Datenschutzbericht

2012/2013

Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

Vierundzwanzigster
Tätigkeitsbericht nach § 29 Abs. 2
Landesdatenschutzgesetz (LDSG)
für die Zeit vom 1. Januar 2012
bis 31. Dezember 2013

LT-Drs. 16/3569

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

Umschlaggestaltung
Petra Louis

22. Mai 2014

Datenschutzbericht

2012/2013

Inhalt

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

Einführung

Gemäß § 29 Abs. 4 LDSG hat der LfDI dem Landtag alle zwei Jahre über seine Tätigkeit zu berichten. Für den Bereich des Datenschutzes wird dieser Bericht hiermit vorgelegt.

Er umfasst die Jahre 2012 und 2013. Da die redaktionellen Arbeiten an diesem Bericht erst Anfang April 2014 abgeschlossen werden konnten, wurden einige datenschutzrelevante Ereignisse aus dem 1. Quartal des Jahres 2014 noch in den Bericht mit einbezogen. Seine Aktualität soll auf diese Weise sichergestellt werden.

Es ist der 24. Tätigkeitsbericht zum Datenschutz. Die ersten fünf Berichte waren noch von einem „Ausschuss für den Datenschutz“ vorgelegt worden, die folgenden sieben von der Datenschutzkommission, und erst ab dem 13. Bericht stammen sie von dem 1991 eingerichteten Landesbeauftragten für den Datenschutz. Alle diese Berichte sind unter http://www.datenschutz.rlp.de/ abrufbar.

Sie dokumentieren nicht nur die Arbeit der in Rheinland-Pfalz für den Datenschutz verantwortlichen Stellen, sondern geben einen Überblick über die Entwicklung des Datenschutzes in den zurückliegenden Jahrzehnten, da die Bundesebene und – wo nötig – auch die europäische Ebene mit einbezogen wurden.

Ich möchte bei dieser Gelegenheit darauf hinweisen, dass die erste Fassung des rheinland-pfälzischen Landesdatenschutzgesetzes am 17. Januar 1974 vom Landtag beschlossen worden war. Nach den hessischen und den schwedischen Datenschutzregelungen war es weltweit das dritte Datenschutzgesetz. Das Land kann also seit Beginn des Jahres 2014 auf mittlerweile 40 Jahre Datenschutz zurückblicken.

Es handelt sich dabei um eine komplexe Geschichte mit vielen Entwicklungsstufen. Diese sind in einem kurzen Abriss zusammengefasst und aus Anlass des 40. Jahrestags des rheinland-pfälzischen Datenschutzgesetzes diesem Bericht in der Anlage beigefügt.

In diesen 40 Jahren gingen maßgebliche Impulse für den Datenschutz im Lande vor allem von zwei Persönlichkeiten aus: in der Zeit von 1974 bis 1991 von dem damaligen Geschäftsführer des Datenschutzausschusses und später der Datenschutzkommission Walter P. Becker, der ab 1979 auch Direktor beim Landtag war, und von 1991 bis 2007 von Prof. Dr. Walter Rudolf, dem ersten Landesbeauftragten für den Datenschutz. Sie und ihre Mitarbeiterinnen und Mitarbeiter und natürlich auch die jeweiligen Mitglieder des Datenschutzausschusses und der Datenschutzkommission haben maßgeblich dazu beigetragen, dass der Datenschutz einen hohen Stellenwert im Lande genießt.

Der vorliegende Bericht bringt zum Ausdruck, dass sich daran nichts geändert hat. Wiederum wurde der LfDI bei seiner Arbeit auf vielfältige Weise unterstützt: von den Abgeordneten aller im Landtag vertretenen Fraktionen, von der Landesregierung in ihrer jeweiligen Zusammensetzung, von der Datenschutzkommission unter ihrem Vorsitzenden, dem Abgeordneten Carsten Pörksen, und von vielen weiteren öffentlichen und privaten Stellen, die Interesse an der Arbeit des LfDI gezeigt und seine Tätigkeit gefördert haben. Diese Unterstützung war hilfreich. Ich darf mich an dieser Stelle dafür bedanken.

Danken möchte ich auch meinen Mitarbeiterinnen und Mitarbeitern für ihren engagierten Einsatz, für ihre Anregungen und ihre Unterstützung. Ihre Belastung ist unverändert groß, so wie die von ihnen und mir wahrzunehmenden Aufgaben unverändert anspruchsvoll, abwechslungsreich und spannend sind.

Edgar Wagner

I. Grundsatzfragen des Datenschutzes

Der Datenschutzbericht für die Jahre 2012 und 2013 gliedert sich in drei Abschnitte: In den beiden ersten Abschnitten werden die Grundsatzfragen des Datenschutzes erörtert und die Arbeitsschwerpunkte des LfDI dokumentiert, im dritten Abschnitt ausgewählte Ergebnisse aus der Prüfungs- und Beratungstätigkeit des LfDI vorgestellt.

Die Grundsatzfragen des Datenschutzes werden vor allem in der derzeit stattfindenden Diskussion über die digitale „Daten-Ausbeutung und Daten-Enteignung“ der Menschen gestellt (vgl. Tz. I-1.1) und in der Auseinandersetzung mit den sog. Snowden-Enthüllungen (vgl. Tz. I-2.1). Dabei geht es vor allem auch um die Notwendigkeit einer digitalen Rechtsordnung. Die Arbeitsschwerpunkte des LfDI beginnen bei seinen digitalen Bildungsmaßnahmen (vgl. Tz. II-2) und der Debeka-Datenproblematik (vgl. Tz. II-6) und reichen über den Datenschutz in Krankenhäusern (vgl. Tz. II-7.1) und in Hotels (vgl. Tz. II-7.2) bis zur Nutzung von Facebook-Fanseiten durch die Behörden des Landes (vgl. Tz. II-7.4.4).

1 Zur Situation des Datenschutzes

1.1 Die Krise des Datenschutzes

Der Datenschutz befindet sich – unabhängig von seiner Lage in Rheinland-Pfalz – seit geraumer Zeit in einer schwierigen Situation. Man kann auch sagen, er steckt in einer tiefen Krise. Zwar erlebte der moderne Datenschutz in seiner über 40-jährigen Geschichte immer wieder „ups and downs“ – Prof. Dr. Dr. h.c. Spiros Simitos, der hessische Datenschutzbeauftragte, stellte etwa kurz nach der bahnbrechenden Volkszählungsentscheidung des Bundesverfassungsgerichts 1984 im hessischen Landtag fest: „Just in dem Augenblick, in dem die Anerkennung ihren Höhepunkt erreicht, steuert der Datenschutz auf seine tiefste Krise zu.“ Doch ist die heutige Situation ernster und die Sorgen sind grundsätzlicher und tiefgreifender als vor 30 Jahren. Selten war der Ruf nach einem wirksamen Datenschutz so laut wie heute, noch war die Ratlosigkeit, wie man dem Rechnung tragen könnte, so groß wie in unseren Tagen. Das mag weniger für den staatlichen Bereich gelten, gewiss aber für den privaten, jedenfalls dort, wo digitale Technologien zum Einsatz kommen und genutzt werden, das heißt vor allem im Netz.

Ein effektiver Schutz vor unberechtigter Nutzung personenbezogener Daten lässt sich nämlich derzeit, vor allem im Internet, bei der Nutzung von Smartphones, beim Cloud Computing und im Zusammenhang mit Big Data nicht mehr oder kaum noch gewährleisten. Hier stößt der Datenschutz immer mehr an die Grenzen seiner Möglichkeiten. Jenseits dieser Grenzen findet eine weitgehend unkontrollierte Datenverarbeitung zu Lasten der Bürgerinnen und Bürger statt, denen zudem oft keine hinreichende Datensicherheit garantiert werden kann, vor allem nicht im Netz.

Zurückzuführen ist diese problematische Entwicklung – die nicht zuletzt auch in den Enthüllungen von Edward Snowden zum Ausdruck kommt (vgl. Tz. I-2.1) – vor allem auf die zunehmende Digitalisierung, die zu einer massenhaften Datenproduktion geführt hat, so dass Daten neben der menschlichen Arbeitskraft, dem Kapital und den Rohstoffen zum vierten Produktionsfaktor in der Wirtschaft geworden sind. Waren die fossilen Rohstoffe noch der Treibstoff des 20. Jahrhunderts, sind es heute im 21. Jahrhundert Daten und die mit ihnen verknüpften Informationen.

Dagegen kann – auch aus der Sicht des Datenschutzes – an sich nichts eingewendet werden, zumal die digitale Nutzung von Daten auch mit vielen Vorteilen und Innovationen und nicht zuletzt auch mit vermehrtem Wohlstand verbunden ist. Problematisch, ja gefährlich ist aber die zu beobachtende exzessive, rücksichtslose und entgrenzte Sammlung, Speicherung und Verwertung von Daten, wie sie etwa in der Geschäftsphilosophie von Facebook zum Ausdruck kommt, die ganze Welt vernetzen und von jedem das ganze Leben digital abbilden zu wollen.

Ein kleiner Baustein bei diesem anmaßendem Unterfangen bilden die derzeit 80 Milliarden

Facebook-Fotos, mit deren Hilfe rund eine halbe Milliarde Menschen weltweit identifiziert worden sind, was die Annahme rechtfertigt, dass das Unternehmen in den vergangenen Jahren die größte biometrische Datenbank der Welt aufgebaut hat, ohne dass diese oder deren mögliche Anwendungsgebiete gesellschaftlich oder staatlich kontrolliert würden.

Auch wenn viele Facebook-Mitglieder, Google-Nutzerinnen und -Nutzer und sonstige Onlinerinnen und Onliner damit einverstanden sind, dass bestimmte Daten von ihnen gesammelt, gespeichert und genutzt werden, wissen doch die wenigsten, in welch gigantischem Umfang die großen Internetunternehmen Daten und Informationen über ihre Mitglieder bzw. Kundinnen und Kunden verfügen, wozu diese Informationen sie befähigen, wem diese Daten unter welchen Bedingungen zugänglich gemacht werden und in welch irrationalem Ausmaß etwa staatliche Geheimdienste Zugang zu diesen und weiteren Daten haben.

Träten nicht Whistleblower wie Edward Snowden auf den Plan, blieben diese Zusammenhänge für die meisten Teilnehmerinnen und Teilnehmer am digitalen Kommunikationsprozess weitgehend unsichtbar, obwohl Eric Schmidt, der derzeitige Aufsichtsratschef von Google, bereits 2010 gesagt hatte: „Wir wissen, wo Du bist. Wir wissen, wo Du warst. Wir können mehr oder weniger wissen, was Du gerade denkst.“ Und das gilt nicht nur für Google, sondern auch für Facebook und damit letztlich auch für den US-amerikanischen Geheimdienst, um nur die derzeit wichtigsten „Nacktscanner“ unserer digitalen Zeit zu nennen.

Folge dieser exzessiven digitalen Datensammlung sind Machtasymmetrie und Fremdbestimmung, aber vor allem eine weitgehende digitale Ausbeutung der Menschen und ihrer Privatsphäre, wie dies kürzlich der Präsident des Europäischen Parlaments in einem Artikel der „Frankfurter Allgemeinen Zeitung“ zutreffend festgestellt hat.

Bedenkt man außerdem, dass die Mitgliedschaft bei Facebook, die Nutzung der Google-Dienste oder die Inanspruchnahme sonstiger Online-Dienste in der Regel davon abhängig gemacht wird, dass die Betroffenen sämtliche Rechte an den von ihnen preisgegebenen oder sonst erhobenen Daten an Google, Facebook und Co. abzutreten haben, liegt der Enteignungs- und Ausbeutungstatbestand auf der Hand, zumal den Betroffenen in der Regel keine Alternativen zu den jeweiligen Online-Angeboten zur Verfügung stehen. Google z.B. hat in Deutschland einen Suchmaschinen-Marktanteil von 91,2 Prozent. Da sind mögliche Alternativen allenfalls theoretischer Art.

Diese Ausbeutung hat – so Bundespräsident Joachim Gauck in seiner Rede zum Tag der Deutschen Einheit – dazu geführt, dass mittlerweile von jedem, vor allem von jenen, die im Internet unterwegs sind, digitale Zwillinge entstanden sind, die beliebigen wirtschaftlichen Zwecken zugeführt werden können, ohne dass die Betroffenen noch in der Lage wären, dies zu steuern oder gar zu verhindern. Im Gegenteil: Sie haben weitgehend die Kontrolle und Herrschaft über ihre Daten und dementsprechend auch über ihre digitalen Zwillinge verloren.

Dem Datenschutz ist es nicht gelungen, diese Entwicklung zu verhindern oder zumindest einzudämmen. Bereits aus diesem Grunde wird man heute von einer krisenhaften Situation des Datenschutzes sprechen müssen. Hinzu kommt, dass er auch nicht in der Lage war und ist, seine über die Rechte der oder des Einzelnen hinausgehende gesamtgesellschaftliche Schutzfunktion hinreichend wahrzunehmen, die nach der Rechtsprechung des Bundesverfassungsgerichts darin besteht, mit den Mitteln des Datenschutzes auch zu einer freiheitlichen demokratischen Ordnung beizutragen.

Denn wenn digitale Ausbeutung um sich greift, wird zwangsläufig die Freiheit der Onlinerinnen und Onliner eingeschränkt und das Freiheitsversprechen, das mit dem Internet verbunden war, gebrochen. Aber nicht nur die oder der Einzelne wird mit Freiheitsverlusten konfrontiert, sondern die Gesellschaft insgesamt.

In einem System, in dem – wie die Snowden-Enthüllungen gezeigt haben – staatliche Geheimdienste, global agierende Internetunternehmen

und Telekommunikationsprovider in der Lage sind, weltweit die komplette Internetkommunikation und weite Teile der sonstigen Telekommunikation der Menschen zu überwachen und auszuwerten, ohne dass Datenschützerinnen und Datenschützer oder sonstige staatliche Stellen in der Lage gewesen wären, die Bürgerinnen und Bürger vor solchen Übergriffen zu schützen, ist unsere freiheitliche Ordnung und die Loyalität der Bürgerinnen und Bürger zu ihrem Staat gefährdet. Zu Recht war deshalb in einem Artikel der „Zeit“ vom 10. April 2014 davon die Rede, dass das sanktionslose Zusammenwirken privater Datenkraken und staatlicher Geheimdienste am Fundament staatlicher Legitimität nage.

Es ist nicht davon auszugehen, dass sich diese Situation in absehbarer Zeit zum Positiven ändern könnte. Im Gegenteil: Die technologische Entwicklung wird dazu führen, dass weitere Lebensbereiche in digitalen Datenspuren abgebildet werden, was die Menschen auch in ihrem Verhalten, ihren Gefühlen und ihren Gedanken durchsichtiger machen und dem Staat und der Wirtschaft Zugriffe auf bisher noch verschlossene Bereiche ermöglichen wird. Vor allem das im Entstehen begriffene „Internet der Dinge“ wird diese Entwicklung maßgeblich befördern.

Die Zukunft des Datenschutzes wird deshalb davon abhängen, ob und in welchem Umfang es gelingen wird, diese Entwicklung aufzuhalten und auf eine dem Menschen, seinem Maß und seiner Würde entsprechende Weise zu beschränken. Skepsis ist angebracht, weil es den Anschein hat, als sei die Notwendigkeit von Gegenstrategien den politischen Entscheidungsträgern, den Verantwortlichen in der Wirtschaft, den Medienmacherinnen und -machern und den Netzaktivistinnen und -aktivisten erst durch die Snowden-Enthüllungen bewusst geworden. Fertige Konzepte liegen jedenfalls noch nicht vor. Im Gegenteil: Erst jetzt beginnt – zum Beispiel in der „Frankfurter Allgemeinen Zeitung“ – eine breite Diskussion darüber, auf welche Weise der digitalen Ausbeutung der Menschen wirksam begegnet werden könnte.

