Auffassung, dass auch in diesem Fall die namentliche Benennung nicht zulässig ist.

Die Anstaltsleitung hat die Eingabe sodann zum Anlass genommen, alle Bediensteten schriftlich darauf hinzuweisen, dass das Nennen der Namen von Gefangenen im Beisein der Kauffrau bzw. deren Mitarbeiterinnen und Mitarbeitern nicht zulässig ist und die Gefangenen ausschließlich unter Nennung ihrer Gefangenenbuchnummer in den Verkaufsraum gerufen werden dürfen. Aufgrund dessen hat der LfDI sodann von weiteren Maßnahmen in diesem Fall abgesehen.

10.1.2 Hinweis „Blutkontakt vermeiden“

Die Deutsche Aidshilfe hatte durch eine Abfrage im Jahr 2017 festgestellt, dass es in deutschen Justizvollzugsanstalten immer noch zur Unterrichtung von Bediensteten über HIV-Infektionen von Gefangenen ohne deren Einwilligung kommt. Dabei wird der Hinweis „Blutkontakt vermeiden“ bzw. ein entsprechendes Kürzel in das von den Justizvollzugsanstalten verwendete EDV-System aufgenommen. Diese Bekanntmachung stellt eine Übermittlung äußerst sensibler personenbezogener Gesundheitsdaten dar, die mangels Einwilligung einer gesetzlichen Grundlage bedarf und danach erforderlich sein muss. Einige Bundesländer haben entsprechende gesetzliche Grundlagen.

In Rheinland-Pfalz verwenden die Vollzugsanstalten weiterhin nicht diesen Hinweis. Von diesem Hinweis Abstand genommen hatten die Justizvollzugsanstalten bereits vor einigen Jahren auf Initiative des LfDI (vgl. 23. Tb., Tz.

II-8.3.2).

10.2 Datenschutzrechtliche Kontrollzuständigkeit bei rheinland-pfälzischen Gerichten

Im Berichtszeitraum gab es auch wieder einer Vielzahl von Eingaben die rheinland-pfälzischen Gerichte betreffend.

Gemäß § 24 Abs. 2 LDSG unterliegen die Gerichte und der Rechnungshof der Kontrolle des LfDI allerdings nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Aufgrund dessen bedarf es bei jeder Eingabe die rheinland-pfälzischen Gerichte betreffend zunächst einiger Aufklärungsarbeit des LfDI, um letztlich beurteilen zu können, ob es sich um eine Verwaltungsangelegenheit in diesem Sinne handelt oder nicht.

Wie dieser Begriff der „Verwaltungsangelegenheiten" zu verstehen ist, wird nicht einheitlich beurteilt. Er wird nicht lediglich in § 24 Abs. 2 LDSG, sondern ebenfalls in § 10 Abs. 3, § 11 Abs. 6, § 18 Abs. 8, § 27 Abs. 1 und § 28 Abs. 2 LDSG verwendet.

Teilweise wird vertreten, Verwaltungsangelegenheiten seien nur solche, die nicht als Erfüllung der Aufgaben der rechtsprechenden Gewalt im Sinne der Art. 92, 97 GG, § 4 Abs. 1, § 25 DRiG qualifiziert werden können, bzw. nur solche der sog. engeren Gerichtsverwaltung (d.h. Personalverwaltung, Bewirtschaftung der Haushaltsmittel, Beschaffung sowie Liegenschaftsverwaltung usw.). Dieser Ansicht ist allerdings nicht zu folgen.

Vielmehr ist der Begriff „Verwaltungsangelegenheiten" weit zu verstehen. Der LfDI vertritt hierzu die Auffassung, dass jede Tätigkeit von Gerichten, die nicht von der richterlichen Unabhängigkeit erfasst ist, eine Verwaltungsangelegenheit in diesem Sinne ist.

Denn mit der Regelung des § 24 Abs. 2 LDSG soll in erster Linie die verfassungsrechtlich garantierte richterliche Unabhängigkeit abgesichert werden. Hintergrund dieser Regelung sind Art. 97 GG und Art. 121 Landesverfassung, wonach die richterliche Gewalt im Namen des Volkes unabhängige Richterinnen und Richter ausüben, die allein der Verfassung, dem Gesetz und ihrem Gewissen unterworfen sind. Diese richterliche Unabhängigkeit richtet sich gegen jede Einflussnahme von außen, die die Richterinnen und Richter zu einer bestimmten Entscheidung veranlassen könnten. Eine solche Einflussnahme könnte mit der datenschutzrechtlichen Kontrolle und der damit verbundenen Bewertung von Sachverhalten, z. B. der Zulässigkeit von Datenerhebungen, einhergehen.

Eine weitere Einschränkung der Kontrolle durch den LfDI durch eine enge Auslegung des Begriffs „Verwaltungsangelegenheiten" ist nicht haltbar. Denn die Kontrolle der Datenverarbeitung durch unabhängige Datenschutzbeauftragte ist ein wesentliches Element der Gewährleistung des Rechts auf informationelle Selbstbestimmung. Die Persönlichkeitsrechte dürfen nicht unnötig stark eingeschränkt werden. Verfassungsrechtlich geboten ist lediglich die Ausnahme der Aufsicht im Bereich der richterlichen Unabhängigkeit und nicht bei sonstigen Tätigkeiten des Gerichtes.

Der Begriff der Verwaltungsangelegenheiten im LDSG betrifft also nicht nur diejenigen Tätigkeiten der Gerichte, die keinen Bezug zu der in richterlicher Unabhängigkeit vorgenommenen Spruchtätigkeit haben. Die Gerichtsverwaltung, also die Verwaltungstätigkeit, die die Gerichte selbst betrifft, gehört ebenso wie die Justizverwaltung, die die Unterstützung der

Rechtsprechung zum Gegenstand hat, zu den Verwaltungsaufgaben in diesem Sinne.

Ausgenommen von der Kontrollbefugnis des LfDI sind damit in der Regel die materiellen Entscheidungen der Richterin oder des Richters, da diese der richterlichen Unabhängigkeit unterfallen.

Jedoch unterfallen nicht sämtliche Tätigkeiten der Richterin und des Richters der richterlichen Unabhängigkeit. Insbesondere Hilfstätigkeiten, die von der Richterin oder dem Richter zwar selbst vorgenommen werden, die aber bloße praktische Bürotätigkeiten darstellen und die auch von technischem Personal ausgeführt werden könnten, unterliegen der Kontrolle.

Die Tätigkeit der Gerichtsvollzieherinnen und Gerichtsvollzieher im Rahmen eines Vollstreckungsverfahrens hat keinen Bezug zur richterlichen Unabhängigkeit. Gründe für eine Freistellung von der externen Datenschutzkontrolle sind mithin nicht ersichtlich. Eine Eintragungsanordnung oder ein Kontenabrufersuchen durch Gerichtvollzieherinnen oder Gerichtsvollzieher und die damit einhergehende Übermittlung personenbezogener Daten durch dieselben ist unter Berücksichtigung obiger Ausführungen damit jedenfalls eine Verwaltungsangelegenheit im Sinne des § 24 Abs. 2 LDSG.

Auch die Tätigkeit einer Rechtspflegerin oder eines Rechtspflegers ist ggf. eine Verwaltungsangelegenheit (soweit nicht die richterliche Unabhängigkeit betroffen ist). Rechtspflegerinnen und Rechtspfleger üben durch ihre Rechtspflegertätigkeit nämlich keine rechtsprechende Gewalt im Sinne von Art. 92 GG aus. Dem entspricht, dass sie selbst nicht mit richterlicher Unabhängigkeit gem. Art. 97 Abs. 1 und 2 GG ausgestattet sind. Zwar sind die Rechtspflegerin und der Rechtspfleger gemäß § 9 RPflG sachlich unabhängig und nur an Recht und Gesetz gebunden. Die Kontrollbefugnisse des LfDI werden dadurch allerdings nicht eingeschränkt.

Die fehlende Kontrollbefugnis des LfDI entbindet die Gerichte bzw. die einzelnen Richterinnen und Richter aber auch nicht davon, die datenschutzrechtlichen Vorschriften einzuhalten. Vielmehr unterfallen Gerichte als öffentliche Stellen dem Anwendungsbereich des Landesdatenschutzgesetzes. Werden die danach zu beachtenden Bestimmungen missachtet, ist das Verhalten rechtswidrig. Diese Rechtswidrigkeit kann gerichtlich überprüft werden.

10.3 Datenschutzwidrige Übermittlung von Ergebnissen eines Kontenabrufersuchen durch Gerichtsvollzieherinnen und Gerichtsvollzieher

Kontenabrufersuchen von Gerichtsvollzieherinnen und Gerichtsvollziehern sind von der Kontrollbefugnis des LfDI erfasst (siehe 25. Tb., Tz. III-10.3).