Während die Einen die Notwendigkeit einer neuen digitalen Rechtsordnung betonen, erwarten Andere die entscheidende Gegenwehr von einer solidarisierten Bürgerbewegung, einem Bündnis für eine freiheitliche Digitalisierung unserer Gesellschaft; wiederum Andere plädieren für innereuropäische Online-Dienste, wie etwa die sog. Schengen-Cloud oder das Schengen-Routing, oder sehen die notwendige Hilfe in technischen Lösungen, die es den Menschen erlauben, sich selbst wirksam zu schützen. Wahrscheinlich muss alles zusammenkommen, um einen hinreichenden Datenschutz und eine freiheitliche Ordnung in unserer digitalen Zeit gewährleisten zu können.

Und selbst das wird nicht ausreichen, wenn diese Maßnahmen nicht auch durch wettbewerbsrechtliche Konsequenzen des Europäischen Kartellamtes ergänzt werden. Denn Google und Facebook sind marktbeherrschende Unternehmen, die ihre Stellung zum Schaden ihrer Konkurrenten, der Gesellschaft und damit auch der Bürgerinnen und Bürger und ihres Datenschutzes ausnutzen.

Die Voraussetzungen für solche Maßnahmen und Entwicklungen sind allerdings nicht günstig. Eine globale Verständigung auf rechtsverbindliche und einheitliche Datenschutzgrundsätze ist nicht zu sehen, auch nicht eine gegenseitige Anerkennung unterschiedlicher regionaler Datenschutzregelwerke. Selbst innerhalb Europas stehen unterschiedliche Datenschutztraditionen einer zügigen Modernisierung im Wege, wie die Beratungen zur europäischen Datenschutz-Grundverordnung zeigen.

Eine solidarisierte Bürgerbewegung, die sich geschlossen gegen digitale Ausbeutung zur Wehr setzt, wird in einer „atomisierten Gesellschaft“ wie der unsrigen kaum noch herzustellen sein. Es überrascht auch nicht, dass allen Umfragen zufolge nur gut zehn Prozent der Deutschen persönliche Konsequenzen für den Schutz ihrer Daten aus dem NSA-Skandal gezogen haben, der bereits zuvor schon keine nennenswerten Proteste in der Bevölkerung ausgelöst hatte.

Soziale Gegenbewegungen, die als Folge der industriellen Revolution entstanden waren, sind jedenfalls in Zeiten der digitalen Revolution noch nicht vorhanden, auch deshalb nicht, weil sich die

Wortführerinnen und Wortführer der Netzgemeinde noch längst nicht über die einzuschlagende Richtung einig sind und weil die Menschen die immateriellen Folgen ihrer digitalen Ausbeutung nicht unmittelbar zu spüren bekommen.

Im Übrigen sind digitale Sicherheitslösungen und Verschlüsslungstechnologien, die massentauglich wären, noch nicht einmal in Ansätzen zu erkennen. Das Internet beruht häufig auf unsicheren Strukturen. Es wird Zeit brauchen, die notwendige Sicherheit zu implementieren.

Es passt in das negative Gesamtbild, dass offenbar auch die Europäische Kommission nicht gewillt ist, etwa den gegen Google erhobenen Wettbewerbsbeschwerden Rechnung zu tragen. Ihre Vergleichsüberlegungen stellen den Gesichtspunkt des freien Datenverkehrs vor alle übrigen schutzwürdigen Interessen, vor allem vor die Notwendigkeit eines effektiven Datenschutzes.

Dieser Befund ändert allerdings nichts daran, dass u.a. eine effektive digitale Rechtsordnung, hinreichende technologische Sicherheitsstandards, eine solidarisierte Bürgerbewegung und wettbewerbsrechtliche Maßnahmen notwendig sind. Diese Maßnahmen müssen aber vor allem von dem Bemühen begleitet werden, den Menschen die notwendigen Kenntnisse von den neuen digitalen Kommunikationsbedingungen und Kommunikationsregeln zu vermitteln und sie dafür zu sensibilisieren, dass ihre persönlichen Daten nicht nur für Google, Facebook und WhatsApp von großem Wert sind, sondern auch für sie selbst und ihre Freiheit. Insoweit ist der Datenschutz mehr den je auch eine Bildungsaufgabe, die allerdings trotz aller Bemühungen immer noch nicht mit der notwendigen Konsequenz wahrgenommen wird.

Mehr denn je ist der Datenschutz also eine Baustelle. Ins Gewicht fällt, dass manche die Arbeit an dieser Baustelle eingestellt haben, zum Teil auch noch die Baupläne fehlen, während gleichzeitig die künftigen Bewohnerinnen und Bewohner auf der Straße warten und nicht einziehen können.

1.2 Rheinland-pfälzische Reaktionen

Von Rheinland-Pfalz aus lässt sich die digitale Enteignung und Ausbeutung der Menschen weder verhindern noch reduzieren. Dafür bedarf es prinzipieller Richtungsentscheidungen, und zwar auch in globalen Dimensionen.

Das heißt aber nicht, dass die Bundesländer ratlos abseits stehen dürften. Es gibt Einflussmöglichkeiten über den Bundesrat, die – wie bereits im letzten Tätigkeitsbericht kritisiert – nicht ausreichend genutzt werden. Vor allem aber kann in den Ländern – mehr als durch den Bund und die Europäische Union – die Sensibilität der Bürgerinnen und Bürger für die digitale Entwicklung und ihre gesellschaftlichen Auswirkungen gefördert werden.

Unter dem Stichwort „Medienkompetenz“ wurde gerade in Rheinland-Pfalz vieles erreicht, aber auch manches unterlassen. Positiv hervorzuheben ist insbesondere, dass für die Haushaltsjahre 2014 und 2015 wieder erhebliche Mittel zur Förderung der digitalen Medienkompetenz zur Verfügung gestellt worden sind. So sehr es im Übrigen zu begrüßen war, dass vor knapp zwei Jahren eine fraktionsübergreifende Große Anfrage zur „Förderung von Medienkompetenz“ gestellt und von der Landesregierung wenig später auch beantwortet worden war (LT-Drs. 16/1478), so bedauerlich ist es, dass diese Antwort bisher nicht im Landtag oder in einem seiner Ausschüsse besprochen worden ist, obwohl dafür durchaus Anlass bestehen würde. Denn die Antwort zeigt auf der einen Seite das große Engagement in Sachen Medienkompetenz, sie belegt andererseits aber auch, dass dieses Engagement besser koordiniert und fokussiert werden könnte als dies zur Zeit geschieht. Im Übrigen stellt sich natürlich auch die Frage, welche Konsequenzen vor dem Hintergrund einer allgemeinen digitalen Datenenteignung aus der Antwort auf diese Große Anfrage gezogen werden müssen.

Unabhängig davon ist es aber besonders hervorzuheben, dass die rheinland-pfälzische Ministerpräsidentin den angesprochenen Fragestellungen erhebliche Aufmerksamkeit zukommen lässt. Sie hat zu Beginn ihrer Amtszeit einen Landesrat für

digitale Entwicklung und Kultur eingesetzt, bald nach den ersten Snowden-Enthüllungen einen Runden Tisch unter Einbeziehung der Datenschutzbeauftragten gefordert, dafür gesorgt, dass der seit zwei Jahren angekündigte sog. MedienkomP@ss zumindest in Ansätzen in rheinland-pfälzischen Schulen eingesetzt wird, und sie hat mit einem Besuch eines vom LfDI durchgeführten Datenschutzworkshops deutlich gemacht, dass ihr die digitale Bildung von Schülerinnen und Schülern ein besonderes Anliegen ist.

All das ist wichtig und aus der Sicht des Datenschutzes sehr zu begrüßen. Angesichts der Dimension der Gesamtproblematik reicht es allerdings nicht aus.

2. Datenschutz in Zeiten von NSA und PRISM

2.1 Die Enthüllungen Edward Snowdens und der Umgang mit ihnen

Der Deutsche Bundestag hat 2010 bei der Einsetzung der Enquete-Kommission „Internet und digitale Gesellschaft“ das Internet als das „freiheitlichste und effizienteste Informations- und Kommunikationsforum der Welt“ bezeichnet. Diese Feststellung ist durch die Snowden-Enthüllungen widerlegt worden. Sie war zu keiner Zeit richtig.

Zwar wurde und wird es immer noch als Ausdruck von Freiheit im Netz verstanden, dass es auf nationaler und erst recht auf europäischer und internationaler Ebene nur einen sehr rudimentären Rechtsrahmen für netzbasierte Kommunikation gibt, so dass Internetnutzerinnen und -nutzer jedenfalls nicht durch Gesetze daran gehindert werden, im Netz hierhin oder dorthin zu gehen, dies oder jenes zu sagen, mit der einen oder mit dem anderen Kontakt aufzunehmen.

Dieser Form von Freiheit stehen aber massive Freiheitsbeschränkungen gegenüber. Sie ergeben sich bereits aus der monopolartigen und netzbeherrschenden Stellung von Google, Facebook und Co., die den Nutzerinnen und Nutzern kaum noch eine wirkliche Alternative zu diesem sozialen Netzwerk oder zu jener Suchmaschine offen lassen. Freiheitsbegrenzend wirkt es sich auch aus, dass jeder Vorgang im Netz, insbesondere jeder Kommunikationsvorgang, digitale Spuren hinterlässt, Inhalts- und Metadaten, die nicht nur erfasst, gespeichert und ausgewertet, sondern ihrerseits im Netz auch kopiert, weiterverarbeitet und neu zusammengeführt werden können, so dass ein riesiges Datenmeer entstanden ist, für das sich der Begriff „Big Data“ etabliert hat. „Big Data“ verliert niemanden aus dem Auge. Selbst im größten Datenmeer lassen sich jedermanns Daten in Sekundenschnelle aufspüren.

Mehr als jede andere Technologie trägt deshalb die digitale Technologie den Schlüssel zur Registrierung, Kontrolle und Überwachung der Menschen in sich. Das Internet und erst recht das im Entstehen begriffene „Internet der Dinge“ bringen deshalb nicht nur Vorteile und Annehmlichkeiten, Innovationen und Wirtschaftswachstum, Bildungschancen und neue Teilhabemöglichkeiten mit sich, sondern begründen auch die Gefahr der gläsernen Verbraucherinnen und Verbraucher und der gläsernen Bürgerinnen und Bürger und damit die Gefahr einer Überwachungsgesellschaft und eines Überwachungsstaats. Die digitale Freiheit könnte sich – wenn sie nicht effektiver als bisher geschützt wird – als Chimäre erweisen.

Dass diese Gefahr nicht nur theoretischer oder abstrakter Natur ist, sondern konkrete Bezugspunkte hat, und zwar auch in westlichen Demokratien, wissen wir seit den Enthüllungen Edward Snowdens, die im Juni 2013 mit der Veröffentlichung geheimer NSA-Dokumente im britischen „Guardian“ und in der US-amerikanischen „Washington Post“ begonnen haben und seither auch in anderen Medien wie dem „Spiegel“ fortgesetzt werden, wobei die Öffentlichkeit vor allem darüber unterrichtet wurde und wird, wer von den Ausspähaktionen der NSA und dem britischen GCHQ (Government Communications Headquarters) auf welche Weise, in welchem Umfange und mit wessen Hilfe betroffen ist. Durch diese Enthüllungen wurde bekannt, dass vor allem von der NSA Staatsoberhäupter und ranghohe Politikerinnen und Politiker überwacht werden, aber auch die Europäische Kommission, das Europäische Parlament und der Europäische Rat sowie Wirtschaftsunternehmen und Bürgerinnen und Bürger in allen Teilen dieser Erde, wobei nicht nur, aber vor allem deren Internetkommunikation von den Ausspähaktionen erfasst werden.

Es geht um Verbindungsdaten von Telefongesprächen, von SMS, E-Mails und Chats, um Standortdaten von Mobiltelefonen und um vieles mehr. Dabei werden transatlantische Unterseekabel ebenso „angezapft“ wie die Datenspeicher von Google, Facebook und Co. und die Datenbestände von Telekommunikationsunternehmen wie der British Telecom und Vodafone oder des belgischen Providers Belgacom. Die entsprechenden Programme heißen u.a. PRISM, TEMPORA,

DISHFIRE und XKeyscore, wobei offenbar auch Verschlüsselungstechniken keinen vollständigen Schutz garantieren. Computer und Smartphones werden mit Spionagesoftware infiltriert, wobei die NSA offenbar auch in der Lage ist, Google-Cookies für ihre Übergriffe zu nutzen.

Auch wenn davon auszugehen ist, dass bisher erst ein Teil der Snowden-Dokumente veröffentlicht wurde, rechtfertigen bereits die bekannt gewordenen Geheimdokumente die Feststellung, dass keine Kommunikationsform so weitgehend und zugleich so weltumspannend überwacht wird, wie die Internetkommunikation, was letztlich – wie gesagt – auch darauf zurückzuführen ist, dass die großen US-Internetfirmen und große Telekommunikationsunternehmen in die globalen Überwachungsaktivitäten der Geheimdienste eingebunden waren und offenbar immer noch eingebunden sind.

In Zeiten von Big Data stellen sich deshalb die NSA und der britische Geheimdienst sowie Google, Facebook und Co. als eine Art „Big Brother-Allianz“ des Internets dar.

Für die entsprechenden Überwachungsstrukturen sind vor allem zwei Umstände entscheidend. Sie betreffen die normativen Grundlagen und die technischen Kompetenzen. In den USA gelten andere rechtliche Rahmenbedingungen, insbesondere erheblich geringere Datenschutzstandards als in Europa, insbesondere in Deutschland. Hinzu kommt, dass die USA in der Lage sind, ihre defizitären Standards auch im Internet und im World Wide Web und damit auch gegenüber den deutschen Internetnutzerinnen und -nutzern durchzusetzen. Das eine – die normativen Inhalte – sind nicht nur, aber ganz wesentlich auf 9/11 zurückzuführen, das andere – die technologische Dominanz und digitale Überlegenheit – darauf, dass das Netz bereits US-amerikanische Wurzeln hat und dann in erster Linie auch im amerikanischen Silicon Valley weiterentwickelt worden ist. Ausdruck dieser US-amerikanischen Internetdominanz sind die das Internet beherrschenden Großunternehmen wie Google, Facebook, Amazon und Apple, die ihren Sitz in den Vereinigten Staaten haben. Gleiches gilt für die Hersteller technischer Netzwerkkomponenten.

Selbst die zur Verwaltung des Internets eingerichtete Organisation ICANN (Internet Corporation for Assigned Names and Numbers) hat ihren Sitz in den USA; leitende Funktionen sind häufig mit US-amerikanischen Mitarbeiterinnen und Mitarbeitern besetzt. Das hat zur Folge, dass auf der einen Seite die USA die Regeln im Netz bestimmen und auf der anderen Seite der Rest der Welt sich – jedenfalls derzeit – kaum dagegen zur Wehr setzen kann, wobei sich nach dem Willen der USA daran auch in Zukunft nichts ändern soll. In seiner Rede zum NSA-Skandal bemerkte der amerikanische Präsident, dass er seine Behörden nicht dafür tadeln könne, wenn sie effektiver seien als die Behörden anderer Staaten. Darum geht es also: möglichst effektiv und lückenlos zu überwachen.

All das hat gravierende Konsequenzen für den Kreis der Überwachten. Zu diesen Konsequenzen zählt die Befürchtung vieler Internetprotagonisten, dass das Netz als Medium der Demokratie, der Freiheit und der Selbstbefreiung zerbrochen sei. Diese Befürchtung wird in dem Satz: „Das Internet ist kaputt“ (Sascha Lobo) und in der Feststellung zusammengefasst: Das freie Internet sei „eine fixe Idee“. Tatsächlich funktioniere es „als Überwachungsmaschine“ (Jacob Appelbaum).

Aber der von der NSA und ihren Helfern angerichtete Schaden betrifft nicht nur das Netz und seine verschiedenen Funktionen. Er betrifft vor allem die Internetnutzerinnen und -nutzer und deren vom Bundesverfassungsgericht begründeten und für das Internetzeitalter weiterentwickelten Datenschutzgrundrechte. Gemeint sind das eng mit der deutschen Geschichte verwobene Recht, grundsätzlich selbst über die Preisgabe der eigenen Daten zu entscheiden (informationelles Selbstbestimmungsrecht; vgl. BVerfGE 65, 1) und der „Anspruch auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (sog. Internetgrundrecht; vgl. BVerfGE 120, 274). Beide Rechte werden mittlerweile bereits als „Ladenhüter“ bezeichnet. Jedenfalls sind derzeit keine Grundrechte so bedroht, wie diese beiden Rechte und das Fernmeldegeheimnis. Sie sind bedroht vor allem durch die NSA und den britischen Geheimdienst, aber auch durch die großen Internetfirmen, die privateste Informa-

tionen ins Netz saugen, auf diese Weise digitale Abbilder der Menschen erzeugen, um sie dann wirtschaftlich zu verwerten oder für staatliche Zwecke bereitzuhalten.

All dies hat mit „Freiheit im Netz“ nichts zu tun. Im Gegenteil: Es gefährdet unsere freiheitliche Ordnung insgesamt, wie Bundespräsident Joachim Gauck zu Beginn der Snowden-Enthüllungen zu Recht festgestellt hat. Man kann anmerken, dass Teil dieser freiheitlichen Ordnung auch unsere Wirtschaftsordnung ist, die ebenfalls beeinträchtigt wird, weil ein Teil der Spähaktionen vermutlich nichts anderes darstellt als Wirtschaftsspionage.

In den vergangenen Monaten haben sich viele staatliche Stellen und zivilgesellschaftliche Einrichtungen, aber auch viele besorgte Bürgerinnen und Bürger in unserem Land, in anderen Staaten, nicht zuletzt in den USA, mit diesem Sachverhalt und den daraus erwachsenen Gefahren befasst und viele Vorschläge entwickelt, wie den Überwachungsexzessen im Internet begegnet werden könnte.

Die UN-Vollversammlung hat im Dezember 2013 eine unter Federführung Deutschlands und Brasiliens erarbeitete Resolution zum Schutz der Privatsphäre im digitalen Zeitalter – wenn auch auf Druck der USA in abgeschwächter Form – angenommen (Deutsch-brasilianische UNO-Resolution vom 18. Dezember 2013 „Das Recht auf Privatheit im digitalen Zeitalter“, http://www.auswaertiges-amt.de/cae/servlet/contentblob/660690/publicationFile/186832/131127_Right2Privacy_DE.pdf)

Das Europäische Parlament hat seinen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) mit der Aufklärung des NSA-Skandals und mit der Erarbeitung von Konsequenzen beauftragt. Sein Bericht liegt jetzt vor. Die Europäische Kommission hat versucht, die Beratungen des Entwurfs einer Europäischen Datenschutz-Grundverordnung (vgl. Tz. I-3.2.2) im Lichte des NSA-Skandals neu zu strukturieren und zu forcieren. Der Europäische Gerichtshof für Menschenrechte wird sich aufgrund einer Beschwerde von Bürgerinnern und Bürgern aus verschiedenen europäischen Staaten ebenfalls mit den Überwachungsvorgängen befassen.

Der Deutsche Bundestag hat u.a. in einer Sondersitzung dieses Thema behandelt und jetzt einen parlamentarischen Untersuchungsausschuss dazu eingesetzt. Die Bundesregierung hatte schon am 19. Juli 2013 ein Acht-Punkte-Programm für einen besseren Schutz der Privatsphäre verabschiedet und in einem Folgebericht am 18. August 2013 über erste Konsequenzen berichtet (Acht-Punkte-Programm der Bundesregierung zum besseren Schutz der Privatsphäre, http://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html; Fortschrittsbericht des Bundesministeriums des Innern und des Bundesministeriums für Wirtschaft und Technologie vom 14. August 2013 „Maßnahmen für einen besseren Schutz der Privatsphäre“, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Pressemitteilungen/2013/08/bericht.pdf?__blob=publicationFile).

Nach der Bundestagswahl haben sich die neuen Koalitionspartner mit „Konsequenzen aus der NSA-Affäre“ befasst und verschiedene Maßnahmen angekündigt: neben einem Abkommen zum Schutz vor Spionage u.a. die Verpflichtung der europäischen Telekommunikationsanbieter, ihre Kommunikationsverbindungen mindestens innerhalb der EU zu verschlüsseln, und das an diese Provider gerichtete Verbot, ihre Daten anderen ausländischen Nachrichtendiensten zugänglich zu machen.

Verschiedene Landesparlamente und Landesregierungen haben das Thema aufgegriffen, nicht zuletzt in Rheinland-Pfalz, wo Ministerpräsidentin Malu Dreyer noch vor der Bundestagswahl einen Runden Tisch mit Vertretern des Bundes, der Länder und der Datenschutzbeauftragten angeregt hatte, die sich zuvor bereits in einer eigenen Entschließung auf ein Maßnahmepaket zur Eindämmung von Überwachungsexzessen verständigt hatten.

Viele Stellungnahmen, Appelle und offene Briefe aus der Gesellschaft kommen hinzu. 560 Schriftsteller aus aller Welt, darunter einige Literatur-

nobelpreisträger, haben in 32 Zeitungen den Aufruf zur Verteidigung der „Demokratie in der digitalen Welt“ veröffentlich. Mehr als 200 Wissenschaftler haben ebenfalls einen Aufruf veröffentlicht, in dem sie die Nationalstaaten auffordern, die Macht der Geheimdienste zu begrenzen und sie besser zu kontrollieren. Bereits Ende Oktober 2013 hatte der BITKOM als Branchenverband der Internetwirtschaft ein Positionspapier für mehr Datenschutz und Datensicherheit vorgelegt (BITKOM-Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit vom 31. Oktober 2013, http://www.bitkom.org/files/documents/BITKOM-Positionspapier_Abhoermassnahmen.pdf). Zu erwähnen ist schließlich auch, dass es am 11. Februar 2014 einen weltweiten Aktionstag gegen die NSA-Überwachung gegeben hat. Unter dem Motto „Today we fight back“ wurden auf über 6.000 Webseiten Banner gegen die Massenüberwachung durch Geheimdienste gezeigt.

Immer wieder haben die Medien über die neusten Enthüllungen und über die Reaktionen aus Politik und Gesellschaft berichtet, auch über die Reaktionen aus den USA, wo sich zwar einerseits Kritik und Widerstand gegen die NSA-Bespitzelungen formiert, andererseits US-Präsident Barack Obama am 17. Februar 2014 angekündigt hat, keine grundsätzlichen Abstriche am Umfang der geheimdienstlichen Überwachungsaktionen machen zu wollen. Lediglich das Mobiltelefon der Bundeskanzlerin soll künftig nicht mehr ausgespäht werden.

Es ist bemerkenswert, dass diese intensive öffentliche Debatte von der Bevölkerung eher mit Gleichmut und Achselzucken wahrgenommen wird. Den vorliegenden Umfragen zufolge werden die Geheimdienstaktionen zwar weder gutgeheißen noch akzeptiert, großer Unmut oder gar Empörung ist aber kaum festzustellen. Laut ZDF-Politbarometer vom Januar 2014 stehen Datenschutz und Datensammlung durch Geheimdienste sechs Monate nach Beginn der Snowden-Enthüllungen nur auf Platz 15 der wichtigsten Probleme in Deutschland. Nur drei Prozent der Befragten fühlen sich dadurch belastet. In der Bevölkerung hat sich eine „Das-war-doch-klar“-Haltung breitgemacht.

Die Gründe dafür liegen auf der Hand. Während einerseits beinahe täglich neue Überwachungsaktivitäten der NSA und des britischen Geheimdienstes bekannt werden, scheinen fast alle Gegenmaßnahmen und Gegenvorschläge ins Leere zu gehen. Jedenfalls ist für die Bürgerinnen und Bürger nicht zu erkennen, dass ihr Staat in der Lage wäre, sie effektiv vor den digitalen Überwachungsmaßnahmen der Geheimdienste und der Beteiligung von Google, Facebook und Co. effektiv zu schützen.

2.2 Forderungen des LfDI

Vor diesem Hintergrund hält der LfDI ein Maßnahmenpaket zur Wiedergewinnung digitaler Freiheit und zur Sicherung der digitalen Grundrechte für erforderlich. Es besteht aus zwölf Punkten, zu denen etwa die Forderung nach Sanktionen, nach Abschluss diverser Abkommen mit den USA und nach Erlass neuer Datenschutzregelungen gehören. Im Einzelnen geht es um folgende Vorschläge:

1. Aufklärung:

Bundestag und Bundesregierung haben sich weiter um die Aufklärung der Überwachungssachverhalte zu bemühen. Dies ist ein Gebot notwendiger Transparenz und muss die Aktivitäten der deutschen Geheimdienste mit einschließen.

2. Sanktionen:

Da die Überwachungsaktivitäten der US-amerikanischen und britischen Geheimdienste sich auch gegen deutsche Staatsbürgerinnen und -bürger richten und jedenfalls zum Teil von deutschem Boden aus durchgeführt wurden und womöglich immer noch werden, verstoßen sie gegen deutsches Recht. Es muss deshalb darauf hingewirkt werden, dass die Bundesanwaltschaft ihr derzeitiges Prüfverfahren in ein offizielles Ermittlungsverfahren überleitet. Unterbleibt dies, wird der Eindruck staatlicher Hilflosigkeit noch verstärkt werden.

3. Prinzipien:

Der Untersuchungsausschuss des Europäischen Parlaments hat in seinem Abschlussbericht vom 8. Januar 2014 darauf hingewiesen, dass auch im

Internet rechtsstaatliche Prinzipien gelten müssen, an die jedes staatliche Handeln zu binden sei. So wie am Anfang von Demokratie und Rechtsstaat der Schutz der persönlichen Freiheit vor willkürlicher Festnahme gestanden habe (Habeas-Corpus-Akte), müsse dieses Prinzip in unseren digitalen Zeiten auch auf die Erfassung des im Netz vorhandenen Persönlichkeitsbildes ausgeweitet werden. Diese Auffassung sollte unterstützt werden.

4. Abkommen:

- Notwendig sind gesetzlich zu ratifizierende Geheimdienstabkommen zwischen den USA und Deutschland sowie auf europäischer Ebene (sog. Anti-Spionage-Abkommen), in denen die grundgesetzlich geforderten Grenzen für geheimdienstliche Aktivitäten ebenso zu regeln sind wie Möglichkeiten, die Einhaltung dieser Grenzen zu überprüfen.
- Soweit die USA nicht zum Abschluss eines solchen Abkommens bereit sind, sollten das mit den USA vereinbarte Abkommen zur Überwachung des Zahlungsverkehrs (SWIFT-Abkommen), das sog. Fluggastdatenabkommen und das Safe Harbor-Abkommen ausgesetzt bzw. gekündigt werden.
- Zwischen der Europäischen Union und den USA muss außerdem ein Datenschutzrahmenabkommen geschlossen werden, durch das den EU-Bürgerinnen und Bürgern wirksame Rechtsmittel gegen die Nutzung ihrer Daten durch US-Behörden eingeräumt wird.
- Ebenso muss das zwischen den USA und der Europäischen Union abgeschlossene sog. Safe Harbor-Abkommen neu verhandelt und nach Maßgabe der von der Europäischen Kommission vorgelegten Vorschläge überarbeitet werden, damit sichergestellt werden kann, dass die aus wirtschaftlichen Gründen stattfindenden Übermittlungen von EU-Bürgerdaten in die USA den EU-Datenstandards entsprechen. Dies ist derzeit offenkundig nicht der Fall. Sollten sich die USA nicht auf eine substantielle Überarbeitung einlassen, ist das Abkommen zu kündigen.
- Das derzeit von der Europäischen Union und den USA angestrebte Freihandelsabkommen darf nur abgeschlossen werden, wenn es Regelungen für einen effektiven Datenschutz enthält und die Einhaltung dieser Bestimmungen sichergestellt werden kann.
- Das Zusatzabkommen zum NATO-Truppenstatut sollte mit dem Ziel geändert werden, die verfassungsrechtlich gebotenen Datenschutzstandards bei der einschlägigen Datenerhebung und -verwendung zu sichern. Das Gleiche gilt für die Verwaltungsvereinbarungen, die derzeit noch eine Zusammenarbeit von Deutschen und US-amerikanischen Geheimdiensten zulassen.

5. Regelungen:

- Auf der Ebene der Vereinten Nationen muss der datenschutzrechtliche Gehalt von Art. 17 UN-Zivilpakt durch ein Zusatzabkommen präzisiert werden, damit ein besserer Schutz vor der flächendeckenden Erfassung und Rasterung der digitalen Kommunikation erreicht werden kann. Entsprechende Forderungen der Bundesregierung sollten unterstützt werden.
- Auf europäischer Ebene muss die Datenschutz-Grundverordnung möglichst zeitnah realisiert werden, wobei vor allem sicherzustellen ist, dass die auf Druck der US-Regierung aus dem Entwurf der Datenschutz-Grundverordnung gestrichene sog. „Anti-Fisa-Klausel“ wieder in den Verordnungstext aufgenommen wird. Auf diese Weise soll sichergestellt werden, dass Internet- und Telekommunikationsunternehmen Daten von EU-Bürgerinnen und Bürgern nur noch dann an Behörden von Drittstaaten (z.B. den USA) weitergegeben dürfen, wenn es dafür eine gesetzliche Grundlage gibt und/oder die Weitergabe gemeldet bzw. genehmigt wird, etwa von den Datenschutzaufsichtsbehörden. Entsprechende Vorschläge der alten Bundesregierung liegen bereits vor.
- Da damit zu rechnen ist, dass die europäischen Regelungen möglicherweise erst mit erheblicher Verspätung in Kraft treten werden, sind auch nationale Regelungen für einen besseren Schutz im Internet zu verabschieden. Das vom Bundesverfassungsgericht entwickelte sog. Internetgrundrecht (Anspruch auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, vgl. BVerfGE 120, 274; vgl. Tz. I-2.8) ist insbesondere vom Bundesgesetzgeber bisher fast völlig ignoriert worden. Mit entsprechenden Ergänzungen des

Telemediengesetzes ließen sich diese Defizite – jedenfalls mit Blick auf soziale Netzwerke und sonstige Internetdienste – beheben.

6. Deutsche Nachrichtendienste:

- Entsprechend den Forderungen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) des Europäischen Parlaments ist die Tätigkeit der Deutschen Nachrichtendienste zu überprüfen und – wenn notwendig – zu ändern, um sicherzustellen, dass diese in Übereinstimmung mit der Europäischen Menschenrechtskonvention tätig werden und ihre Aktivitäten mit den fundamentalen Rechten auf Datenschutz, Privatheit und der Unschuldsvermutung vereinbar sind.
- In Übereinstimmung mit den Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist insbesondere sicherzustellen, dass die Kontrolle der Nachrichtendienste durch eine Erweiterung der Befugnisse und eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert wird und bestehende Kontrolllücken geschlossen werden. Dabei ist auch zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden sollen.
- Die Informationsfreiheitsgesetze des Bundes und der Länder sollten zur Herstellung größerer Transparenz jedenfalls grundsätzlich auch auf die Tätigkeit der Nachrichtendienste angewendet werden können.

7. Internetstrukturen:

- Es bedarf einer nationalen bzw. europäischen IT-Strategie, um sich auch im Netz gegenüber den USA behaupten zu können. Ziel muss der Aufbau einer eigenen europäischen Kommunikations- und Informationsstruktur sein, was auch die Förderung europäischer, nationaler und lokaler Cloud-Lösungen mit einschließt. Große europäische Unternehmen und Initiativen im Luft- und Raumfahrtbereich sind dafür gute Vorbilder.
- Außerdem ist zu prüfen, ob für Datenströme, deren Ausgangspunkt und Ziel in Deutschland bzw. der Europäischen Union oder im Schengenraum liegen, die Wegewahl (Routing) so gesteuert wird, dass diese in nationalen Netzen bzw. in Netzen des Schengenraums verbleiben. Transatlantische Kommunikationswege mögen im Einzelfall wirtschaftlicher oder schneller sein, sicherer oder vertrauenswürdiger sind sie nur bedingt. Ergänzend zur Verschlüsselung können nationale Routing-Vereinbarungen ein weiterer Sicherheitsbaustein in einem Konzept zur Sicherung der Vertraulichkeit und Vertrauenswürdigkeit von Kommunikationsstrukturen sein.
- Außerdem ist der Frage nachzugehen, ob und in welchem Umfang die infolge der NSA-Übergriffe vor allem aus der Netzgemeinde vorgelegten Vorschläge für ein dezentrales Netz und den Einsatz von freier Software gefördert werden können.