Bezüglich des datenschutzkonformen Umgangs mit Informationen, die die Gerichtsvollzieherin oder der Gerichtsvollzieher auf Grundlage eines Kontenabrufersuchens erhält, besteht teilweise noch Uneinigkeit. Dabei ist der Umgang mit solchen Informationen immer wieder Gegenstand von Eingaben.

Gerichtsvollzieherinnen und Gerichtsvollzieher haben die jeweilige Gläubigerin oder der Gläubiger über das Ergebnis eines Ersuchens an das Bundeszentralamt für Steuern gemäß § 802l Abs. 1 Satz 1 Nr. 2 ZPO unverzüglich zu unterrichten (§ 802l Abs. 3 Satz 1 ZPO). Dabei haben sie allerdings die Daten, die für die Zwecke der Vollstreckung nicht erforderlich sind, unver-

züglich zu löschen oder zu sperren (§ 802l Abs. 2 Satz. 1 ZPO).

In der Vergangenheit wurde in der Rechtsprechung wiederholt vertreten, dass Konten von Dritten, an denen eine Verfügungsberechtigung des Schuldners bestehe, dem Gläubiger mitzuteilen seien. Begründet wurde dies damit, dass Bankkonten eines Dritten, für die der Schuldner bevollmächtigt sei, zwar nicht Bestandteile des Schuldnervermögens seien, sich aber aus diesen Angaben „sonstige Forderungen" ergeben könnten. Diese Daten seien für die Zwangsvollstreckung erforderlich, da nicht auszuschließen sei, dass der Schuldner auch über diese Konten Zahlungen erhalte. Durch diese Mitteilung werde auch nicht in unzulässiger Weise in Rechte Dritter eingegriffen, da durch die Vollmachtserteilung auch mit einer Kenntnis von dieser zu rechnen sei (Amtsgericht Bayreuth, Beschluss vom 04. Juli 2013, Az. 7 M 289/13).

Allerdings wird nicht jedes Drittkonto vom Schuldner für eigene Zwecke genutzt; sondern es gibt oftmals schlicht ein praktisches Bedürfnis für eine Vollmachtserteilung. Dennoch entspreche es aber umgekehrt der Lebenserfahrung, dass Schuldner Drittkonten dazu nutzen würden, Geldverkehr abzuwickeln Da § 802l ZPO den umfassenden Schutz des Gläubigers bezwecke und nicht ausgeschlossen werden könne, dass der Schuldner Konten naher Angehöriger zum Zwecke des eigenen Geldverkehrs nutze, könne auch nicht festgestellt werden, dass gemäß § 802 l Abs. 2 ZPO solche Daten für die Zwecke der Vollstreckung nicht erforderlich seien. Nur solche Daten seien zu löschen, bei denen klar sei, dass diese definitiv nicht erforderlich sind, was aber bei Verfügungsberechtigungen des Schuldners über Drittkonten pauschal gerade nicht behauptet werden könne (Amtsgericht Soest, Beschluss vom 03. Oktober 2014, Az. 9 M 1129/14; Amtsgericht Hamburg-St. Georg, Beschluss vom 29. September 2015, Az. 904 M 2330/15).

Dieser Auffassung ist allerdings nicht zu folgen.

Zwar mag es für die Zwangsvollstreckung insgesamt ggf. hilfreich sein zu wissen, ob der bargeldlose Zahlungsverkehr des Schuldners über das Konto eines Dritten abgewickelt wird, da der Gläubiger gegen den Dritten, der sein Konto dem Schuldner zur Verfügung stellt, möglicherweise einen Anspruch auf Auskehrung der wirtschaftlich dem Schuldner zuzuordnenden Beträge aus § 667 BGB hat. Allerdings ist Sinn und Zweck eines Kontenabrufersuchens, die Bankverbindung, d.h. eigene Konten und Depots des Schuldners bei Kreditinstituten in Erfahrung zu bringen, um letztlich in diese Konten hinein vollstrecken zu können, und nicht andere ggf. gegenüber sonstigen Dritten bestehende Ansprüche in Erfahrung zu bringen.

Außerdem steht der Mitteilung der personenbezogenen Daten des Dritten dessen informationelles Selbstbestimmungsrecht entgegen (so auch Amtsgericht Kiel, Beschluss vom 28. September 2016, Az. 21 M 1787/16) – insbesondere da die Mitteilung allein aus dem Grund erfolgt, dass eine Verfügungsmacht eingeräumt wurde und unabhängig davon, ob tatsächlich eine Kontenleihe des Dritten vorliegt.

Dass das Recht des Schuldners im Rahmen der Zwangsvollstreckung gegenüber dem Gläubigerschutz zurücktreten muss, ist eine bewusste Entscheidung des Gesetzgebers, die dieser durch Abwägung beider Interessen getroffen hat. Der Schuldner muss bei Nichtbegleichen einer Forderung auch damit rechnen, dass es zu Maßnahmen kommt, die sein informationelles Selbstbestimmungsrecht tangieren. Eine Kontenabfrage erfolgt erst nach Aufforderung zur Abgabe einer Vermögensauskunft. Deshalb muss jeder, der zur Abgabe einer Vermögens-

auskunft aufgefordert wird, damit rechnen, dass eine Kontenabfrage durchgeführt wird (BT-Drs. 16/10069, S. 32). Letztlich ist eine Kontenabfrage mit Tangieren des informationellen Selbstbestimmungsrechts für den Schuldner daher zumindest vorhersehbar und in der Regel auch beherrschbar.

Dass der Gesetzgeber auch insoweit dem Gläubigerschutz gegenüber dem informationellen Selbstbestimmungsrecht des Dritten, der dem Schuldner nur eine Verfügungsmacht – aus welchen Gründen auch immer – eingeräumt hat, den Vorrang eingeräumt hat, ist der Gesetzesbegründung nicht zu entnehmen. Zudem ist es für Dritte auch weder vorhersehbar und auch nicht beherrschbar, dass Gläubiger eines Schuldners an ihre personenbezogenen Daten gelangen. Dass Dritte dies bereits mit Erteilung einer Verfügungsmacht – aus welchen Gründen auch immer – bewusst in Kauf nehmen, ist lebensfremd und daher nicht anzunehmen.

Zudem ist der Gläubiger auch bei Nichtmitteilung der Drittkonten, über die der Schuldner verfügungsberechtigt ist, nicht gänzlich schutzlos. Er kann andere Wege einschlagen, um Informationen bezüglich möglicher Auskehransprüche zu erhalten. Ferner ist auch dabei nochmals zu beachten, dass Sinn und Zweck des Kontenabrufersuchens primär ist, Konten des Schuldners in Erfahrung zu bringen und nicht andere ggf. gegenüber sonstigen Dritten bestehende Ansprüche (ähnlich in der soeben dargestellten Argumentation auch Amtsgericht Kiel, Beschluss vom 28. September 2016, Az. 21 M 1787/16).

Konten Dritter mit Verfügungsmacht des Schuldners sind dem Gläubiger folglich nicht bekannt zu machen. Dies wurde gegenüber dem Ministerium der Justiz auch bereits dargelegt.

10.4 Ausgestaltung von E-Mail-Verteilern bei der rheinland-pfälzischen Justiz

Ein Petent wendete sich an den LfDI wegen der Ausgestaltung eines E-Mail-Verteilers bei der rheinland-pfälzischen Justiz. Im Zuge einer Erteilung von Informationen kam es zu einer Gestaltung eines E-Mail-Verteilers in der Form, dass alle Adressaten der E-Mail für jeden E-Mail-Empfänger ersichtlich waren. Dabei handelte es sich um private E-Mail-Adressen von nicht der Justiz angehörigen Personen.

Fragen zur datenschutzkonformen Ausgestaltung von E-Mail-Verteilern treten allerdings nicht nur im Bereich Justiz auf, sondern werden an den LfDI von den unterschiedlichsten verantwortlichen Stellen herangetragen.

Beim Versenden von E-Mails gibt es letztlich drei Möglichkeiten der Adressierung:

Zum einen kann man sämtliche Empfänger in das „An-Feld“ eintragen. Möglich ist auch zusätzlich die Verwendung des „Cc-Feldes“ („Carbon-Copy“); damit kann man eine Kopie der E-Mail an weitere Empfänger senden. Schließlich gibt es auch noch das Feld „Bcc“ („Blind Carbon Copy“), das man alternativ oder kumulativ zum „Cc-Feld“ zur Sendung von Kopien an Empfänger nutzen kann.