8. IT-Sicherheit:

- Die europäischen Telekommunikationsanbieter sollen – wie im Koalitionsvertrag vereinbart – verpflichtet werden, ihre Kommunikationsverbindungen mindestens innerhalb der Europäischen Union zu verschlüsseln.
- Darüber hinaus sollten im öffentlichen und im privaten Bereich verstärkt Verschlüsselungstechnologien eingesetzt und in die jeweiligen Produkte und Dienstleistungen eingebunden werden. Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten sollten zu einer integrierten Standortoption werden.
- Die Ausgaben der öffentlichen Hand für IT-Sicherheit sollten erhöht werden. Die im Koalitionsvertrag getroffene Vereinbarung, Bundesbehörden zu verpflichten, 10 Prozent ihres IT-Budgets für die IT-Sicherheit zu verwenden, sollte für Landesbehörden und andere öffentliche Stellen übernommen werden.

9. Beratungen:

Die digitale Beratung staatlicher Einrichtungen, Unternehmen, Universitäten, Forschungseinrichtungen, Verbände und Kammern über Informationssicherheitserfordernisse sollte durch eine Stärkung des Landesbetriebs Daten und Information und durch den Aufbau eines Beratungsnetzwerks unter Einschluss des LfDI intensiviert werden.

10. Internetkompetenz:
Die Maßnahmen zur Förderung der Medien-, insbesondere der Internetkompetenz, die gerade in Rheinland-Pfalz für alle Altersgruppen angeboten und in den Schulen auch mit Hilfe externer Fachleute durchgeführt werden (vgl. Tz. II-2.7), müssen als Folge des NSA-Skandals vor allem die Fähigkeit der Bürgerinnen und Bürger verbessern, sich sicher im Netz bewegen zu können. Das schließt vor allem die Fähigkeit ein, die eigenen Spuren im Netz beseitigen und die eigenen Daten und E-Mails verschlüsseln zu können. Die Verschlüsselung der eigenen Internetaktivitäten muss zu einer digitalen Selbstverständlichkeit, zum sozialen Standard werden. Dies bietet auch gegenüber den Entschlüsselungsstrategien der NSA einen gewissen Schutz und wäre im Übrigen Ausdruck digitaler Souveränität.

11. Kooperationen:
Der NSA-Skandal hat deutlich gemacht, dass zivilgesellschaftliche Einrichtungen, Internetaktivisten und staatliche Stellen enger zusammenarbeiten sollten. Nach dem Vorbild des Landesrates für digitale Entwicklung und Kultur (vgl. http://www.landesrat-rlp.de/) sollten entsprechende Foren auch auf europäischer und nationaler Ebene eingerichtet werden. Im Übrigen ist der Austausch zwischen digitalen Entwicklern und staatlichen Stellen zu fördern.

12. Gesellschaftlicher Diskurs:
Die Diskussion über die Kontrolle des Internets, die Rolle, welche die Geheimdienste, die großen Internetunternehmen und die Provider dabei spielen, und welche Abwehrstrategien ggf. erfolgreich sein könnten, leidet darunter, dass sie bisher im Wesentlichen nur in politischen Gremien, innerhalb der Netzgemeinde und in den Feuilletons überregionaler Zeitungen und Zeitschriften geführt wird; eine gesamtgesellschaftliche Diskussion findet dagegen derzeit nicht statt.

Das hat eine Reihe von Gründen; vor allem hängt es damit zusammen, dass es bisher an diskussionsfähigen Strategien und Konzepten mangelt. Selbst in den diversen Berichten der Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages finden sich zur Freiheit im Netz und zur Sicherung digitaler Grundrechte kaum Thesen und Orientierungsvorschläge, die eine gesamtgesellschaftliche Diskussion befördern könnten.

Der LfDI empfiehlt daher zur Förderung der digitalen Achtsamkeit und Sensibilität einschlägige Kampagnen durchzuführen bzw. zu fördern und Veranstaltungen wie den am 11. Februar 2014 durchgeführten Aktionstag gegen die NSA-Überwachung zu unterstützen.

2.3 Ein Datenschutzpreis für Edward Snowden?

In der immer noch anhaltenden Diskussion über die globalen Überwachungsmaßnahmen insbesondere des US-amerikanischen und des britischen Geheimdienstes wurden und wird von vielen Persönlichkeiten aus Politik, Wirtschaft und Zivilgesellschaft betont, dass dem US-amerikanischen Whistleblower Edward Snowden Respekt entgegen zu bringen sei. Auch Bundespräsident Joachim Gauck hat sich in diesem Sinne geäußert. Die Angst, Telefonate oder Mails würden von ausländischen Geheimdiensten erfasst oder gespeichert, schränke – so stellte er in einem Interview fest – das Freiheitsgefühl der Menschen ein, wodurch die Gefahr bestehe, dass die Freiheit an sich beschädigt werde. Diese Einschätzung trifft sicherlich zu. Aus der Sicht des Datenschutzes kommt noch hinzu, dass die Enthüllungen Edward Snowdens in den USA, in Europa und vor allem auch in unserem Land zu einer intensiven Diskussion über Fragen des Datenschutzes und der Datensicherheit geführt haben, die sich nicht nur auf die künftige digitale Rechtsordnung erstreckt, sondern auch die Kommunikationsinfrastrukturen, insbesondere im Internet betrifft. Unter diesen Gesichtspunkten haben sich auch der Landtag und die Landesregierung mit den Enthüllungen Edward Snowdens befasst.

Vor diesem Hintergrund hatte der LfDI angeregt, für die Verleihung des vom LfDI und dem Bildungsministerium getragenen Datenschutzpreises eine Nominierung Edward Snowdens ins Auge zu fassen und dafür die Ausschreibungs-

richtlinien zu modifizieren, da sie bisher nur wissenschaftliche Arbeiten für eine Preisverleihung zulassen.

Dieser Vorschlag ist in dem für die Preisvergabe eingerichteten Beirat allerdings auf ein geteiltes Echo gestoßen. Zwar wurde der Mut Edward Snowdens, seine Zivilcourage und die Bedeutung seiner Enthüllungen anerkannt, eine ausdrückliche Würdigung seiner Person durch eine öffentliche Stelle angesichts der Tatsache, dass die Enthüllungen in weiten Teilen offenbar auf strafbaren Handlungen beruhten, jedoch als problematisch angesehen. Problematisiert wurden im Übrigen auch die möglicherweise nachteiligen Auswirkungen einer Preisverleihung auf die Außenbeziehungen unseres Landes zu den USA.

Vor diesem Hintergrund hat der Beirat zum Bedauern des LfDI von einer Auszeichnung Edward Snowdens abgeraten. Allerdings hat er vorgeschlagen, anlässlich der Verleihung des Datenschutzpreises eine gesonderte Erklärung zu verabschieden. Darin soll die Bedeutung gewürdigt werden, welche die immer noch nicht zum Abschluss gekommenen Enthüllungen für den Datenschutz und seine freiheitliche Staats- und Gesellschaftsordnung haben. Eine solche Erklärung wird bis Mitte 2014 vorliegen.

2.4 Trotz alledem! – Verschlüsselung als sozialer Standard

„Die Waffen, die der Sieg uns gab, der Sieg des Rechts trotz alledem, die nimmt man sacht uns wieder ab“, heißt es in einem Gedicht von Ferdinand Freiligrath. An diese resignative Erkenntnis nach der gescheiterten Märzrevolution von 1848 fühlt man sich in diesen Zeiten erinnert. Die immer neuen Enthüllungen zur Überwachung der Internetkommunikation durch Geheimdienste lassen glauben, dass das Recht auf freie und unbeobachtete Kommunikation mit atemberaubender Geschwindigkeit erodiert. Nach der weitreichenden Sammlung und Auswertung von Verbindungs- und Metadaten scheinen mit dem Eindringen der NSA in verschlüsselte Kommunikation auch bislang sicher geglaubte Kommunikationsinhalte den digitalen Augen und Ohren der Nachrichtendienste preisgegeben zu sein.

Dies darf jedoch nicht dazu führen, dass die Bemühungen um den Schutz der Privatheit aufgegeben werden. Zwar beherrscht die NSA offenbar bestimmte Formen der Verschlüsselung, aber eben nicht alle. Auch die Fähigkeiten der NSA zur Entschlüsselung haben nach Aussage Edward Snowdens Grenzen. Der Einsatz starker Verschlüsselungslösungen ist danach eines der wenigen Dinge, auf die man noch vertrauen könne.

Außerdem ist die Privatsphäre im Internet nicht nur durch die NSA bedroht. Auch wenn der kommunikative Allmachtsanspruch der NSA ein Problem ist, so ist es doch nicht das Einzige. Viele Stellen im Internet verfolgen, was wir dort tun, Provider, Administratoren, Netzbetreiber usw. Mit wem wir worüber kommunizieren, was wir in der Cloud speichern oder wohin wir surfen, interessiert all diejenigen, die auf der Auswertung unserer Daten ihre Geschäftsmodelle aufbauen. Wenn wir dieser industriellen Ausbeutung unserer Daten begegnen wollen, bleibt die Nutzung von Verschlüsselungstechnologien das Gebot der Stunde. Verschlüsselung sollte Normalität werden, um sie vom Makel des verdächtigen Verhaltens zu befreien. Oder, wie es Phil Zimmerman, der Erfinder der freien Verschlüsselungslösung PGP vor kurzem in einem Interview gesagt hat: „Verschlüsselung ist Bürgerpflicht.“

Crypto-Sessions / Selbstdatenschutz

Im Rahmen von Crypto-Sessions informiert der LfDI darüber, wie man sich mit Verschlüsselung gegen unerwünschtes Lauschen und Datensammeln zur Wehr setzen kann und wie sich Datenspuren im Internet vermeiden lassen.

http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2013090901

Weitere Informationen zum Selbstdatenschutz im Internet bietet der LfDI in seinem Internetangebot in der Rubrik „Selbstdatenschutz“ (http://www.datenschutz.rlp.de/de/selbstds.php).

2.5 Mehr Sicherheit für Unternehmensdaten

Der LfDI hat die Meldungen über mögliche Wirtschafts- und Industriespionage durch US-amerikanische und britische Geheimdienste und das angebliche Eindringen in verschlüsselte Kommunikationsverbindungen (VPNs) durch deren Überwachungsprogramme zum Anlass genommen, die rheinland-pfälzischen Unternehmen zu größeren Anstrengungen bei ihrer IT-Sicherheit aufzurufen. Jüngste Untersuchungen bestätigten, dass immer noch rund 80 Prozent der mittelständischen Wirtschaftsunternehmen keine Verschlüsselungstechnologie nutzen, weil das eigene Unternehmen nicht als gefährdet angesehen werde. Angesichts eines Gesamtschadens von bis zu 60 Milliarden Euro, der der deutschen Wirtschaft durch Wirtschaftsspionage pro Jahr entsteht, ist eine solche Einstellung blauäugig.

Die Meldungen zum NSA-Überwachungsprogramm „Bullrun“ geben darüber hinaus Anlass, an der Sicherheit, Verlässlichkeit und Vertrauenswürdigkeit von Verschlüsselungslösungen zu zweifeln, die unter maßgeblicher Beteiligung US-amerikanischer Stellen entwickelt wurden. Die Forderung des Bundesverbands IT-Mittelstand e.V., Sicherheitstechnologie „made in Germany“ in Anspruch zu nehmen, ist deshalb richtig und wird von den Datenschützern auch unterstützt.

Dies gilt auch für die Forderung nach einem entsprechenden staatlichen Förderprogramm. Es muss sichergestellt werden, dass Deutschland nicht nur beim Datenschutz, sondern auch bei der Datensicherheit und der IT-Sicherheitstechnologie führend ist.

Notwendig sind dabei auch größere Anstrengungen der Kammern und der zuständigen staatlichen Stellen. Sie müssen Sicherheitskompetenznetzwerke auch in den Ländern aufbauen, in denen neben den Unternehmen, den Wirtschaftsverbänden und den Kammern auch die zuständigen staatlichen Stellen einschließlich der Datenschützer vertreten sein sollten. Diese Netzwerke sollten die Unternehmen mit notwendigen Informationen versorgen und Hilfestellungen bei aktuellen Spionage- oder Hacker-Angriffen zur Verfügung stellen.

Der LfDI begrüßt insoweit das vom Bundeswirtschaftsministerium veröffentlichte Zehn-Punkte-Programm mit seinen Handlungsempfehlungen für einen sicheren Umgang mit Unternehmensdaten im Internet (http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Redaktion/PDF/10-punkte-fuer-einen-sicheren-umgang-mit-unternehmensdaten-im-internet,property=pdf,bereich=itsicherheit,sprache=de,rwb=true.pdf). Nicht zuletzt die Anregung, auf Cloud-Anbieter zurückzugreifen, welche die Unternehmensdaten nach europäischen Datenschutzgrundsätzen verarbeiten, wird nachdrücklich unterstützt.

2.6 Digitale Vorsorge. Selbstdatenschutz im Internet

Die Enthüllungen um die Spähprogramme PRISM und TEMPORA haben vor Augen geführt, wie weit die Überwachung des Internets reicht und wie intensiv die Spuren, die wir dort hinterlassen, ausgewertet werden. Das Internet von heute bietet eine Vielzahl von Diensten, und jeder Klick, jeder Chat, jedes Foto, jede Suche, jeder Post und jede Nachricht hinterlassen eine Datenspur. Diese sind jedoch nicht nur für Nachrichtendienste von Interesse.

Der Datenschatten, den wir im Internet werfen, weckt viele Begehrlichkeiten. Die Daten werden für Zwecke der Kundenbindung, der Online-Werbung oder der Marktforschung erfasst und ausgewertet und zu individuellen Nutzungs-, Kauf- oder Bewegungsprofilen verdichtet. Je mehr das Internet im Alltag genutzt wird, desto mehr Datenspuren liefern Hinweise auf Interessen, Vorlieben und Verhaltensweisen der Nutzerinnen und Nutzer. Es ist das legitime Recht aller Nutzerinnen und Nutzer, den digitalen Augen und Ohren im Internet nicht alles preiszugeben. Wer nicht will, dass seine Daten im Internet Neugier und Sammelwut preisgegeben sind, sollte Vorsorge treffen.

Der LfDI hat daher sein Internetangebot um eine Rubrik „Selbstdatenschutz“ erweitert, die zeigt,

wie die Nutzerinnen und Nutzer selbst digitale Vorsorge im Internet treffen können. Hier wird gezeigt, welche Möglichkeiten bestehen, Datenspuren im Internet zu vermeiden, wie E-Mailinhalte durch Verschlüsselung geschützt werden können, mit welchen Maßnahmen man Inhalte in Online-Speichern vertraulich halten kann oder wie sich die penetrante Dateninkontinenz von Smartphones unterbinden lässt.

Internet-Angebot des LfDI zum Selbstdatenschutz:

- Datenspuren vermeiden
  http://www.datenschutz.rlp.de/de/selbstds.php?submenu=datenspuren
- E-Mailinhalte schützen
  http://www.datenschutz.rlp.de/de/selbstds.php?submenu=email
- Dropbox & Co sicher nutzen
  http://www.datenschutz.rlp.de/de/selbstds.php?submenu=cloud
- Smartphones & Tablets
  http://www.datenschutz.rlp.de/de/selbstds.php?submenu=mobile
- Selbsttests
  http://www.datenschutz.rlp.de/de/selbstds.php?submenu=selbsttest

2.7 Systemverwaltung und Datenschutz

Die Konzeption gegenwärtiger Betriebssysteme und IT-Verfahren sieht zumeist die Rolle eines „Administrators“ vor, die mit umfangreichen Zugriffsrechten ausgestattet ist. Der mögliche und aufgrund der Reichweite der Berechtigungen u.U. nicht erkennbare Missbrauch von Zugriffsrechten wird seit langem als grundsätzliches datenschutzrechtliches Problem gesehen. Dass den mit Systemverwalterfunktionen betrauten Personen damit eine besondere Vertrauenswürdigkeit abverlangt wird, hat auch Eingang in die Rechtsprechung der Arbeitsgerichte gefunden, wonach ein Missbrauch eine außerordentliche Kündigung rechtfertigt.

In technisch-organisatorischer Hinsicht gibt es verschiedene Ansatzpunkte, das Missbrauchsrisiko einzuschränken, z.B.:

- Ein förmlicher Hinweis bzw. eine förmliche Belehrung für die mit Systemverwalterfunktionen betrauten Personen auf das besondere Vertrauensverhältnis, das ihre Funktion bedingt und die arbeitsrechtlichen bzw. dienstlichen Folgen im Fall eines Missbrauchs; Abverlangen einer persönlichen Verpflichtungserklärung, die gesetzten Regeln einzuhalten, Bekanntgabe der Regeln.
- Aufteilung von Systemverwalteraufgaben auf verschiedene Personen:
  Eine Reihe von IT-Verfahren unterstützt die Trennung von Systemverwaltung, Berechtigungsverwaltung und Datenbankverwaltung. Wo dies nicht durch entsprechend getrennte „Rollen“ vorgesehen ist, besteht die Möglichkeit, Authentifizierungsinformationen (z.B. Passwörter) so zu verteilen, dass jede Personen nur eine Hälfte der Information besitzt. Dies ist im Tagesgeschäft umständlich und daher u.U. nicht praktikabel, für sensible Funktionen (z.B. Zugriffe auf Protokolldaten) aber möglich. Soweit Zwei-Faktor-Authentisierungen möglich sind (Passwort und Token, wie z.B. Chipkarte, Dongle oder USB-Speicher), können Wissen und Besitz ebenfalls auf zwei Personen aufgeteilt werden.
- Verschlüsselung von Nutzdaten, Dokumenten etc.:
  Nicht alle Systemverwalterfunktionen erfordern den Zugriff auf Nutzdaten, wie etwa bei der systemnahen oder technischen Betreuung der eingesetzten Systeme. Lösungen, bei denen sensible Informationen verschlüsselt werden, erlauben es, eine inhaltliche Kenntnisnahme der auf dem System gespeicherten Daten zu vermeiden. Hier stehen Lösungen zur Verfügung, die weitgehend automatisiert eine Verschlüsselung erlauben.
- Protokollierung und Verschlüsselung von Protokolldaten:
  Dort, wo Berechtigungen nicht auf mehrere Personen aufgeteilt und Missbräuche u.U. nicht verhindert werden können, kann durch eine angemessene Protokollierung jedoch eine Kontrolle bzw. Aufklärung erfolgen. Um zu vermeiden, dass die Protokolldaten manipuliert werden, sollten diese verschlüsselt werden und das Passwort dem Administrator nicht zugänglich sein. Zwar sind auch hier Wege

möglich, dies zu umgehen, die Vorgehensweise erschwert dies jedoch.

In der Praxis sind damit in vielen Fällen Näherungslösungen denkbar, eine alle Missbräuche ausschließende Situation lässt sich jedoch nur in Ausnahmefällen und meist mit hohem Aufwand verbunden herstellen. Regelmäßig umsetzbar ist jedoch die eingangs genannte ausdrückliche Belehrung und Verpflichtung.

2.8 Infrastrukturelle IT-Maßnahmen

Gegenwärtig werden in zwei Tagen so viele Daten erzeugt wie zuvor vom Beginn der menschlichen Zivilisation bis zum Jahr 2003. Im Telekommunikationsbereich liegt z.B. das Datenaufkommen allein in den Netzen der Deutschen Telekom bei ca. 400.000 Terabyte im Monat. Um solche Datenbestände überhaupt handhaben zu können, entstehen unter dem Begriff „Big Data“ zur Zeit neue Ordnungs-, Sortier- und Auswertungsmöglichkeiten. Diese sind die Grundlage für spezielle Vorhersagemodelle. Nutzungs- und Standortdaten werden zu Kommunikations-, Konsum-, Verhaltens- und Bewegungsprofilen verdichtet, Aggregation und Kontextinformationen erlauben bereits heute erstaunlich verlässliche Voraussagen, wo sich eine Person zu einem bestimmten Zeitpunkt aufhalten und was sie dann tun wird. Wie hoch der Preis für solche Erkenntnisse sein wird, wissen wir nicht. Aber die Erfahrung lehrt, dass wir dafür werden zahlen müssen – mit individuellen Missbräuchen und gesellschaftlichen Risiken.

Infrastrukturelle Maßnahmen und nutzerorientierte Mechanismen

Dies macht zumindest eines deutlich: der bisherige Ansatz, Datenschutzmechanismen allein verfahrensbezogen zu betrachten – ein zentraler Gedanke der gegenwärtigen Datenschutzgesetze – hat sich überlebt. Die in den meisten Datenschutzgesetzen enthaltenen Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes stammen im Kern aus den 1970er Jahren des letzten Jahrhunderts und lassen sich immer weniger auf die heutige Welt vernetzter und ubiquitärer Systeme übertragen. Sie fußen auf homogenen, zentralen, einheitlich organisierten und von einer Stelle betriebenen IT-Strukturen, wie sie heute vielfach nicht mehr anzutreffen sind. Heutige IT-Lösungen sind oftmals durch ausgeprägt dezentrale Strukturen, einen hohen Vernetzungsgrad, verteilte Anwendungen und Verantwortlichkeiten und unterschiedliche Betreiber gekennzeichnet (Internetportale, Online-Shops, RFID-Anwendungen, ortsbezogene Dienste, etc.). Mit den vorhandenen technisch-organisatorischen Regelungen kann dem nur unzureichend entsprochen werden.

Diese defizitäre Situation ist kein neuer Gedanke; bereits 2001 wurden in einem Gutachten für das Bundesinnenministerium die unzureichenden Technikregelungen der Datenschutzgesetze problematisiert und im März 2010 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder dies in ihren Eckpunkten für ein Datenschutzrecht für das 21. Jahrhundert aufgegriffen und vorgeschlagen, künftigen Datenverarbeitungen infrastrukturelle Datenschutzziele zugrunde zu legen:

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Transparenz
- Nichtverkettbarkeit als technische Sicherung der Zweckbindung
- Intervenierbarkeit als Ansatzpunkt für die Ausübung von Betroffenenrechten.

Das vom Bundesverfassungsgericht 2008 formulierte Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme weist in die gleiche Richtung (Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, Az. 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274). Wenngleich es sich bei Vertraulichkeit und Integrität um verfassungsrechtlich zu interpretierende und nicht primär technische Begriffe handelt, sind Hashwerte, Verschlüsselung und Authentizitätsnachweise zu erwartende Aspekte, in denen sich die konkrete Ausformung des IT-Grundrechts niederschlagen wird, arrondiert durch verfahrensmäßige Instrumente wie Auditierung, Zertifizierung,

Kennzeichnungspflichten, Prüf- und Revisionsmöglichkeiten.

Der bisherige Ansatz ist u.a. auch deshalb unzureichend, weil seine Anforderungen allesamt auf den jeweiligen Datenverarbeiter, d.h. den Betreiber einer IT-Infrastruktur zielen. Keiner der tradierten Mechanismen ist dazu vorgesehen, von Betroffenen eingesetzt zu werden, um Art, Umfang, Reichweite und ggf. Dauer der Verarbeitung ihrer Daten zu steuern. Neben infrastrukturellen Datenschutzkonzepten bedarf es daher Mechanismen, die den Nutzerinnen und Nutzern entsprechende Möglichkeiten an die Hand geben. Hierzu zählen neben kryptografischen Funktionen Mechanismen für eine anonyme oder pseudonyme Nutzung, bei der die Identifikationsdaten – soweit möglich – unter der Kontrolle der Nutzerinnen und Nutzer bleiben sowie effektive Möglichkeiten, einen Widerspruch gegen bestimmte Datenverarbeitungen auszuüben.

Interessanterweise bleibt auch die für eine einheitliche Regelung des Datenschutzes in Europa vorgesehene Datenschutz-Grundverordnung der Europäischen Kommission in dieser Hinsicht merkwürdig blass. Trotz verschiedener Ansätze enthält sie mit Bezug auf die Gegebenheiten im Internet nahezu keine Regelungen zum technischen Datenschutz.

Zwei Vorschläge stellen einen gewissen Fortschritt dar. Der Entwurf der europäischen Datenschutz-Grundverordnung formuliert in Art. 17 das Recht auf Vergessen und in Art. 18 das Recht auf Übertragbarkeit bzw. Portierung personenbezogener Daten. Unter dem Begriff „digitaler Radiergummi“ haben die ersten Realisierungen dieser Idee des Vergessens im Internet zwar eine gewisse Häme erfahren, dies ändert jedoch nichts an der konzeptionellen Stimmigkeit des Ansatzes. Die Idee teilt derzeit in gewisser Weise das Schicksal der in § 3a BDSG genannten Grundsätze der Datensparsamkeit und Datenvermeidung. Konzeptionell stimmig fristen sie in der Praxis jedoch ein eher stiefmütterliches Dasein.

Not täte, statt halbherziger und teilweise eher drollig wirkender Bemühungen die Entwicklung technischer Umsetzungen solcher Konzepte wirksam zu fördern. Die Schwächen vorhandener Ansätze oder bestehende Möglichkeiten der Umgehung führen nicht die Idee an sich ad absurdum. Auf der Grundlage standardisierter Datenformate und vertrauenswürdiger Infrastrukturdienste sind Lösungen möglich, die vielleicht nicht in jedem Fall ein Vergessen gewährleisten, jedoch ein Erinnern erschweren.

2.9 Situation in der Landesverwaltung

Ausgehend von den Enthüllungen Edward Snowdens und dem Ausspähen der Kommunikation der Bundeskanzlerin durch den US-amerikanischen Nachrichtendienst NSA hat sich die Frage gestellt, wie es um die Sicherheit und Vertrauenswürdigkeit der Kommunikation der rheinland-pfälzischen Verwaltungen bestellt ist, was die Enthüllungen für die Landes- und Kommunalverwaltung bedeuten und ob und welche Konsequenzen gezogen werden müssen.

Gegenwärtig besteht in diesem Zusammenhang folgende Situation:

Die Landesverwaltung nutzt das rlp-Netz für die Datenkommunikation. Dieses wird vom Landesbetrieb Daten und Information (LDI) betrieben, die genutzten Leitungsstrecken werden von der Deutschen Telekom als Provider zur Verfügung gestellt. Alle Knoten des Netzes, d.h. alle Vermittlungseinrichtungen (Router) befinden sich zugangsgeschützt in Liegenschaften der Polizei. Diese Netzknoten werden ausschließlich vom LDI administriert und überwacht, Zugriffsmöglichkeiten für den Provider bestehen nicht. Die Kommunikation auf den von der Telekom angemieteten Leitungen wird verschlüsselt und die Schlüsselhoheit – d.h. die Entscheidung über die kryptografischen Algorithmen, die Erzeugung der kryptografischen Schlüssel, das Einbringen in die Netzknoten usw. – liegt beim LDI. Diese Konzeption wurde vor einigen Jahren vom LDI in Zusammenarbeit mit dem LfDI erarbeitet und hat in der nunmehr durch Edward Snowden offengelegten Situation ihre Bestätigung erfahren.

Der Betrieb des rlp-Netzes – d.h. die eingesetzte Technik sowie die Organisation und betrieblichen

Abläufe – wurden vom Bundesamt für Sicherheit in der Informationstechnik sicherheitszertifiziert. Über ein solches Zertifikat verfügt bundesweit lediglich eine weitere Datenzentrale; Rheinland-Pfalz war dabei das erste Land, das eine solche Zertifizierung in die Wege geleitet hat.

Die Kommunalverwaltungen nutzen das Kommunale Netz Rheinland-Pfalz (KNRP). Dessen Betrieb liegt in Händen einer Tochtergesellschaft der Kommunalen Spitzenverbände; Provider ist hier die British Telecom. Auch im Kommunalnetz wird die Kommunikation verschlüsselt, im Unterschied zum rlp-Netz liegt die Administration der Netzknoten jedoch beim Provider. Auf Empfehlung des LfDI wurden zunächst Teile der Administration zurückgeholt, um gegenüber dem Provider sicherheitsmäßig unabhängiger zu werden. Insgesamt besteht im Kommunalnetz bislang jedoch keine dem rlp-Netz vergleichbare Situation. Auch ist der Betrieb des KNRP gegenwärtig nicht sicherheitszertifiziert.

Da es sich bei der British Telecom um einen britischen Provider handelt, hat sich im Zusammenhang mit der Diskussion um Zugriffsmöglichkeiten ausländischer Geheimdienste die Frage gestellt, ob dieser ggf. Datenanforderungen britischer staatlicher Stellen unterliegt. Trotz konkreter Fragestellungen eröffnen die Antworten hierzu Interpretationsspielräume.

Im Bereich der Telefonie (Mobil und Festnetz) greift das Land überwiegend auf Vodafone als Provider zurück. Hier ergeben sich ähnliche Fragen wie bei der British Telecom. Die Sprachkommunikation der Landesverwaltung (Mobilfunk- und Festnetz) ist ungeschützt gegenüber einer etwaigen Weitergabe von Verbindungs- oder Inhaltsdaten an ausländische Stellen durch den Provider (Vodafone). Die Vertragsregelungen schließen dies zwar aus, deren Einhaltung ist faktisch jedoch nicht zu kontrollieren, und technisch besteht die Möglichkeit, Metainformationen und Inhaltsdaten abzuziehen. Auch hier wurden entsprechende Fragen an den Provider gerichtet; die Antworten entbehren auch in diesem Fall der gewünschten Eindeutigkeit. Hier sollte die Landesregierung angesichts der bekanntgewordenen Zusammenarbeit des GCHQ mit Vodafone prüfen, welche Risiken sich daraus ergeben und ob zumindest partiell auch hier Verschlüsselungslösungen eingesetzt werden können und sollen. Für die Festnetztelefonie der Landesverwaltung bestünde die Möglichkeit, diese als Voice over IP-Telefonie über das rlp-Netz abzubilden; die notwendige technische Struktur ist jedoch nicht bei allen Verwaltungen vorhanden. Ein Umstieg kann aus wirtschaftlichen Gründen allenfalls mittelfristig erfolgen; dieser sollte vor dem aktuellen Hintergrund aus Sicht des LfDI jedoch ins Auge gefasst werden, um auch die Sprachkommunikation der Verwaltungen im Festnetz über verlässlich vertrauenswürdige Infrastrukturen zu führen.

Der LfDI hat jedoch keine Anhaltspunkte dafür, dass ausländische Stellen in der Vergangenheit Daten über die Provider erhalten haben. Es gibt allerdings auch keine klaren Aussagen dazu, ob dies der Fall war oder sein könnte. Dort, wo die Infrastruktur keine ausreichende Sicherheit bietet und die Art der Daten es verlangt, muss die notwendige Vertraulichkeit oberhalb der Netzebene, d.h. in den genutzten Anwendungen sichergestellt werden, z.B. durch eine Verschlüsselung von E-Mails, oder der Verschlüsselung beim Zugriff auf zentrale Verfahren. In einigen Fällen erfolgt dies bereits, bei der E-Mailkommunikation gibt es jedoch, das zeigen die Erkenntnisse des LfDI, Handlungsbedarf.

Gegen Angriffe auf die IT-Strukturen der Verwaltungen helfen Firewalls und Detektionssysteme sowie ein Sicherheits- und Datenschutzmanagement, das festlegt, wie Vorfälle vermieden bzw. damit umgegangen werden soll (Sicherheitsleitlinien). Dies ist z.B. im rlp-Netz der Fall. Im kommunalen Bereich ist die Situation jedoch sehr unterschiedlich. Ein Teil der Kommunen verfügt über entsprechende Lösungen und Ressourcen, andere Kommunen, meist kleinere, bleiben hinter solchen Lösungen zurück.