Sämtliche Adressen, die in das „An-Feld“ und das „Cc-Feld“ eingetragen werden, sind für alle übrigen Empfänger sichtbar. Lediglich die in das „Bcc-Feld“ eingetragenen Adressen sind nicht für die übrigen Empfänger sichtbar.

Bei E-Mail-Adressen handelt es sich um personenbezogene Daten gemäß § 3 Abs. 1 LDSG. Durch den offenen Versand über eine Verteiler-E-Mail durch alleinige Nutzung der „An- und Cc-Felder“ werden diese personenbezogenen Daten an Dritte übermittelt. Die Übermittlung

personenbezogener Daten ist allerdings grundsätzlich unzulässig, wenn sie nicht durch einen Erlaubnistatbestand gedeckt ist. Vielfach dürfte ein Erlaubnistatbestand nicht vorliegen.

Der LfDI empfiehlt daher – wenn eine Verteiler-E-Mail als notwendig erachtet wird – die Nutzung des „Bcc-Feldes", um datenschutzrechtliche Verstöße infolge der unzulässigen Übermittlung von personenbezogenen Daten insoweit zu vermeiden.

Nachdem die Justiz in ihrer Stellungnahme zu diesem Sachverhalt versicherte, zukünftig auf datenschutzkonforme E-Mail-Verteiler zu achten, wurde seitens des LfDI auf weitere Maßnahmen verzichtet.

10.5 Aufsichtsbehördliche Befugnisse und Anwendbarkeit der Vorschriften des Bundesdatenschutzes auf Rechtsanwältinnen und Rechtsanwälte

Auch die Verarbeitung personenbezogener Daten von Rechtsanwältinnen und Rechtsanwälten ist immer wieder Gegenstand von Eingaben.

Dabei geht es häufig immer wieder um grundlegende Fragen, nämlich die der möglichen Vorrangigkeit spezialgesetzlicher Regelungen im Berufsrecht vor den allgemeinen Regelungen des Bundesdatenschutzgesetzes und der Aufsichtsbefugnis des LfDI im Generellen Rechtsanwältinnen und Rechtsanwälten gegenüber.

Im Hinblick auf die Vorrangigkeit der spezialgesetzlichen Regelungen insbesondere gegenüber § 34 BDSG ist das Folgende zu beachten:

Die Bestimmungen der Bundesrechtsanwaltsordnung sind keine bereichsspezifische Sonderregelung im Sinne des § 1 Abs. 3 Satz 1 BDSG. Denn die berufsrechtlichen Regelungen der Bundesrechtsanwaltsordnung betreffen überwiegend den Schutz der Mandanten und das öffentliche Interesse an einer funktionierenden Strafrechtspflege, während das Bundesdatenschutzgesetz sämtliche Personen schützt, die durch den Umgang der Rechtsanwältin oder des Rechtsanwalts mit personenbezogenen Daten beeinträchtigt werden. Allerdings ist § 1 Abs. 3 Satz 2 BDSG einschlägig, demzufolge andere gesetzliche Vorschriften die Anwendung des Bundesdatenschutzgesetzes ausschließen, wenn sie derartige Geheimhaltungspflichten zum Gegenstand haben und den davon betroffenen Personenkreis weitergehend als im Bundesdatenschutzgesetz schützen – so wie § 43a Abs. 2 BRAO (vgl. Kammergericht Berlin, Beschluss vom 20. August 2010, Az. 1 Ws(B) 51/07, 1 Ws(B) 51/07 – 2 Ss23/07).

In Bezug auf die Frage der Aufsichtsbefugnis des LfDI im Bereich der rechtsanwaltlichen Tätigkeit gilt Folgendes:

Gemäß § 38 Abs. 1 BDSG kontrolliert der LfDI als zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich in Rheinland-Pfalz (§ 24 Abs. 1 Satz 2 LDSG) die Ausführung der Vorschriften über den Datenschutz.

Bei den Rechtsanwälten handelt es sich insoweit um nicht-öffentliche Stellen. Eine Kompetenznorm, die entgegen dieser Regelung die Aufsicht für Rechtsanwälte auf die Rechtsanwaltskammern überträgt, ist nicht ersichtlich. Insbesondere ist weder dem Wortlaut der §§ 56, 73 BRAO zu entnehmen noch ergibt sich aus deren Sinn und Zweck, dass diese gegenüber § 38 BDSG abschließende und speziellere Sonderregelungen sein sollen. Zudem ist der LfDI eine hinreichend unabhängige Stelle, um auch Aufsichtsbehörde für Datenschutz im Bereich der rechtsanwaltlichen Tätigkeit zu sein.

11. VERBRAUCHERSCHUTZ

Der Verbraucherdialog ist ein bundesweit einzigartiges Format eines Expertenforums basierend auf der Initiative des Verbraucherschutzministeriums in bewährter Kooperation mit der Verbraucherzentrale Rheinland-Pfalz e.V. und dem LfDI. Ziel der Verbraucherdialoge ist es, zusammen mit Expertinnen und Experten aus Wirtschaft, Wissenschaft und Technik, von Behörden, Institutionen und Organisationen datenschutz- und verbraucherfreundliche Anforderungen an neue digitale Technologien unter Berücksichtigung der neuesten Kenntnisse und Erfahrungen zu formulieren.

Im September 2017 fiel der Startschuss für den 5. Verbraucherdialog in Mainz, der sich dem Thema „Wearables: Fitnessarmbänder & Co“ widmete. Schritte zählen, Schlafgewohnheiten beobachten, den Blutdruck oder die Blutwerte messen – sog. Wearables, wie z.B. Fitnesstracker oder Smart Watches, aber auch smarte Kleidung machen es möglich und werden von immer mehr Menschen genutzt. Wearables sind am Körper tragbare Computertechnologien, die körperliche Aktivitäten und Abläufe messen und Aussagen über Fitness, Gesundheit und Wohlbefinden ermöglichen. Vernetzte Kleidungsstücke erfassen Vital- und Bewegungsdaten oder steuern durch Bewegung das Smartphone. Spezielle Ohrhörer reagieren bei der Musikauswahl auf Körpersignale. Diese rasante Entwicklung wirft brisante Fragen für den Daten- und Verbraucherschutz auf. Mit den Vor- und Nachteilen dieser technischen Möglichkeiten befasst sich der 5. Verbraucherdialog mit dem Ziel, gemeinsam Handlungsempfehlungen für Anbieter zu erarbeiten.

Beim Kick-Off im September erfolgten eine thematische Einführung durch die Hausspitzen der Kooperationspartner und die Vorstellung eines Fragenkatalogs, der sich an die Teilnehmenden richtete und als Basis für die Erarbeitung der Handlungsempfehlungen dienen wird. Das erste Arbeitstreffen mit den Teilnehmenden fand Ende November 2017 statt und hatte den Fokus auf der Verbraucherfreundlichkeit. Das zweite Arbeitstreffen mit dem datenschutzrechtlichen Schwerpunkt findet im Januar 2018 statt und wird vom LfDI vorbereitet, moderiert und bearbeitet. Im schriftlichen Umlaufverfahren werden die Handlungsempfehlungen finalisiert, um sie im März 2018 auf der Abschlussveranstaltung vorzustellen. Sie werden dazu beitragen, dass Verbraucherinnen und Verbraucher neue Technologien unter Wahrung ihres Rechts auf informationelle Selbstbestimmung mit Vertrauen und Mehrwert nutzen können.

Der LfDI setzt sich vor allem für die Transparenz der Datenverarbeitungsprozesse, für Datensouveränität der Verbraucherinnen und Verbraucher, für Datensicherheit sowie für Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ein https://s.rlp.de/entschliessung042016.

12. FINANZEN

12.1 Falsche Versendung von Abgabenbescheiden

Im Berichtszeitraum kam es in einer Verbandsgemeinde zur fehlerhaften Versendung von Abgabenbescheiden. Die Verbandsgemeinde hatte einen Dienstleister beauftragt, Abgabenbescheide zu versenden. Bei diesem Dienstleister war es zu einem Fehler gekommen, der dazu geführt hatte, dass Abgabepflichtige Bescheide erhielten, die nicht für sie bestimmt waren.

Auch für kommunale Abgaben gilt gem. § 3 Abs. 1 Nr. 1 KAG i.V.m. § 30 AO das Steuergeheimnis. Durch die Versendung von Abgabebescheiden an die falschen Empfänger wurde dieses Steuergeheimnis verletzt. Zudem handelte es sich um eine Datenpanne, bei der nicht nur unverzüglich die Betroffenen, sondern auch der LfDI zu informieren waren (§ 18a LDSG).

Darüber hinaus gilt, dass eine Auftragsdatenverarbeitung im Gebührenbereich nur dann unproblematisch ist, wenn ein Dienstleister in öffentlicher Trägerschaft, z.B. ein kommunales Rechenzentrum, den Auftrag erhält. An gesetzliche Grenzen stößt man jedoch bei der Vergabe an private Anbieter. Denn das auch für kommunale Abgaben geltende Steuergeheimnis steht gem. § 4 Abs. 4 Satz 2 LDSG grundsätzlich einer Auftragsdatenverarbeitung durch nicht öffentliche Stellen entgegen. Danach soll an nicht öffentliche Stellen ein Auftrag zur Datenverarbeitung nur vergeben werden, wenn überwiegende schutzwürdige Interessen, insbesondere Berufs- oder besondere Amtsgeheimnisse, nicht entgegenstehen. Das Erstellen und Versenden von Gebührenbescheiden durch ein privates Unternehmen ist nur ausnahmsweise zulässig (vgl. 20. Tb., Tz. 13.4).

Der LfDI hat in diesem Zusammenhang eine Beanstandung gem. § 25 LDSG ausgesprochen. Die Verbandsgemeinde hat mittlerweile den Auftrag datenschutzrechtlich überabreitet und neu vergeben.

12.2 Informantenschutz durch das Finanzamt

Ein Petent zeigte beim Finanzamt ein nach seiner Auffassung nicht steuergemäßes Verhalten an, das ihm in einem Gewerbetrieb aufgefallen war. Daraufhin leitete das zuständige Finanzamt ein Steuerstrafverfahren gegen den Inhaber des Gewerbebetriebes ein. Im Rahmen des Strafverfahrens erlangte der Angezeigte Kenntnis davon, wer ihn angezeigt hatte. Hier war fraglich, wie und warum der Angezeigte an die Information gelangte.

Grundsätzlich ist die Identität von Hinweisgebern und Informanten vertraulich zu behandeln. Die Behörden sind grundsätzlich geheimhaltungspflichtig bezüglich der Information, wer sie auf rechtswidriges Verhalten Dritter hingewiesen hat. Denn die rechtskonform die Verwaltung unterstützenden Bürgerinnen und Bürger sind vorrangig schutzwürdig gegenüber den rechtsbrechenden Bürgerinnen und Bürgern. Etwas anderes gilt nur dann, wenn ausreichende Anhaltspunkte dafür vorliegen, dass der Informant die Behörde wider besseres Wissen oder leichtfertig falsch unterrichtet oder in der Absicht gehandelt hat, dem Betroffenen rechtswidrig Schaden zuzufügen. Diese Auffassung wird auch von der rheinland-pfälzischen Steuerverwaltung geteilt.

So komme man dem Schutz des Informanten durch Prüfung bzw. sorgfältige Abwägung nach. Das Recht auf Akteneinsicht nach § 147 StPO trete insoweit hinter das Steuergeheimnis nach § 30 AO zurück und stelle grundsätz-

lich keinen Durchbrechungstatbestand dar. Eine Offenbarung lasse sich im Regelfall nur auf § 30 Abs. 4 und 5 AO stützen. Letztendlich sei die Einsichtnahme in die Anzeige daher eine Entscheidung, die von den Umständen des Einzelfalles abhängig sei (z.B. der Qualität der Anzeige als einziges Beweismittel, dem Verfahrensstand, dem Wahrheitsgehalt der Angaben). Bestehe keine Offenbarungsbefugnis, sei der Informant in der Anzeige zu schwärzen, ein den Inhalt der Anzeige wiedergebender Aktenvermerk zu fertigen oder die Anzeige überhaupt nicht vorzulegen.

Diese Auffassung ist aber mit den Regelungen der Strafprozessordnung zu vereinbaren. Denn für das Strafverfahren wegen Steuerstraftaten gilt gem. § 385 AO die Strafprozessordnung. Nach § 147 Abs. 1 StPO ist der Verteidiger befugt, die Akten, die dem Gericht vorliegen oder diesem in Falle der Erhebung der Anklage vorzulegen wären, einzusehen sowie amtlich verwahrte Beweisstücke zu besichtigen.

Letztlich war davon auszugehen, dass der Angezeigte über das Gericht, das die Akten beim Finanzamt angefordert hatte, die Informationen erhalten hatte. Das Finanzamt selbst hatte wohl keine Auskünfte erteilt. Aufgrund dieses Vorfalls plant das Finanzamt zukünftig eine andere Aktenhaltung: Hinweise auf die Anzeigenerstatterinnen und –erstatter sollen in einer Nebenakte geführt werden, die dem Gericht dann auch nicht vorzulegen ist, so dass durch Akteneinsicht bei Gericht die Informationen nicht an die Angezeigten gelangen.

12.3 Lohnbuchhaltung durch Steuerberaterinnen und –berater

Viele Steuerberaterinnen und -berater führen für ihre Kunden auch die Lohn- und Gehaltsabrechnung durch. Aus datenschutzrechtlicher Sicht ist es fraglich, ob sie dann als Auftragsdatenverarbeiter handeln oder ob ihnen die Aufgabe zur selbständigen Erledigung (sog. Funktionsübertragung) übertragen wird. Die Unterscheidung hat Konsequenzen: Ist es eine Auftragsdatenverarbeitung, muss ein entsprechender Vertrag gem. § 11 BDSG abgeschlossen werden und verantwortlich bleibt der Auftraggeber, also die Firma oder das Unternehmen. Wird dagegen die Funktion übertragen, sind die Steuerberaterinnen und –berater verantwortlich.

Die Unterscheidung kann nicht pauschal getroffen werden, sondern es kommt im Wesentlichen darauf an, inwieweit die Lohn- und Gehaltsbuchhaltung als weisungsgebundene Tätigkeit ausgeübt wird. Lediglich wenn die Steuerberaterinnen und -berater absolut weisungsgebunden in dieser Angelegenheit tätig werden, also keinerlei selbständige Entscheidungsbefugnis haben, sind diese Arbeiten als Auftragsdatenverarbeitung im Sinne des § 11 BDSG zu beurteilen.

Erledigen die Steuerberaterinnen und -berater dagegen die ihnen übertragenen Aufgaben im großen Maße selbständig und kann der Auftraggeber auf die Verarbeitung nicht ohne Weiteres Einfluss nehmen, ist von einer Funktionsübertragung auszugehen. Dies ist z.B. dann der Fall, wenn die Steuerberaterin oder der Steuerberater im Rahmen des Mandates zur Erstellung der Gehaltsabrechnung auch Lohnsteuer- und Sozialversicherungsprüfungen begleitet und weitere teilweise eigenverantwortliche Tätigkeiten ausübt, z.B. das Ausstellen von Bescheinigungen, das Tätigen von Meldungen sowie das soeben erwähnte Begleiten von Prüfungen.

Von einer Funktionsübertragung ist also dann auszugehen, wenn Steuerberaterinnen und -berater auch im Rahmen ihrer Steuerbera-

tungsfunktion die Lohn- und Gehaltsbuchhaltung selbständig quasi nach ihren eigenen Vorgaben als Steuerberater durchführen. Inwieweit dies in jedem Einzelfall zutrifft, muss die Steuerberaterin oder der Steuerberater selbst beurteilen.

Die Auftragsdatenverarbeitung wird auch grundsätzlich nach der Datenschutz-Grundverordnung bzw. dem neuen Bundesdatenschutzgesetz möglich sein. Sie wird dann Auftragsverarbeitung heißen, der Auftraggeber Verantwortlicher und der Auftragnehmer Auftragsverarbeiter. Auch zukünftig hat der Auftraggeber zu prüfen, ob der Auftragsverarbeiter geeignet ist, insbesondere ob er geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz getroffen hat. Als Beleg hierfür können genehmigte Verhaltensregeln oder Zertifizierungen herangezogen werden. Auch zukünftig ist ein Vertrag zur Auftragsdatenverarbeitung mit weitgehend gleichem Inhalt zu schließen. Dies kann auch elektronisch erfolgen. Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Datenverarbeitung, wird er insoweit selbst zum Verantwortlichen mit allen rechtlichen Folgen. So muss er z.B. die Betroffenenrechte erfüllen. Betroffene können gegen ihn auch Schadensersatzansprüche geltend machen. Der Auftragsverarbeiter hat künftig auch ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Datenpannen sind dem Verantwortlichen, also dem Auftraggeber, unverzüglich anzuzeigen. Bußgelder können ggf. auch gegen Auftragsverarbeiter verhängt werden.