Letztlich kommt es darauf an bewusst zu machen, dass die zunehmende Vernetzung der IT-Strukturen tatsächliche Risiken birgt. Die Enthüllungen Edward Snowdens und die offengelegten Überwachungsaktivitäten der NSA haben deutlich gemacht, dass diese nicht theoretischer Natur sind.

3. Entwicklung des Datenschutzrechts

3.1 Die Bedeutung des Rechts im digitalen Zeitalter

Der LfDI hat nicht nur gemäß § 24 Abs. 1 LDSG die Einhaltung der Datenschutzgesetze zu kontrollieren, er hat auch zu beobachten, ob diese Gesetze ihren Zweck erfüllen, um – wenn dies nicht der Fall wäre – Gesetzesänderungen oder neue Gesetze anregen und empfehlen zu können. Dies gilt aber nicht nur für die Landesgesetze, die sich mit dem Datenschutz beschäftigen, sondern auch für Bundesgesetze und europarechtliche Regelungen, da auch sie für rheinland-pfälzische Bürgerinnen und Bürger gelten. Allerdings geschieht die Auseinandersetzung mit Bundes- und europarechtlichen Regelungen – schon aus Kapazitätsgründen – nicht mit derselben Intensität wie bei Landesgesetzen. Kompensiert wird dies durch eine enge Kooperation mit den Datenschutzbeauftragten des Bundes und der anderen Länder in diesen Fragen.

Diese Aufgabe ist gerade derzeit von besonderer Bedeutung. Denn die digitale Umgestaltung unserer Gesellschaft geht auch an unserer Rechtsordnung nicht spurlos vorbei, wobei allerdings auf allen Ebenen große Unsicherheit darüber besteht, in welchem Umfange und mit welchen Inhalten eine Neuorientierung unserer Datenschutzrechtsordnung notwendig ist.

Das kommt etwa darin zum Ausdruck, dass Bundesminister Dr. Thomas de Mazière in seiner ersten Amtszeit als Bundesinnenminister einen Gesetzentwurf ausgearbeitet hatte, mit dem nicht überschreitbare „rote Linien“ für das Internet gezogen werden sollten, wovon er zu Beginn seiner zweiten Amtszeit in dieser Funktion aber schon nichts mehr wissen will. Das zeigt sich an dem Versuch, den Anbietern von sozialen Netzwerken das Privileg einer Selbstregulierungsermächtigung einzuräumen, wovon diese dann aber gar keinen Gebrauch machen. Das zeigt sich auch darin, dass die Europäische Kommission den Entwurf einer Datenschutz-Grundverordnung vorlegt hat, dann aber feststellen muss, dass in den Mitgliedstaaten ganz unterschiedliche Datenschutzkulturen herrschen, sodass den Mitgliedstaaten ein gemeinsames Vorgehen in Datenschutzangelegenheiten regelmäßig schwerfällt.

Aber die Auseinerandersetzungen um adäquate Datenschutzregelungen sind noch viel grundsätzlicher und prinzipieller als diese Beispiele vermuten lassen. Denn während die einen eine Art „digitalen Code civil“ verlangen, wehren sich die anderen, um – wie sie sagen – die Freiheit im Netz zu sichern, gegen jeden staatlichen Eingriff, auch wenn er in Form von Gesetzen daherkommt. Vor diesem Hintergrund sind die gegenwärtigen Gesetzgebungsaktivitäten auf internationaler und europäischer, auf Bundes- und Landesebene zu beurteilen.

Angesichts der globalen Dimension der digitalen Technologie geht es dabei allerdings zunächst um die Frage, ob auch globale Regelungen, mindestens bilaterale Abkommen zwischen der EU und den USA oder jedenfalls europäische Normen vorhanden sind oder auf den Weg gebracht werden können.

3.2 Internationales Recht und Europarecht

3.2.1 Abkommen mit den USA

Das Datenschutzverständnis in den Vereinigten Staaten von Amerika unterscheidet sich von dem in Europa, speziell von dem Datenschutzverständnis in Deutschland erheblich. Dies ist auch auf unterschiedliche geschichtliche Erfahrungen zurückzuführen. Umso mehr ist es zu begrüßen, dass auch in den USA gegenwärtig eine Diskussion zur Stärkung des Datenschutzes geführt wird.

Im Februar 2012 veröffentlichte beispielsweise das Weiße Haus ein Papier mit dem Titel „Consumer Privacy Bill of Rights“, also eine Leitlinie für den Datenschutz in der Informationsgesellschaft, die Ansprüche der Verbraucherinnen und Verbraucher gegenüber Unternehmen begründen soll (http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights).

In Folge der NSA-Affäre hat US-Präsident Barack Obama verschiedene Arbeitsgruppen eingesetzt, die

die Geheimdienste unter unterschiedlichen Aspekten untersuchen sollen. Eine von diesen Arbeitsgruppen (unter James Poterba) hat im April 2014 sehr unterstützenswerte Empfehlungen veröffentlicht, die den Schutz aller Internetnutzerinnen und -nutzer verbessern sollen, nicht nur den von US-amerikanischen Staatsbürgern, (FAZ vom 3. Mai 2014, „Amerikas Regierung will Daten von Internetnutzern schützen“).

Dies zeigt, dass eine Diskussion im Gange ist, die Anlass zu vorsichtigem Optimismus geben könnte.

Rahmenabkommen mit den USA zum Datenschutz im Strafverfolgungsbereich

Das seit 2011 zwischen der Europäischen Union und den USA diskutierte Datenschutzabkommen im Strafverfolgungsbereich ist allerdings noch kein Beispiel für sich ändernde Datenschutzkultur in den Vereinigten Staaten. Durch dieses Abkommen sollen Datenübermittlungen zwischen der EU und den USA in Bezug auf Bürgerdaten erleichtert werden, die für die Terrorismus- und Straftatenbekämpfung nützlich sein können. Die Datenübermittlungen sollen durch Datenschutzregelungen flankiert werden. Das Abkommen ist bis jetzt noch nicht zum Abschluss gekommen, weil die Vereinigten Staaten wesentliche Forderungen der Europäischen Union – etwa nach Klagemöglichkeiten von EU-Bürgerinnen und -Bürgern gegen US-amerikanische Handlungen im Zusammenhang mit diesem Abkommen – nicht erfüllen wollen (http://www.heise.de/newsticker/meldung/EU-sieht-offene-Fragen-beim-Datenschutz-Abkommen-mit-den-USA-2170545.html; https://netzpolitik.org/2014/internes-dokument-der-eu-kommission-usa-wollen-transatlantisches-datenschutz-abkommen-verwaessern/).

Wenn kein adäquater Datenschutzstandard erreicht werden kann, wäre es aus Datenschutzsicht in der Tat besser, dieses Abkommen erst gar nicht abzuschließen. Es darf nicht sein, dass nur eine Grundlage für neue und umfangreichere Datenströme in die USA geschaffen wird, ein wirksamer Schutz gegen unberechtigte Speicherung und Nutzung von Daten durch die Vereinigten Staaten aber unterbleibt (vgl. Patrick Breyer, http://www.zeit.de/2014/19/datenschutzabkommen-ueberwachung-nsa).

Swift-Abkommen

In seinen letzten Tätigkeitsberichten (vgl. 23. Tb., Tz. I-2.1.3; 22. Tb., Tz. 2.1.1; 21. Tb., Tz. 2.7 und 22.3) hat der LfDI die datenschutzrechtlichen Bedenken wegen der im **SWIFT-Abkommen** vorgesehenen Datenübermittlungen über Banktransaktionen an die USA dargestellt. Ziel dieser Datenübermittlungen ist die Terrorbekämpfung. Die Übermittlungen sind Teil des „Terrorist Finance Tracking Systems“ (TFTS). Bei Kontrollen der Datenübermittlungen wurde durch die Gemeinsame Kontrollinstanz (GKI) Europol im Jahr 2011 festgestellt, dass zu einigen Abfragen nicht geprüft werden könne, ob sie verhältnismäßig seien, da die Begründungen für die Anfragen fehlten oder unzureichend seien. Da die Berichte der GKI jedoch als geheim eingestuft wurden, dürfen sie auch nicht veröffentlicht werden und lassen sich somit auch nicht überprüften, nicht einmal durch das Europäische Parlament.

Durch die EU-Kommissarin Cecilia Malmström wurden Eckpunkte für ein neues Verfahren veröffentlicht, das in Europa anstatt des bisherigen TFTS der USA eingerichtet werden soll. Der Bundesrat hat mit Beschluss vom 23. September 2011 ebenfalls ein neues System befürwortet (BR-Drs. 415/11). Dabei betonte er, dass das Ziel eines solchen neu zu entwickelnden EU-Systems sein müsse, ohne eine massenhafte Übermittlung von Zahlungsverkehrsdaten auszukommen.

Seitdem sind allerdings keine weiteren Bestrebungen zur Einführung eines neuen Systems zu beobachten. Das Europäische Parlament setzte jedoch im Oktober 2013 ein politisches Signal. Angesichts des NSA-Überwachungsskandals hat es Ende Oktober 2013 die Kommission aufgefordert, das Abkommen vorübergehend auszusetzen. Die Europäische Kommission ist dem nicht gefolgt, da festgestellt worden sei, dass die USA im Zuge der Terrorismusbekämpfung nicht gegen das Abkommen verstoßen hätten Die Aufsichtsbehörden Belgiens und der Niederlande haben allerdings angekündigt, in einer gemeinsamen Aktion bei SWIFT zu prüfen, ob es unberechtigte Zugriffe der USA auf die Banktransaktionsdaten europäischer Bürgerinnen und Bürger gegeben habe.

Flugpassagierdaten-Abkommen

Ein Thema, mit dem sich der LfDI seit Jahren beschäftigt hat, ist die Speicherung und Übermittlung von Flugpassagierdaten (vgl. 23. Tb., Tz. I-2.1.3). Im November 2011 hatte die Europäische Kommission einen erneuten Beschlussentwurf für ein Abkommen der Europäischen Union mit den Vereinigten Staaten von Amerika über die Verwendung von Fluggastdatensätzen vorgelegt. Dadurch sollte für die Datenübermittlung an das United States Department of Homeland Security eine einheitliche Rechtsgrundlage innerhalb der Europäischen Union geschaffen werden. Trotz heftiger Kritik aus Datenschutzkreisen an der sehr langen Datenspeicherung – fünf Jahre in einer aktiven Datenbank und weitere zehn Jahre in einer ruhenden Datenbank – sowie an den begrenzten Rechtsschutzmöglichkeiten (nur nach US-amerikanischem Recht auch für europäische Bürgerinnen und Bürger) ist das Abkommen im Sommer 2012 in Kraft getreten.

So wie das SWIFT-Abkommen, soll auch das Fluggastdaten-Abkommen suspendiert werden. Eine entsprechende Forderung des Europäischen Parlamentes vom Juli 2013, die ebenfalls im Zusammenhang mit den Snowden-Enthüllungen stand, und offenbar auch von der zuständigen EU-Kommissarin unterstützt worden war, wurde allerdings nicht weiter verfolgt.

Dieses Abkommen mit den USA sollte nach Willen der Europäischen Kommission auch Vorbild für weitere Abkommen dieser Art werden. Ein vergleichbares europäisches System zur Sammlung und Auswertung von Flugpassagierdaten konnte aber aufgrund massiver Kritik gestoppt werden. Eine solche Regelung begegnet in der Tat verfassungsrechtlichen Bedenken. So wird durch eine automatisierte Auswertung und Analyse durch Polizei und Strafverfolgungsbehörden sowie durch die geplanten Datenabgleiche die Möglichkeit einer anlasslosen Rasterfahndung eröffnet. Auch die angestrebte verdachtslose Speicherung aller Flugpassagierdaten auf Vorrat verstößt gegen die Rechtsprechung des Bundesverfassungsgerichts.

Safe Harbor

Im Zusammenhang mit dem NSA-Skandal ist auch die Safe-Harbor-Vereinbarung zwischen der Europäischen Union und den USA wieder problematisiert worden (vgl. auch 23. Tb., Tz. I-2.1.3). Auf ihrer Grundlage können Daten europäischer Unternehmen zulässiger Weise in die USA transferiert, z.B. in eine Cloud ausgelagert werden, deren Verarbeitung nicht im Europäischen Wirtschaftsraum, sondern in den USA stattfindet.

Schon in den vergangenen Jahren waren Zweifel an diesem Agreement aufgekommen. Zwar seien mittlerweile weit über 1.000 US-amerikanische Unternehmen dem Abkommen beigetreten und hätten sich damit auch zur Beachtung bestimmter Datenschutzstandards verpflichtet, doch würden sie diese in ihrer Datenverarbeitungspraxis tatsächlich nicht einhalten. Jedenfalls würde ihre Praxis nicht von der zuständigen Federal Trade Commission überprüft.

Bereits im Jahre 2003 hätte die Europäische Kommission das Safe-Harbor-Abkommen evaluieren müssen. Dies ist allerdings nicht geschehen. Nachdem sich u.a. das Europäische Parlament – aber auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder – im Zusammenhang mit dem NSA-Skandal für eine Suspendierung dieses Abkommens ausgesprochen hatte, hat die Kommission endlich eine Überprüfung des Abkommens in Angriff genommen und am 27. November 2013 bekannt gegeben, dass sie beabsichtige, eine Entscheidung über eine vorübergehende Aussetzung, inhaltliche Abänderung oder Aufhebung des Rechtsakts zu Safe Harbor im Sommer 2014 treffen werde. Bis dahin wurden der US-Seite 13 Empfehlungen an die Hand gegeben, mittels derer der auf Safe Harbor gestützte Datentransfer optimiert werden könne.

In einer gemeinsamen Presseerklärung vom 24. Juli 2013 forderten daher die Datenschutzbeauftragten des Bundes und der Länder von der Bundesregierung eine Begrenzung des Zugriffs ausländischer Geheimdienste („Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten“, vgl. http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2013072401) Des

Weiteren sollen Datenübermittlungen an Drittstaaten ausgesetzt werden, bis ein angemessener Datenschutz sichergestellt werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder gehen im Übrigen davon aus, dass gerade auch bei den Verhandlungen zur **transatlantischen Freihandelszone** Regelungen mit aufgenommen werden, die sicherstellen, dass Datenzugriffe öffentlicher Stellen in den USA auf personenbezogene Daten aus dem europäischen Wirtschaftsraum nur erfolgen dürfen, wenn sie verhältnismäßig und erforderlich sind.

3.2.2 Die Europäische Datenschutz-Grundverordnung

Die aus dem Jahr 1995 stammende europäische Datenschutzrichtlinie (RL 95/46 EG) stellte lediglich einen datenschutzrechtlichen Minimalrahmen dar, der den Mitgliedsstaaten genügend Gesetzgebungsspielräume beließ, so dass sich vor allem in Deutschland das Datenschutzrecht weiterentwickeln konnte. Die Rechtsprechung des Europäischen Gerichtshofs, wonach auch diese Richtlinie eine Sperrwirkung gegenüber dem nationalen Gesetzgeber entfaltet, wenn dieser höhere Datenschutzstandards regeln will, ist erst jüngeren Datums (Urteil des Europäischen Gerichtshofs vom 24. November 2011, Az. C 468/10 und C 469/10; http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=de) und hat das deutsche Recht bislang noch nicht wesentlich beeinflusst.

Allerdings muss nach nunmehr fast 20 Jahren und der stürmischen Entwicklung der Informationstechnologie das Datenschutzrecht der Europäischen Union modernisiert werden. Auf Ersuchen des Europäischen Rates hatte die Europäische Kommission vor gut fünf Jahren die Initiative zu einer grundlegenden Novellierung ergriffen. Seit 2009 fanden öffentliche Anhörungen zum Datenschutz statt. Am 4. November 2010 veröffentlichte die Europäische Kommission die Mitteilung über ein Gesamtkonzept für den Datenschutz in der Europäischen Union (KOM(2010) 609); es folgte der Entwurf einer Datenschutz-Grundverordnung (Datenschutz-Grundverordnung – KOM(2012) 11 endgültig) sowie der Entwurf einer „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ (KOM(2012) 11 endgültig). Die Gesamtkonzeption ist erläutert in der Mitteilung „Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert“ (KOM(2012) 9 endgültig). Für den „zukunftsfesten“ Datenschutz werden fünf Eckpunkte formuliert:

- das Recht auf Vergessenwerden,
- Transparenz,
- Datenschutz durch Gestaltung,
- Verantwortung für den Umgang mit personenbezogenen Daten und
- eine unabhängige Datenschutzkontrolle, die abgestimmte Entscheidungen treffen soll (vgl. Viviane Reding, Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive, ZD 2011, 1 ff.).