13. VERKEHR

Immer mehr Einkaufsmärkte, die einen Parkplatz für ihre Kunden vorhalten, gehen dazu über, die Bewirtschaftung des Parkraums an darauf spezialisierte Firmen zu übertragen. Dies bedeutet in der Regel für die Parkplatznutzerinnen und -nutzer, dass sie nur eine beschränkte Zeit, nämlich für die Dauer ihres Einkaufs dort parken dürfen. Sie sind dann verpflichtet, eine Parkscheibe auszulegen. Die Parkplätze werden durch die beauftragte Firma überwacht. Verstößt jemand gegen die Parkregeln, wird er mit einer Vertragsstrafe belegt. Um den Falschparker ausfindig zu machen, führen die einschlägigen Firmen eine Halterabfrage bei den Zulassungsstellen durch, um dann bei der Halterin oder dem Halter oder über sie oder ihn die Vertragsstrafe zu kassieren. Dies trifft viele Parkende, die den Parkplatz nicht gemäß den Vorgaben nutzen, also z.B. keine Parkscheibe auslegen oder länger parken als erlaubt. Dann kommt es zu Nachfragen, ob solche Halterabfragen durch die Parkraumbewirtschafter überhaupt zulässig sind.

Grundsätzlich hält der LfDI Halterabfragen in diesem Zusammenhang für datenschutzrechtlich nicht unzulässig.

Im Rahmen der sog. einfachen Registerauskunft sind durch die Zulassungsbehörde oder durch das Kraftfahrtbundesamt bestimmte Fahrzeuge und Halterdaten zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeugidentifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung und der Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt (§ 39 Abs. 1 StVG). Bei der (vermeintlichen)

unberechtigten Nutzung eines Kundenparkplatzes ist in der Regel davon auszugehen, dass zur Verfolgung evtl. Rechtsansprüche eine einfache Registerauskunft im Sinne von Abs. 1 zu erteilen ist.

Weiterhin ist davon auszugehen, dass hier auch der erforderliche Zusammenhang mit dem Straßenverkehr besteht. So führt z.B. das Verwaltungsgericht Gießen in seinem Urteil vom 03.03.1999 (Az.: 6 E 81/98 (1)) dazu Folgendes aus:

„Straßenverkehr im Sinne des StVG und der auf seiner Grundlage ergangenen Verordnungen ist nur der öffentliche Verkehr, d.h. der auf öffentlichen Wegen und Plätzen stattfindende Verkehr (vgl. § 1 StVG, § 1 StVO). Dem öffentlichen Straßenverkehr dienen alle Flächen, die der Allgemeinheit zu Verkehrszwecken offenstehen (...). Voraussetzung ist die ausdrückliche oder stillschweigende Freigabe durch den Berechtigten zur allgemeinen Verkehrsbenutzung, wobei maßgeblich ist, dass tatsächliche Zugänglichkeit für die Allgemeinheit (faktische Öffentlichkeit) besteht."

Bei Kundenparkplätzen, z.B. die eines Einkaufsmarktes, ist also grundsätzlich davon auszugehen, dass sie der Allgemeinheit tatsächlich zugänglich sind.

Wenn eine unberechtigte Nutzung des Kundenparkplatzes im Raume steht, kann der Betreiber des Parkplatzes bzw. ein von ihm dazu Bevollmächtigter hiergegen rechtlich vorgehen. Der erste Schritt hierzu ist, die Halterin oder den Halter des vermeintlich falschparkenden Fahrzeugs zu ermitteln, um dann ggf. in einem weiteren Schritt gegen die tatsächliche Nutzerin oder den tatsächlichen Nutzer des Fahrzeuges vorgehen zu können. Dabei kommt es nach Einschätzung des LfDI nicht darauf an, dass bereits zum Zeitpunkt der Halterabfrage die tatsächliche Fahrerin oder der tatsächliche Fahrer feststeht. Wäre dies Voraussetzung, wäre eine weitere rechtliche Verfolgung im Bereich des Straßenverkehrs quasi ausgeschlossen. Zudem geht z.B. der Bundesgerichtshof in seinem Urteil vom 18.12.2015 (Az.: VZR 160/14) davon aus, dass die Halterin oder der Halter, auch wenn sie oder er nicht Fahrerin oder Fahrer ist, als sog. Zustandsstörer in Anspruch genommen werden kann.

Die weitere Datenverarbeitung beim Parkplatzbetreiber bzw. Parkraumbewirtschafter richtet sich sodann nach den allgemeinen datenschutzrechtlichen Vorgaben gem. dem Bundesdatenschutzgesetz. Letztlich dürfen die Daten nur für den Zweck verwendet werden, für den sie erhoben wurden und sind dann zu löschen, wenn sie zur Erreichung des Zweckes nicht mehr erforderlich sind. Letztlich überprüft die Einhaltung dieser datenschutzrechtlichen Vorgaben die für das Unternehmen zuständige Datenschutzaufsichtsbehörde.

Inwieweit tatsächlich eine unberechtigte Nutzung eines Kundenparkplatzes erfolgt ist und ob dafür wirksam eine Vertragsstrafe erhängt werden darf, muss letztlich zivilrechtlich überprüft werden.

14. VERWALTUNG DIGITAL

14.1 Videoüberwachung

Bereits in den Jahren 2008 und 2009 hat der LfDI zahlreiche öffentliche Stellen, darunter alle Kommunen, zur Videoüberwachung öffentlich und nicht öffentlich zugänglicher Räume befragt. U.a. wegen der sinkenden Kosten und der gleichzeitig zunehmenden Leistungsfähigkeit von Videoüberwachungssystemen hat die Zahl solcher Anlagen seitdem zugenommen.

Jedenfalls ist die Videoüberwachung fester Bestandteil der Tätigkeit des LfDI und somit regelmäßig Thema in den Datenschutzberichten der vergangenen Jahre (vgl. 22. Tb., Tz. 3.2 und Tz. 10.1.1; 23. Tb., Tz. II. 7.1.3; 24. Tb., Tz. III. 7.1.2).

In der Regel erfolgt eine datenschutzrechtliche Bewertung auf der Grundlage von § 34 LDSG. Demnach ist die Überwachung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen bei bloßer Videobeobachtung (Monitoring) und bei Videoaufzeichnung mit unterschiedlichen Voraussetzungen zulässig, weil letztere tiefer in das informationelle Selbstbestimmungsrecht der Betroffenen eingreift.

Videoüberwachung in einem Hallenbad

Von einer Besucherin bzw. einem Besucher wurde die Videoüberwachung in Form der Aufzeichnung in bestimmten Bereichen eines Hallenbades, die Anzahl der Kameras und deren mangelnde Kennzeichnung problematisiert. Mit insgesamt neun Kameras wurden nicht nur die Wertschließfächer überwacht, sondern u.a. auch der Barfußgang zwischen den Umkleidekabinen oder die Gänge zwischen den Garderobenschränken. Begründet wurde dies vom Träger des Schwimmbades mit Diebstählen und Sachbeschädigungen.

Gemäß § 2 Abs. 3 LDSG kommt im Falle von öffentlich-rechtlichen Wettbewerbsunternehmen § 6b BDSG zur Anwendung. Danach ist die Beobachtung bzw. Speicherung mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit dies zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Besucherinnen und Besucher halten sich zum Zweck der Freizeitgestaltung im Hallenbad auf, weshalb sie besonderen Schutz genießen. Die Prüfung des Vorliegens der gesetzlichen Voraussetzungen, insbesondere der Angemessenheit der Überwachungsanlage, bedarf daher besonderer Sorgfalt. So überwiegen schutzwürdige Interessen der Besucherinnen und Besucher stets die Interessen des Schwimmbadträgers, wenn die Intimsphäre der Betroffenen berührt ist.

Der LfDI hat die Zulässigkeit jeder einzelnen Kamera bewertet. Auf seine Einwände und Anmerkungen hin wurden zwei Kameras in sensiblen Bereichen demontiert und bei weiteren zwei Kameras von der Aufzeichnung auf bloßes Monitoring umgestellt.

14.2 Einsatz von per Funk auslesbaren Wasserzählern

Auf den Einsatz von per Funk auslesbaren Wasserzählern wurde der LfDI von mehreren Bürgerinnen und Bürgern aufmerksam gemacht, nachdem kommunale Versorgungsunternehmen die üblicherweise eingesetzten „analogen“ Wasserzähler gegen solche mit neuer Technik ausgetauscht hatten. Vorrangiges Ziel der Unternehmen ist dabei die Minderung

des personellen Aufwandes beim Ablesen der Wasserzähler zum Zwecke der jährlichen Verbrauchsabrechnung, da die Zählerstände von den Messeinrichtungen der „neuen Generation“ mittels eines speziellen Gerätes erfasst werden können, ohne dass ein Gebäude betreten werden müsste.

Die jeweiligen kommunalen Versorgungsunternehmen setzen Produkte verschiedener Hersteller ein. Die Messeinrichtung eines Wettbewerbers wurde von einem Vertriebsingenieur dem LfDI vorgestellt.

Ein per Funk auslesbarer, elektronischer Wasserzähler sendet unabhängig vom Ablesen zum Zwecke der Abrechnung über ein eingebautes Funkmodul fortlaufend in kurzen Abständen verschlüsselte Datenpakete aus.

Die Abgrenzung zu „Smart Meter“ ist darin zu sehen, dass von einem solchen Wasserzähler Verbrauchsstände übermittelt werden, nicht dagegen konkrete Wasserverbräuche in beispielsweise Küche oder Bad zu unterschiedlichen Zeitpunkten. Eine Tarifbildung ist damit nicht verbunden.

Anknüpfungspunkt aus datenschutzrechtlicher Sicht ist dabei, dass die Zählernummer mit dem jeweils aktuellen Zählerstand über die Verbindung mit einer Adresse ein personenbezogenes Datum darstellt. Ein Gebührenschuldner ist bestimmbar im Sinne von § 3 Abs. 1 LDSG, da dieser mittels des in der Entgeltabteilung vorhandenen Zusatzwissens über die Zählernummer einer Person auch unmittelbar zugeordnet werden kann.

Der LfDI vertritt hier die Auffassung, dass mit der Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser, dem § 48 Abs. 1 S. 1 und Abs. 4 S.1 LWG und den einschlägigen kommunalen Satzungen eine ausreichende Rechtsgrundlage für den Einsatz oben genannter Wasserzähler zu Abrechnungszwecken vorliegt, wenn die per Funk ausgelesenen Daten am Erforderlichkeitsgrundsatz gemessen werden und bestimmte technische Anforderungen erfüllt sind (vgl. bereits Der Hessische Datenschutzbeauftragte in seinem 43. (2014) und 45. (2016) Tätigkeitsbericht).

Dieser Standpunkt wurde der Arbeitsgemeinschaft der kommunalen Spitzenverbände und dem Verband Kommunaler Unternehmen e.V. mitgeteilt und im Anschluss gemeinsam Formulierungen für die Änderung des Satzungsmusters der Allgemeinen Wasserversorgungssatzung erarbeitet. Dabei wurden auch technische Vorgaben beschrieben, damit ein unbefugtes Auslesen verhindert wird, und im öffentlichen Interesse liegende weitere Zwecke festgelegt, für die anlassbezogen bestimmte zusätzliche Daten verarbeitet werden dürfen.

14.3 Digitalisierung des Personenstandsarchivs beim Landeshauptarchiv

Das Landeshauptarchiv trat mit der Erwägung an den LfDI heran, die in der Benutzung stark nachgefragten Zweitschriften des Personenstandsarchivs zu digitalisieren und damit zu schonen und beabsichtigte, mit dieser Tätigkeit einen externen bzw. kommerziellen Dienstleister zu beauftragen.

Das Personenstandsregister beim jeweiligen Standesamt besteht aus Ehe-, Geburten- und Sterberegister und ist nach dem Ablauf bestimmter Fristen dem zuständigen öffentlichen Archiv zur Übernahme anzubieten.

Von datenschutzrechtlicher Relevanz wäre das Vorhaben insbesondere, wenn die Betroffenheit personenbezogener Daten von lebenden,

natürlichen Personen nicht ausgeschlossen werden kann oder über ein Personenstandsregister auch Aussagen über lebende Angehörige ggf. ermittelt werden können, weil aus den Registereinträgen familiäre Zusammenhänge bei bestimmten Merkmalen erschlossen werden können.

Das Vorhaben, die Zweitschriften des Personenstandsarchivs zu digitalisieren, kann zwar grundsätzlich durch einen externen bzw. kommerziellen Dienstleister als Auftragnehmer im Rahmen eines Vertrages über die Datenverarbeitung im Auftrag (§ 4 LDSG) erfolgen. Der Vorgang der Digitalisierung könnte als weisungsgebundene, technisch vorhersehbare Unterstützungsleistung und damit als Gegenstand der Auftragsdatenverarbeitung gesehen werden.

Im Raum stand aber, dass einem möglichen Dienstleister aufgrund der ansonsten anfallenden hohen Kosten als Entgelt für diese Tätigkeit die Möglichkeit eingeräumt werden soll, die Digitalisate (Dateien, in welche Dokumente mit dem Scanvorgang überführt werden) für eigene Zwecke, z.B. kostenpflichtige Nutzung durch Dritte im Internet, zu verwenden. Das Personenstandsarchiv erhielte für seine Zwecke Duplikate der Digitalisate.

Ein solcher Vorgang wäre datenschutzrechtlich aber als Übermittlung vom Landeshauptarchiv als öffentlicher Stelle an eine nicht-öffentliche Stelle einzustufen, wofür gemäß § 5 Abs. 1 LDSG entweder eine Einwilligung oder eine gesetzliche Erlaubnis vorliegen müsste.

Einschlägig ist nach der Übernahme eines Personenstandsregisters von einem Standesamt § 3 LArchG, der die Nutzung von öffentlichem Archivgut regelt. Soweit sich das Archivgut auf natürliche Personen bezieht, darf es erst zehn Jahre nach deren Tod, oder, wenn das Todesjahr dem Archiv nicht bekannt ist, erst 100 Jahre nach der Geburt der Betroffenen genutzt werden (§ 3 Abs. 3 S. 2 LArchG).

Für die Nutzung von Archivgut nach Ablauf der Sperrfrist muss eine berechtigtes Interesse dargelegt werden (§ 3 Abs. 1 S. 1 LArchG), jedoch ist die Nutzung von der Archivverwaltung im Einzelfall einzuschränken oder zu versagen, wenn u.a. Grund zu der Annahme besteht, dass schutzwürdige Belange Betroffener oder Dritter entgegenstehen (§ 3 Abs. 2 Nr. 2 LArchG).

Die von dem Dienstleister gewünschte Nutzung ist damit nach Auffassung des LfDI nicht vereinbar, weil eine Prüfung im Einzelfall nicht erfolgen kann und die Wahrung der Persönlichkeitsrechte und das daraus sich ableitende Recht auf Vertraulichkeit von Abstammungsinformationen der Betroffenen das Interesse des Dienstleisters an der Verfolgung seiner Geschäftsidee regelmäßig überwiegen dürfte. Außerdem ist es auch fraglich, ob die Archivverwaltung eine Prüfung im Sinne von § 3 Abs. 6 LArchG gewährleisten könnte.

Jedenfalls könnte dann ein Zugang zum Personenstandsarchiv für Dritte über den Dienstleister erfolgen, ohne dass die Einhaltung der dafür in § 3 Abs. 1 S. 1 und Abs. 2 Nr. 2 LArchG geregelten Voraussetzungen behördlicherseits geprüft und nur an ökonomischen Grundsätzen ausgerichtet würde.

Weiterhin ist aus datenschutzrechtlicher Sicht auch zu berücksichtigen, dass die Über¬nahme von Archivgut in ein Archiv anstelle einer Löschung im Sinne von § 19 Abs. 2 LDSG vorgesehen ist. Der mit dem datenschutzrechtlichen Löschungsgebot bezweckte Schutz wird durch die Archivierung gewährleistet. Ein gewisser Ausgleich dafür, dass eigentlich zu löschende Unterlagen im Rahmen des Archivrechts weiter genutzt werden dürfen, sind die archivrechtli-

chen Schutz- bzw. Sperrfristen.

Das oben geschilderte Vorhaben wäre mit der aktuellen Rechtslage nicht vereinbar.

15. WEITERE TECHNISCHE THEMEN

15.1 Datenschutzrelevante Aspekte beim Betrieb öffentlicher WLAN-Hotspots

Im Berichtszeitraum wurde der Landesbeauftragte mehrfach auf die für den Betrieb öffentlicher WLAN-Hotpots maßgebenden Datenschutzanforderungen angesprochen.