Das Reformpaket stieß auf Zustimmung und Kritik (vgl. Masing, SZ vom 9. Januar 2012, S. 10; ders., Herausforderungen des Datenschutzes, NJW 2012, 2305 ff.). Der Bundesrat erhob am 30. März 2012 die Subsidiaritätsrüge (BR-Drs. 52/12). Ebenfalls die Subsidiaritätsrüge machten der schwedische Reichstag (MittRA 0042/2012), die Abgeordnetenkammer der Republik Italien (MittRA 0045/2012) und die belgische Abgeordnetenkammer (MittRA 0041/2012) geltend. Damit wurde allerdings nicht die Zahl der Rügen erreicht, die erforderlich ist, um rechtsförmliche Folgen zu entfalten. Die Europäische Kommission hat sich darauf beschränkt, den Rüge erhebenden Stellen gegenüber ihre entgegenstehende Auffassung zu begründen. Das Rechtsetzungsverfahren ist davon unbeeinflusst fortgeführt worden.

Das Europäische Parlament hat die Datenschutz-Grundverordnung inzwischen abschließend beraten; es hat eine große Zahl von Änderungen beschlossen, die vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) angeregt worden waren. Die nunmehr vorgelegte Fassung muss abschließend vom Europäischen Rat, also den Regierungen, sowie der Europäischen

Kommission erörtert und akzeptiert werden. Erst dann kann das Regelwerk in Kraft treten.

Zur Würdigung des Reformpakets ist vor allem auf folgende Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu verweisen:

- „Ein hohes Datenschutzniveau für ganz Europa!“ vom 21./22. März 2012,
- „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 7./8. November 2012,
- „Europa muss den Datenschutz stärken“ vom 13./14. März 2013 und
- Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutz-Grundverordnung (vgl. Tz. IV-A.2).

In der Stellungnahme zur Datenschutz-Grundverordnung vom 11. Juni 2012 wiesen die Datenschutzbeauftragten auf Kernpunkte hin, die ihrer Meinung nach unbedingt bei den weiteren Gesprächen zu beachten seien. So sei vor allem bei einer Harmonisierung des Datenschutzrechts ein möglichst hohes Datenschutzniveau für alle Mitgliedstaaten vorzuschreiben. Des Weiteren seien delegierte Rechtsakte auf das erforderliche Maß zu reduzieren. Technische und organisatorische Maßnahmen, welche zu treffen sind, um den Datenschutz zu gewährleisten, müssten sich auch in Zukunft am jeweiligen Stand der Technik orientieren. Die Möglichkeit der Verarbeitung von personenbezogenen Daten zur Profilbildung müsste in konkreten Regelungen begrenzt werden, vor allem bei Minderjährigen sei sie zu verbieten. Da es in den EU-Mitgliedstaaten kein einheitliches Verwaltungsverfahrens-, Verwaltungsprozess- und Verwaltungsvollstreckungsrecht gibt, sei die Regelung der „One-Stop-Shops“ für die Datenschutzaufsichtsbehörden nur praktikabel, wenn sie nicht als ausschließliche Zuständigkeit zu verstehen sei. Das beabsichtigte Kohärenzverfahren würde die Aufsichtsbehörden in deren Unabhängigkeit beeinträchtigen und verstoße damit sogar gegen die europäische Rechtsprechung.

Grundsätzlich befürworten die Datenschutzbeauftragten des Bundes und der Länder in der Entschließung vom 7./8. November 2012, dass ein einheitliches Datenschutzrecht für den öffentlichen Bereich und den nicht-öffentlichen Bereich gilt. Für den öffentlichen Bereich wird von den Datenschutzbeauftragten des Bundes und der Länder bekräftigt, dass in der Datenschutz-Grundverordnung Mindestanforderungen festgelegt werden sollten, um den jeweiligen Mitgliedstaaten die Möglichkeit einzuräumen, ein höheres Schutzniveau durch einzelstaatliche Regelungen zuzulassen. Das stärke den Subsidiaritätsgedanken und bekräftige die Verfassungsidentität der Mitgliedstaaten.

Mit Blick auf aktuelle Änderungsvorschläge verabschiedeten die Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 eine Entschließung „Europa muss den Datenschutz stärken“ mit Erläuterungen zu zehn Kernpunkten. In dieser Entschließung weisen die Datenschutzbeauftragten nochmals ausdrücklich auf ihre Befürchtungen hin, dass mit der neuen Datenschutz-Grundverordnung eine Absenkung des Datenschutzniveaus erfolgen könnte. Dies sei aus einigen Änderungsvorschlägen ersichtlich, in denen vorgeschlagen wird, Grundanforderungen an die Datenverarbeitung zu streichen, um für wirtschaftliche Interessen größere Spielräume zu lassen. Die angestrebten Regelungen widersprächen jedoch auch den Forderungen des Europäischen Parlaments, welches eine Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert hatte. Auch diese Entschließung und die entsprechenden Erläuterungen wurden an die EU-Kommissarin Viviane Reding übersandt.

Diese Stellungnahmen sind vom LfDI mitgetragen worden.

Der LfDI hat sich darum bemüht, in die Datenschutz-Grundverordnung auch Regelungen zur Datenschutzbildung und -erziehung aufzunehmen. Auf seinen Vorschlag sind in die detaillierte Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Vorschläge aufgenommen worden:

„Die Konferenz schlägt vor, eine Regelung ‚Erziehung und Bildung’ aufzunehmen. Der Datenschutz dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche

Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

'Art. xx – Erziehung und Bildung
Um sich in der Informationsgesellschaft behaupten zu können, ist den Bürgerinnen und Bürgern durch geeignete Maßnahmen Datenschutzkompetenz zu vermitteln. Sie ist Teil der übergreifenden Medienkompetenz; ihre Vermittlung ist eine gesamtgesellschaftliche Aufgabe in den Mitgliedstaaten, die hierbei von der Union unterstützt werden.'

Ausgehend von dem Vorschlag, eine Regelung zu 'Erziehung und Bildung' aufzunehmen, sollten auch die Aufgaben der Aufsichtsbehörden entsprechend erweitert werden. Die Konferenz schlägt für Art. 52 (2) daher folgenden Wortlaut vor:

‚Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und über geeignete Maßnahmen zum eigenen Schutz. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder.'“

Der LfDI hat diese Vorschläge nicht nur dem Berichterstatter des EU-Parlaments für die Datenschutz-Grundverordnung, dem Abgeordneten Jan Philipp Albrecht, übersandt; er hat sie auch dem Bundesinnenminister sowie der Bundesjustizministerin zur Verfügung gestellt. Beide Ressorts haben positiv reagiert und zugesagt, diese Überlegungen in die Verhandlungen des Rats einzuführen.

Problematisch ist, dass durch die Verordnung ein eigener Handlungsspielraum in den Mitgliedstaaten weitgehend wegfallen würde. Dies betrifft auf der Ebene der Bundesländer besonders die Gesetze, die sich auf die staatliche Verwaltung beziehen, denn nur in diesem Bereich haben die Landesgesetzgeber datenschutzrechtliche Regelungskompetenzen. Die Datenschutz-Grundverordnung würde deshalb die Landesdatenschutzgesetze obsolet machen. Es sollten in jedem Falle Gestaltungsspielräume für die Mitgliedstaaten angestrebt werden, insbesondere dürfen keine Obergrenzen vorgegeben werden, die zu einer Absenkung bereits erreichter Standards auf mitgliedsstaatlicher Ebene führen. Die grundsätzlich zu begrüßende Modernisierung des europäischen Datenschutzrechts darf nicht dazu führen, dass das deutsche Datenschutzrecht auch in seiner identitätsstiftenden Gestalt verloren geht. Dies wäre aus der Sicht des LfDI inakzeptabel.

Auch die Bundesregierung will eigene Datenschutzstandards nicht zugunsten einer europaweiten Kompromissregelung aufgeben. Dies verdeutlichte Bundeskanzlerin Angela Merkel in ihrer Regierungserklärung vom 29. Januar 2014, in der sie feststellte: „Wir arbeiten an einer europäischen Datenschutz-Grundverordnung mit Hochdruck. Aber wir achten dabei sehr darauf, dass der deutsche Datenschutz durch die Vereinheitlichung des europäischen Datenschutzes nicht unverhältnismäßig geschwächt wird.“ Der Verordnungsvorschlag sieht aber bisher keinerlei Öffnungsklauseln oder Subsidiarität vor, die es den einzelnen Mitgliedstaaten erlauben würde, strengere nationale Regelungen vorzusehen.

Das Ziel, die Datenschutz-Grundverordnung noch 2014 zu beschließen wurde allerdings verfehlt. Das neu gewählte Europäische Parlament wird sich deshalb noch einmal mit dem Entwurf der Datenschutz-Grundverordnung befassen müssen, auch die neu gewählte Europäische Kommission. Der Rat hat sich bisher noch gar nicht auf eine gemeinsame Linie verständigen können. Von einer Einigung im sog. Trilog – das sind die Konsultationen zwischen Europäischem Parlament, Europäischer Kommission und Europäischem Rat – ist man also noch weit entfernt. Der dafür jetzt ins Auge gefasste Termin, Mitte 2015, erscheint deshalb viel zu optimistisch.

Realistischer Weise wird man davon ausgehen müssen, dass eine Verabschiedung der europäischen Datenschutz-Grundverordnung nicht vor 2016 erfolgen wird. Da dann eine bei europäischen Regelungen übliche zweijährige Übergangsfrist

beginnen wird, wird die Datenschutz-Grundverordnung nicht vor 2018 in Kraft treten und selbst dann noch nicht uneingeschränkt handhabbar sein, weil zu diesem Zeitpunkt immer noch nicht die vielen Ausführungsbestimmungen vorliegen werden, die sich die Kommission in diesem Zusammenhang vorbehalten hat.

Das hat zur Folge, dass der Bund seine eigenen Bemühungen für einen besseren Datenschutz nicht mit Blick auf bevorstehende europäische Regelungen einstellen darf. Das wäre nicht mit seiner verfassungsrechtlichen Verpflichtung vereinbar, sich bei erkennbaren Gefahren schützend vor seine Bürgerinnen und Bürger zu stellen. Deshalb sollten vor allem die vom Bundesrat in der letzten Legislaturperiode eingebrachten Gesetzentwürfe zur Verbesserung des Datenschutzes bei sozialen Netzwerken (Gesetzesantrag des Landes Hessen vom 21. März 2011, BR-Drs. 156/11) und bei Geodatenangeboten im Internet (Gesetzentwurf des Bundesrates vom 9. Juli 2010, BR-Drs. 259/10) sowie das vom Bundesinnenminister am 1. Dezember 2010 vorgestellte Konzept eines „Rote-Linien-Gesetzes“ (Gesetzentwurf des Bundesministeriums des Innern zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile) wieder aufgegriffen und – mit weiterentwickelten Inhalten – parlamentarisch beraten werden. Damit würde dem europäischen Gesetzgeber auch verdeutlicht werden, welche Standards aus deutscher Sicht angemessen sind.

3.2.3 Vorratsdatenspeicherung

Bei der Vorratsdatenspeicherung werden Verbindungsdaten (Verkehrsdaten) gespeichert, also z.B.: Wer hat wann mit wem telefoniert, wer hat wem eine E-Mail geschrieben, mit welcher IP-Adresse war wer wie lange im Internet unterwegs? Das geschieht ohne bestimmten Anlass, also „auf Vorrat“. Die Inhalte der Kommunikation werden nicht gespeichert, doch lassen sich aus den Verbindungsdaten auch Rückschlüsse auf den Inhalt der Kommunikation ziehen.

Eine Speicherungspflicht trifft die Telekommunikationsunternehmen. Auf ihren Servern sollen die Daten für den Zugriff durch bestimmte staatliche Behörden verfügbar sein. Dieser ist nicht automatisch möglich, sondern nur unter bestimmten Voraussetzungen, z.B. zum Zweck der Aufklärung von Straftaten.

In Deutschland existiert derzeit keine Pflicht der Telekommunikationsunternehmen zur Vorratsdatenspeicherung. Die entsprechenden gesetzlichen Regelungen vom November 2007 hat das Bundesverfassungsgericht durch Urteil vom 2. März 2010 für nichtig erklärt. Es hat bei dieser Gelegenheit aber auch darauf hingewiesen, dass die Vorratsdatenspeicherung durch ein neues Gesetz unter stark eingrenzenden Bedingungen eingeführt werden könnte (Az. 1 BvR 256/08, 1 BvR 236/08, 1 BvR 586/08; vgl. 23. Tb., Tz. II-8.2.4; vgl. auch 22. Tb., Tz. II-7.2).

Gegen die EU-Richtlinie aus dem Jahr 2006, in der die Mitgliedstaaten verpflichtet worden sind, entsprechende gesetzliche Regelungen zu schaffen (RL 2006/24/EG vom 15. März 2006), hatten Irland und Österreich Klage erhoben. Am 8. April 2014 hat der Europäische Gerichtshof über diese Klage entschieden (EuGH C-293/122 und C-594/12, abrufbar unter http://www.datenschutz.rlp.de/de/gerichtsentscheidungen.php?submenu=euro). Er hat die genannte Richtlinie – so wie das Bundesverfassungsgericht die deutschen Regelungen – für ungültig erklärt, weil der darin angeordnete Eingriff in die Rechte der Bürgerinnen und Bürger unverhältnismäßig sei.

Im Koalitionsvertrag haben sich die regierungstragenden Parteien für eine erneute Gesetzesinitiative zur Umsetzung der europäischen Vorratsdaten-Richtlinie verständigt. Da eine solche Richtlinie aber wegen der Entscheidung des Europäischen Gerichtshofs derzeit nicht existiert, sollte schon aus diesem Grunde von einer entsprechenden Gesetzesinitiative Abstand genommen werden.

Im Übrigen sieht der LfDI in der Vorratsdatenspeicherung nach wie vor einen nicht verhältnismäßigen Eingriff in die Rechte der Bürgerinnen und Bürger. Das immer noch vorgebrachte Argument, man könne durch die vorrätigen Daten effektiver schwerwiegende Straftaten bekämpfen, ist auch heute noch umstritten und nicht zweifelsfrei belegt. Untersuchungen haben vielmehr gezeigt, dass noch nicht einmal 0,006 Prozent mehr Straftaten durch diese Datenspeicherung aufgeklärt werden könnten.

Mehrere Gutachten, Untersuchungen und Studien bezweifeln, dass dieser schwere Grundrechtseingriff im Verhältnis stehe zu den unter günstigsten Umständen zu erwartenden Verbesserungen bei der Strafverfolgung oder der Gefahrenabwehr. Der LfDI wird deshalb weiterhin dafür eintreten, dass die Telekommunikationsunternehmen ausschließlich die Daten speichern dürfen, die sie zu Abrechnungszwecken benötigen und diese auch wieder zeitnah löschen.