Der LfDI hat sich dazu folgendermaßen geäußert:

Betreiber öffentlicher WLAN-Hotspots sind „Diensteanbieter“ i.S.d. § 3 Nr. 6 Telekommunikationsgesetz Mitteilung Nr. 149/2015 im Amtsblatt der Bundesnetzagentur vom 4. März 2015). Soweit sich das Angebot auf die kurzzeitige lokal beschränkte Nutzung eines eigenen vorhandenen TK-Anschlusses beschränkt, stellt dies im Regelfall lediglich eine Mitwirkung an der Erbringung von TK-Diensten dar und kein eigenständiges Erbringen (§ 3 Nr. 6 b TKG). Dies unterliegt nicht der Meldepflicht nach § 6 Abs. 1 TKG; gleichwohl begründet die Mitwirkung an der Erbringung von TK-Diensten die Pflicht zur Wahrung des Fernmeldegeheimnisses nach § 88 TKG. Typische Konstellationen in diesem Zusammenhang sind Callshops, Internet-Cafes, Hotels, Restaurants mit WLAN-Angebot oder privat betriebene, öffentlich zugängliche Hotspots.

https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/Amtsblattmitteilung_Nr149_2015.pdf

Diese Dienste unterliegen nicht der Meldepflicht nach § 6 Abs. 1 TKG; gleichwohl begründet die Mitwirkung an der Erbringung von

TK-Diensten die Pflicht zur Wahrung des Fernmeldegeheimnisses nach § 88 TKG.

Da es sich bei den Betreibern der o.g. Hotspots nicht um eigenständige Erbringer öffentlich zugänglicher Telekommunikationsdienste handelt, unterliegen sie nicht der Pflicht zur Speicherung von Verkehrsdaten nach § 113b TKG. Weiterhin ist die Erhebung von Bestandsdaten nach § 95 TKG bei einer unentgeltlich und jeweils nur vorübergehend zugestandenen WLAN-Nutzung nicht erforderlich.

Betreiber öffentlicher WLAN-Hotspots unterliegen nach § 110 TKG i.V.m. § 3 Telekommunikationsüberwachungsverordnung (TKÜV) der Pflicht zur Umsetzung von Überwachungsmaßnahmen nicht, wenn an den Hotspot weniger als 10.000 Nutzungsberechtigte angeschlossen sind (vgl. Hinweise BNetzA).

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/WLanUeberwachung/WLanUeberwachung_node.html

Die Erhebung von Bestandsdaten wäre grundsätzlich nach § 95 TKG zulässig, wenn dies für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erforderlich wäre. Dies ist bei einer unentgeltlich und jeweils nur vorübergehend zugestandenen WLAN-Nutzung zunächst nicht der Fall. Der EUGH (Rechtssache C-484/14) hat jedoch festgestellt, dass eine Sicherungsmaßnahme, bei der die Nutzer nicht anonym handeln können, diese davon abschrecken kann, Schutzrechte zu verletzen. Allerdings darf Hotspotbetreibern keine allgemeine Verpflichtung zur Überwachung der von Ihnen übermittelten Informationen auferlegt werden.

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d610337f87162d4abe9c93846f688fac04.e34KaxiLc3eQc40LaxqMbN4Pahu-Se0?text=&docid=185304&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=117512

Betreiber von WLAN-Hotspots müssen nach der Rechtsprechung des BGH sicherstellen, dass ihr Netzwerk nicht von Dritten missbraucht werden kann. Sie sollen „zumutbare Maßnahmen“ ergreifen, um z.B. Urheberrechtsverletzungen zu verhindern. Damit kann die Nutzung von WLAN-Hotspots an bestimmte Bedingungen geknüpft werden, in die die Nutzer zuvor eingewilligt haben müssen. Die Gestaltung der Einwilligung und der Umfang der Verarbeitung personenbezogener Daten müssen dabei datenschutzrechtlichen Vorschriften entsprechen. Dies betrifft u.a. Art und Umfang der Speicherung von Verkehrsdaten (Protokollierung) sowie ihre Nutzung (Auswertung) und Löschung.

15.2 Cloud-Computing

Auf allen Geräten die gleichen Daten abzurufen, erfordert heute nicht mehr das mühselige Kopieren mit dem USB-Stick von einem Computer auf einen anderen. Stattdessen kann man alle Daten auf einem Speicherplatz im Internet, in der sogenannten Cloud, sichern und so von mehreren Geräten darauf zugreifen. So lassen sich etwa z. B. Bilder von überall angucken, ohne dass man sie lokal speichern muss – aber Cloud-Computing kann noch mehr. In diesem Beitrag werden viele interessante Aspekte beleuchtet und Tipps gegeben.

Bisher war es üblich, dass man seine Daten wie Fotos, Musik oder Dokumente auf einzelnen

Geräten wie Computer oder Laptop speichert. Das Problem an der Sache: Sobald man mehrere Geräte hat, muss man die Daten umständlich von einem zum anderen kopieren. Auch von unterwegs kann man nur auf die Daten zugreifen, die auf dem jeweils mitgeführten Gerät vorhanden sind.

So entstand der Bedarf nach einer Speichermöglichkeit, auf die von überall aus zugegriffen werden kann. Hier kommen Clouds ins Spiel, was übersetzt „Wolken“ bedeutet. Das Praktische am sogenannten Cloud-Computing ist nicht nur, dass man mit unterschiedlichsten Endgeräten auf seine Daten zugreifen kann, sondern dass es auch von überall aus funktioniert – und zwar über das Internet.

Die Anbieter solcher Cloud-Dienste stellen ihren Benutzerinnen und Benutzern dafür Speicherplatz im Netz zur Verfügung. Die Benutzerin oder der Benutzer meldet sich beim Anbieter an und kann dann von seinem Computer, Laptop, Smartphone oder Tablet auf seinen persönlichen Speicherplatz zugreifen.

Was einen so innovativen Namen hat, ist gar nicht so neu. Früher nannte man das Webspace oder Online-Speicher. Jede bzw. jeder, die oder der schon einmal eine E-Mail in einem Internetbrowser gelesen oder geschrieben hat, hat bereits einmal eine (Daten-)Wolke genutzt. Wie jeder Cloud-Dienst greift auch das E-Mail-Konto auf Speicherplatz im Internet zurück.

Allerdings sollte man darauf achten, wie umfangreich die Daten sind. Zum einen bieten kostenlose Cloud-Dienste meist nur einen begrenzten Speicherplatz an, und zum anderen benötigt das Kopieren von großen Datenmengen auch bei einer schnellen Internetverbindung viel Zeit. Ein funktionierender Internetzugang ist also Voraussetzung für die Nutzung einer Cloud. In Gebieten mit schlechter Mobilfunkversorgung kann eine unzuverlässige Verbindung zu Cloud-Diensten die Freude an der Nutzung erheblich mindern.

Zusätzlich ist bei allen Cloud-Diensten eine Registrierung beziehungsweise ein Nutzerkonto bei dem entsprechenden Anbieter erforderlich.

Es gibt die unterschiedlichsten Anbieter und Angebote. Ein deutscher Cloud-Anbieter ist die Telekom Deutschland GmbH. Andere bekannte Anbieter, in der Regel mit Sitz in den USA, sind Amazon, Apple, Google, Microsoft oder Dropbox. Die Hersteller von Betriebssystemen wie Windows oder Android bauen Zugriffsmöglichkeiten für die von ihnen betriebenen Clouds schon jetzt in ihre Produkte ein, so dass keine Zusatzsoftware notwendig ist. Wer den eigenen Cloud-Speicher auch mit dem Tablet oder Smartphone nutzen möchte, muss bei der Auswahl darauf achten, ob es dafür passende Apps gibt.

Clouds bieten auch Gefahren, denn oft weiß man nicht, wo sich die Daten genau befinden und wer alles darauf Zugriff hat.

Worauf man bei der Auswahl eines Cloud-Dienstes achten sollte

Cloud-Nutzerinnen und -Nutzer sollten darauf achten, dass die Cloud so transparent und sicher wie möglich gestaltet ist. Das bedeutet, dass die Verbraucherin oder der Verbraucher darüber informiert wird:

- wo (Land, Region) sich welche persönlichen Daten befinden,
- welche Subunternehmer noch eingeschaltet werden,
- wer Zugriff auf die Daten hat und

› welche Rechte und Pflichten der Cloud-Anbieter und welche die Cloud-Nutzerin bzw. -Nutzer hat,

› ob der Anbieter die Daten für den Transport und die Lagerung verschlüsselt.

15.3 Digitale Identitäten / Identitätsdiebstahl

In der digitalen Welt agiert man unter sogenannten digitalen Identitäten, d.h. Kennzeichen, Pseudonymen oder Kennungen, hinter denen die jeweiligen Nutzer stehen.

Wichtig ist, sich klar zu machen, über welche digitalen Identitäten man verfügt. Dies geht über die Profile in Sozialen Netzwerken hinaus und umfasst z.B. auch Accounts bei E-Mail-Servern, Online-Banking, Streaming-Plattformen, Online-Shops, Kundencentern oder anderen Online-Diensten. Aber auch in der Offline-Welt existieren digitale Identitäten wie etwa die Zugangsdaten zu Packstationen oder der E-ID-Funktion des elektronischen Personalausweises. Letztlich handelt es sich um Identifikationsmerkmale unter denen Daten, Funktionen, Berechtigungen, etc. einer bestimmten Person zugeordnet werden. Diese können (Personalausweis), müssen aber nicht (Zugangsdaten) auf einem Datenträger verkörpert sein.

So wie in der realen Welt der „gute Name“ missbraucht werden kann, kann es auch hier dazu kommen, dass digitale Identitäten unbefugt für ärgerliche oder kriminelle Zwecke genutzt werden. Dies reicht von missbräuchlich verwendeten Mailadressen, über gefälschte Profile in Sozialen Netzwerken bis hin zu ausgespähten oder gestohlenen Online-Banking-Zugängen.

Daher sollte insbesondere bei Zugangskennungen einer Wahl starker Passworte besonderes Augenmerk geschenkt werden.

Empfehlungen für die Gestaltung und Verwendung von Passwörtern existieren: (siehe zu Länge, Zeichenarten, Gültigkeit, Aufbau z.B. https://s.rlp.de/passwortgestaltung).

Darüber hinaus empfiehlt es sich, für verschiedene Dienste verschiedene Zugangsdaten zu verwenden, zumindest hinsichtlich des Passworts. Häufig verwenden Nutzerinnen und Nutzer für die Registrierung bei Online-Diensten ihre E-Mail-Adresse. Wenn hierbei auch das gleiche Passwort genutzt wird und es bei einem der Dienste zu einer Kompromittierung der Zugangsdaten kommt, sind potentiell alle genutzten Dienste betroffen.

Wenn man den Verdacht hat, dass eine der eigenen digitalen Identitäten kompromittiert worden sein könnte, sollten als erstes die Zugangsdaten geändert und der Anbieter des Dienstes unterrichtet werden. Die meisten Sozialen Plattformen bieten eine unmittelbare Kontaktmöglichkeit für derartige Vorkommnisse (siehe https://www.checked4you.de/profil-gehackt).

Je nach Schwere des Vorfalls kommt ggf. eine Strafanzeige in Betracht. Unbegründeten Rechnungen und Mahnungen sollte unmittelbar widersprochen werden. Freunde, Bekannte, Kollegen und ggf. Geschäftspartner sollten informiert werden, dass die Identitätsdaten kompromittiert wurden und ggf. missbraucht werden könnten. Schließlich sollte man versuchen, die Ursache zu klären und prüfen, ob ggf. Schadsoftware auf einem der genutzten Geräte dafür verantwortlich sein kann (Virenprüfung).

Welche Möglichkeiten bestehen, einem Miss-

brauch digitaler Identitäten vorzubeugen bzw. wie man reagieren sollte, wenn es zu einem entsprechenden Vorfall gekommen ist, ist u.a. hier dargestellt:

http://www.ndr.de/nachrichten/netzwelt/Identitaetsdiebstahl-im-Netz-was-tun-hilfe,identitaetsdiebstahl102.html
https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html

Aufgrund sich häufender Fälle gefälschter oder kompromittierter Nutzerprofile hat Facebook Ende 2015 ein besonderes Meldesystem für derartige Vorkommnisse eingeführt (http://www.heise.de/newsticker/meldung/Facebook-warnt-vor-Identitaetsdiebstahl-3150542.html). Hier können Nutzerinnen und Nutzer entsprechende Vorfälle melden und ein Profil ggf. sperren lassen.

15.4 Sicherheit der Verarbeitung und datenschutzkonforme Gestaltung von IT-Verfahren

15.4.1 Sicherheit der Verarbeitung

Eine angemessene Sicherheit bei der automatisierten Verarbeitung ist ein datenschutzrechtliches Gebot, sie liegt jedoch auch im Interesse der datenverarbeitenden Stellen. Geschäftsprozesse werden zunehmend ins Internet verlagert und IT-Strukturen durch den Einsatz mobiler Geräte und die Nutzung von Cloud-Lösungen auf Bereiche außerhalb der eigenen Organisation ausgedehnt. Die Einbindung von Geschäftspartnern, Dienstleistern und Lieferanten in Wertschöpfungsketten, E-Commerce- und E-Government-Lösungen sowie die elektronische Anbindung von Kundinnen und Kunden bzw. Bürgerinnen und Bürgern eröffnen zunehmend Zugriffsmöglichkeiten durch externe Stellen. Mit dieser fortschreitenden Digitalisierung nehmen Angriffe auf IT-Strukturen von Verwaltungen und Unternehmen zu. Informationen über Wettbewerber und Märkte, Technologien, Kundinnen und Kunden, aktuelles Know-how oder staatliche Kommunikation wecken vielfältige Begehrlichkeiten. Rheinland-Pfalz mit einer Wirtschaftsstruktur in Feldern, in denen technologische Kompetenz und Know-how von essentieller Bedeutung sind (Chemie, Fahrzeugbau, Maschinenbau etc.) und mit einer Exportquote von über 50 Prozent im verarbeitenden Gewerbe ist hier besonders exponiert.

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 ergibt sich ein Schadensvolumen zwischen zwei und vier Milliarden allein in Rheinland-Pfalz.

Die Datensicherheit ist, vor allem bei kleinen und mittleren Unternehmen und Verwaltungen oftmals jedoch noch ausbaufähig (vgl. Nr. 2). Nach einer Untersuchung des Branchenverbandes BITKOM verfügt weniger als die Hälfte der Unternehmen über einen Notfallplan für IT-Sicherheitsvorfälle und lediglich ein Viertel über eine Sicherheitsstrategie, um sich gegen Angriffe zu schützen (https://www.bitkom.org/Presse/Presseinformation/Unternehmen-muessen-bei-IT-Sicherheit-nachbessern.html). Die Roadmap der Landesregierung zum Digitaldialog nimmt daher folgerichtig die Sicherheit der Datenverarbeitung und den Aufbau sicherer IT-Strukturen in den Blick.

Die kommende Datenschutz-Grundverord-

nung sieht in diesem Zusammenhang sowohl eine standardmäßige Analyse und Bewertung der mit der automatisierten Verarbeitung verbundenen Risiken vor (Art. 25 (1), Art. 32 (1) DSGVO), als auch die Einführung eines Verfahrens mit dem die getroffenen Sicherheitsmaßnahmen und ihre Wirksamkeit regelmäßig überprüft werden (Art. 32 (1 d) DSGVO.

Risikoanalyse und IT-Sicherheits- und Datenschutzmanagement sind daher Anforderungen, die Unternehmen und Verwaltungen gleichermaßen treffen und als integraler Bestandteil von Digitalisierungsprojekten vorgesehen werden müssen.

15.4.2 Datenschutzkonforme Gestaltung von IT-Verfahren

Soweit personenbezogen Daten automatisiert verarbeitet werden, ist neben den Zulässigkeitsvoraussetzungen (z.B. Rechtsgrundlage, Unterrichtung/Einwilligung, Zweckbindung) auch die datenschutzkonforme Gestaltung in den Blick zu nehmen. Von besonderer Bedeutung ist hierbei die Einhaltung der Grundätze nach Art. 5 (1 c) (Datenminimierung), Art. 5 (1 f) (Integrität und Vertraulichkeit), Art. 25 DSGVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) sowie die Wahrung der Betroffenenrechte (Art. 13 ff. DSGVO). Hier setzt das im Auftrag der Datenschutzkonferenz entwickelte Standard-Datenschutzmodell (http://s.rlp.de/sdm) an. Es fußt auf dem Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. März 2010 und ergänzt die Ziele der IT-Sicherheit um datenschutzbezogene Schutzziele:

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Datensparsamkeit
- Transparenz
- Wahrung der Betroffenenrechte (Intervenierbarkeit)
- Sicherstellung der Zweckbindung

Das Standard-Datenschutzmodell berücksichtigt damit grundlegende Datenschutzprinzipien und ermöglicht die datenschutzgerechte Gestaltung von informationstechnischen Verfahren. Es sollte daher bei der Gestaltung von IT-Verfahren einbezogen werden.

Zentrale Aspekte einer datenschutzfreundlichen Technikgestaltung (Privacy by Design, vgl. Art. 25 DSGVO und Nr. 1) sind weiterhin Verschlüsselung und Pseudonymisierung. Diese ermöglichen es, oftmals datenschutzkritische Technologien wie Big Data und Data Mining datenschutzgerecht abzufedern. Sie eröffnen Auswertungs- und Verarbeitungsmöglichkeiten, mit denen deren Potenziale erschlossen werden können und die datenschutzrechtlichen Anforderungen dabei angemessen entsprechen.

Verschlüsselung und Pseudonymisierung sollten bei der Gestaltung von IT-Verfahren als grundsätzliche Datenschutzmechanismen berücksichtigt werden.

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497

poststelle@datenschutz.rlp.de