3.3 Bundesrecht

3.3.1 Beschäftigtendatenschutz

Die Skepsis, die der LfDI bereits im Datenschutzbericht 2010/2011 hinsichtlich der Erfolgsaussichten eines Beschäftigtendatenschutzgesetzes geäußert hatte (vgl. 23. Tb., Tz. I-2.2), war leider berechtigt. Bei diesem für den Datenschutz besonders wichtigen Projekt der alten Bundesregierung ist man keinen Schritt vorangekommen. Der Gesetzentwurf der Bundesregierung vom 15. Dezember 2010 (BT-Drs. 17/4230) war intensiv und kontrovers in den Bundestagsausschüssen, aber auch in der Öffentlichkeit diskutiert worden. Nach einer Anhörung im Bundestagsinnenausschuss blockierten sich jedoch die Koalitionsfraktionen offenbar gegenseitig. Mahnungen, wie die der Präsidentin des Bundesarbeitsgerichts, die mit Nachdruck ein Arbeitnehmerdatenschutzgesetz gefordert hatte, fruchteten nicht. Einmal mehr ist deutlich geworden, dass beim Beschäftigtendatenschutz kein Wille zum Kompromiss vorhanden ist. Nicht nur die politischen Akteurinnen und Akteure, auch die Interessenvertreterinnen und -vertreter auf Arbeitgeber- und Arbeitnehmerseite sehen sich offenbar außer Stande, dieses konfliktgeladene Thema zu einem einvernehmlichen Abschluss zu bringen. Eine vollständige Analyse der Gründe dieses Scheiterns würde den Rahmen dieses Tätigkeitsberichts sprengen, die wesentlichen Aspekte hierzu hat der LfDI in seinem Beitrag vor dem Rechtspolitischen Forum der Universität Trier „Die Geschichte des Beschäftigtendatenschutzes – von der Unfähigkeit zum Kompromiss" dargelegt (http://www.uni-trier.de/fileadmin/fb5/inst/IRP/Rechtspolitisches_Forum/65_Brink_EBook_geschuetzt.pdf).

In Stellungnahmen gegenüber der Landesregierung, im Rahmen von Veranstaltungen mit der Zukunftsinitiative Rheinland-Pfalz, mit den Geschäftsführern der Landesvereinigung Unternehmensverbände Rheinland-Pfalz sowie mit Gewerkschaften und Parteien hat der LfDI Bedeutung und Notwendigkeit einer gesetzlichen Regelung des Beschäftigtendatenschutzes sowohl für die Arbeitgeber- als auch für die Arbeitnehmerseite unterstrichen. Entgegen der etwas missverständlichen Bezeichnung „Beschäftigten-Datenschutz“ geht es bei diesem Gesetzesvorhaben nämlich nicht allein und einseitig um die Deklaration von Arbeitnehmerrechten; auf der Grundlage dieses Gesetzes ginge es auch um das Recht der Arbeitgeberseite, zu prüfen und sicherzustellen, ob die Arbeitnehmerinnen und Arbeitnehmer ihren arbeitsvertraglichen Verpflichtungen nachkommen. Dass dies auch angemessene Kontroll- und Überwachungsmaßnahmen der Arbeitgeberseite umfasst, ist eine Selbstverständlichkeit.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in einer Entschließung vom 22. Juni 2010 („Beschäftigtendatenschutz stärken statt abbauen“) eine Nachbesserung des Gesetzentwurfs der Bundesregierung gefordert. In ihrer Entschließung vom 17. März 2011 („Beschäftigtendatenschutz stärken statt abbauen“) hatte die Konferenz nochmals die Notwendigkeit bekräftigt, durch umfassende Datenschutzregelungen mehr Rechtssicherheit am Arbeitsplatz zu schaffen und bestehende Schutzlücken zu schließen. Dem hatte sich auch der Düsseldorfer Kreis mit seinem Beschluss vom 23. November 2011 angeschlossen, der Beschäftigtenscreenings bei AEO-Zertifizierungen betraf („Beschäftigtenscreenings bei AEO-Zertifizierungen wirksam begrenzen“). Vor dem Hintergrund datenschutzrechtlich zweifelhafter Praktiken der Zollverwaltung hatte der Düsseldorfer Kreis insbesondere Unternehmen aufgefordert, Datenscreenings nicht pauschal und anlasslos durchzuführen. Die Bundesregierung wurde gebeten, die derzeitige AEO-Zertifizierungspraxis einer umfassenden Evaluation zu unterziehen.

In ihrer Entschließung vom 25. Januar 2013 („Beschäftigtendatenschutz nicht abbauen, sondern stärken!“) erinnerte die Konferenz der Datenschutzbeauftragten an ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz.

Insgesamt zeigte sich die Konferenz enttäuscht vom Stand der Beratungen der Koalitionsfraktionen. Zwar nehme ein zwischenzeitlich vorgelegter Änderungsentwurf einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärke das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten werde jedoch – gemessen am ursprünglichen Gesetzentwurf – in wesentlichen Bereichen sogar noch weiter abgesenkt.

Als besonders bedenklich wurden die folgenden Regelungsvorschläge eingestuft:

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

Die Konferenz appellierte daher an den Bundestag, bei seinen Beratungen den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

Nachdem im Frühjahr 2013 auch die letzte Chance verstrichen war, im Innenausschuss des Deutschen Bundestages die Beratungen zum Gesetzentwurf wieder aufzunehmen, war das Projekt „Beschäftigtendatenschutzgesetz“ wieder einmal gescheitert.

Aber auch der Koalitionsvertrag der neuen Großen Koalition macht wenig Hoffnung, dass die für die Arbeitgeber- wie die Arbeitnehmerseite so notwendige Orientierung an einer gesetzlichen Regelung des Beschäftigtendatenschutzes in der nun laufenden Legislaturperiode realisiert wird. Denn im Koalitionsvertrag heißt es:

> „Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutz-Grundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen.“ („Deutschlands Zukunft gestalten“, Koalitionsvertrag zwischen CDU, CSU und SPD 18. Legislaturperiode, S. 70)

Inhaltliche Vorgaben, auf die man sich verständigt hätte, finden sich im Koalitionsvertrag also nicht, ebenso fehlen klare zeitliche Vorgaben. Damit stehen alle Beteiligten weiterhin ohne die nur durch eine gesetzliche Regelung zu schaffende Rechtssicherheit im Bereich des Beschäftigtendatenschutzes da.

Deshalb wird es in den kommenden Jahren zu den Aufgaben der Datenschutzaufsichtsbehörden zählen, durch Beratung im Einzelfall und durch eine vom LfDI angeregte Orientierungshilfe zum Beschäftigtendatenschutz zu verdeutlichen, wo die Überwachungs- und Kontrollbefugnisse der Arbeitgeberseite enden und wo das informationelle Selbstbestimmungsrecht der Arbeitnehmerinnen und Arbeitnehmer Vorrang genießt.

3.3.2 E-Government-Gesetz

Das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz) ist seit dem 1. August 2013 in Kraft (BGBl. I 2013, S. 2749). Ziel des Gesetzes ist es, die elektronische Kommunikation der Verwaltung zu erleichtern und Bund, Ländern und Kommunen zu ermöglichen, einfachere, nutzer-

freundlichere und effizientere elektronische Verwaltungsdienste anzubieten. Diese Zielsetzung wird vom LfDI unterstützt; allerdings bietet das Gesetz aus datenschutzrechtlicher Sicht an mehreren Punkten Anlass zur Kritik.

So birgt die in § 6 des Gesetzes vorgesehene elektronische Aktenführung Risiken. Bei elektronischen Akten gibt es die Möglichkeit von Volltextrecherchen, Verknüpfungen, Auswertungen und Profilbildungen, die zu beliebigen Zwecken ausgenutzt werden könnten. Die Einhaltung der datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Zweckbindung, der informationellen Gewaltenteilung und der Datensparsamkeit muss durch besondere Vorkehrungen gesichert werden, die das Gesetz aber nur in unzureichendem Maß konkretisiert.

Abzulehnen ist die in § 14 EGovG vorgesehene ausnahmslose Georeferenzierung. Diese Regelung verpflichtet die Behörden, in elektronische Register, die Angaben mit Bezug zu Grundstücken enthalten, eine Georeferenzierung (Koordinaten) zu dem jeweiligen Flurstück oder dem Gebäude aufzunehmen. Damit werden die Grundstücke und ihre Eigentümerinnen und Eigentümer eindeutig bestimmbar. Es besteht die Gefahr, dass die Zweckbindung der Registerdaten nicht eingehalten wird und Daten unzulässig zusammengeführt werden. Detaillierte Profilbildungen werden möglich. Die genannte Verpflichtung zur Georeferenzierung ist insbesondere bei den Registern im Personenstands-, Melde-, Pass- und Personalausweiswesen nicht erforderlich. Auch der Bundesrat hat in seiner Stellungnahme vom November 2012 entsprechende Zweifel geäußert (BR-Drs. 557/12 (B), Nr. 13).

Die Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt soll in jedem Fall auch durch eine Veröffentlichung im Internet erfüllt werden können (§ 15 EGovG). Insbesondere Veröffentlichungen von Gemeinden in ihren Mitteilungs- und Verkündungsblättern enthalten häufig personenbezogene Daten, die durch eine Veröffentlichung im Internet dauerhaft und weltweit verfügbar gemacht werden würden. Damit wird das informationelle Selbstbestimmungsrecht der Betroffenen erheblich beeinträchtigt. Durch eine Internetveröffentlichung wird nicht nur ein weltweiter Zugriff auf die Daten, sondern – mit Hilfe von Suchmaschinen – auch eine elektronische Auffindbarkeit ermöglicht, die es erlaubt, sämtliche zu den betroffenen Personen vorhandenen Angaben zu sammeln und – losgelöst vom ursprünglichen Informationszweck – zur Erstellung eines Persönlichkeitsprofils zu nutzen. Vor jeder Internetveröffentlichung müsste folglich mindestens eine Interessenabwägung durchgeführt und die Dauer der Veröffentlichung in der elektronischen Ausgabe begrenzt werden, um die Persönlichkeitsrechte Betroffener zu schützen (so auch die Forderung des Bundesrats, BR-Drs. 557/12 (B), Nr. 14). Das Gesetz enthält keine derartigen Pflichten.

Schließlich senkt das E-Government-Gesetz das Sicherheitsniveau bei der elektronischen Kommunikation mit Behörden. Bislang war nur die qualifizierte elektronische Signatur nach dem Signaturgesetz anerkannt. Nunmehr sind weitere Alternativen zur elektronischen Ersetzung der Schriftform eingeführt worden (§ 3a Abs. 2 VwVfG, § 36a Abs. 2 SGB I, § 87a Abs. 3 AO):

- Elektronische Formulare der Verwaltung dürfen in Verbindung mit einer sicheren elektronischen Identifizierung, insbesondere durch die Online-Ausweisfunktion (eID-Funktion) des neuen Personalausweises, übermittelt werden;
- De-Mails dürfen unter Verwendung der Versandoption nach § 5 Abs. 5 De-Mail-G, welche eine „sichere Anmeldung“ (§ 4 Abs. 1 Satz 2 De-Mail-G) der oder des Erklärenden voraussetzt, genutzt werden.

Diese Technologien stellen jedoch kein Äquivalent zur Schriftform dar, das mit der qualifizierten elektronischen Signatur vergleichbar und hinreichend sicher ist. Die eID-Funktion ermöglicht lediglich eine sichere Authentifizierung der absendenden Person. Durch das Übermitteln der persönlichen Personalausweisdaten kann weder gewährleistet werden, dass eine zusätzlich übersendete Erklärung inhaltlich von demjenigen herrührt, die sich als Ausstellende ausgeben, noch ist überprüfbar, ob die Mitteilung nach dem Absendevorgang auf dem Übertragungsweg verändert wurde. Ob die Nachricht auf dem Versandweg verändert wurde, können auch Empfängerinnen und Empfänger einer De-Mail nicht erkennen. Da der Absendenachweis nur durch die Anmeldung am De-Mail-Konto erfolgt, können im

Übrigen die Absenderinnen und Absender einer De-Mail nicht sicher bestimmt werden.

Aus Datenschutzsicht ist die Einführung von De-Mail als Möglichkeit der rechtsverbindlichen und sicheren Behördenkommunikation außerdem aufgrund der fehlenden Ende-zu-Ende-Verschlüsselung bedenklich. Eine durchgängige Verschlüsselung zwischen Senderinnen bzw. Sender und Empfängerin bzw. Empfänger ist standardmäßig nicht vorgesehen. Dies ist bereits im Zusammenhang mit der Entstehung des De-Mail-Gesetzes von den Datenschutzbeauftragten des Bundes und der Länder kritisiert worden (Entschließung vom 16. April 2009; „Datenschutz beim vorgesehenen Bürgerportal unzureichend“). Eine De-Mail liegt auf dem Versandweg im Verantwortungsbereich des Diensteanbieters kurz unverschlüsselt vor, um die Nachricht auf Schadsoftware zu überprüfen. Dieses Defizit wiegt insbesondere beim Versand besonders geschützter Daten, z. B. Sozial- oder Steuerdaten, schwer. Der hohe technische Maßstab, den das Sozialgesetzbuch sowie die Abgabenordnung in Bezug auf Datensicherheit wegen der besonderen Sensibilität der zu übermittelnden Daten setzen (insbesondere aufgrund des Verschlüsselungsgebots in Anlage zu § 78a SGB X und in § 87a Abs. 1 Satz 2 AO), wird im Bereich der De-Mail ausgehebelt. Eine Ende-zu-Ende-Verschlüsselung ist hier jedoch aus Datenschutzsicht unabdingbar.

Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach im Rahmen des Gesetzgebungsverfahrens auf die datenschutzrechtlichen Defizite hingewiesen. Bedauerlicherweise blieben diese Hinweise zum Schutz des Persönlichkeitsrechts der Bürgerinnen und Bürger – ebenso wie die entsprechenden Vorschläge des Bundesrates – unberücksichtigt. Der LfDI appelliert an den Landesgesetzgeber, bei dem geplanten E-Government-Gesetz für das Land Rheinland-Pfalz datenschutzgerechte Lösungen vorzuschreiben.

3.4 Landesrecht

3.4.1 Novellierung des Polizei- und Ordnungsbehördengesetzes: Verkürzung der Anordnungsfrist für die Quellen-TKÜ

Das Polizei- und Ordnungsbehördengesetz wurde ilm Berichtszeitraum in verschiedenen Punkten geändert. Der LfDI hatte Gelegenheit, dazu im Rahmen einer Anhörung des Innenausschusses dazu Stellung zu nehmen.

Aus der Sicht des Datenschutzes betraf die bedeutsamste Änderung die – vorgesehene und auch so beschlossene – Verkürzung der Anordnungshöchstdauer bei der Quellen-TKÜ von drei auf zwei Monate. Diese Verkürzung hat der LfDI begrüßt. Eine Quellen-TKÜ unterscheidet sich so deutlich von einer Telekommunikationsüberwachung mit herkömmlichen Mitteln, dass eine solche Fristverkürzung gerechtfertigt ist. Die Quellen-TKÜ betrifft die Fälle, in denen die Kommunikation verschlüsselt über das Internet erfolgt, etwa über Dienste wie „Skype“. Ein Zugriff auf die Inhaltsdaten auf dem Übertragungsweg ist dann nicht zielführend, weil die Polizei nicht in der Lage ist, diese starken Verschlüsselungen zu entschlüsseln. Im Regelfall erfordert dann der Zugriff auf die Gesprächsinhalte, dass das informationstechnische System, das an der Kommunikation als Quelle oder auch als Ziel beteiligt ist, so präpariert wird, dass vor der Verschlüsselung bzw. nach der Entschlüsselung auf diese Inhaltsdaten zugegriffen wird. Zu diesem Zweck müssen Veränderungen an den betroffenen Systemen vorgenommen werden. Nach dem Polizei- und Ordnungsbehördengesetz muss vor allem durch Vorkehrungen zum technisch-organisatorischen Datenschutz Folgendes sichergestellt sein:

- Es kann nur auf Gesprächsdaten zugegriffen werden.
- Die Datenerhebungen und -übermittlungen können nicht durch Dritte zur Kenntnis genommen werden.
- Die vorgenommenen Änderungen am System des Betroffenen werden auch wieder rückgängig gemacht.
- Alle getroffenen Maßnahmen werden auch für Prüfzwecke nachvollziehbar protokolliert.

Dies ändert aber nichts daran, dass zumindest für die Dauer der Maßnahme ein Computer so präpariert wird, dass von außen zugegriffen werden kann. Eine solche Veränderung ermöglicht zumindest theoretisch auch Dritten erleichterte Zugriffsmöglichkeiten und begründet weitere Gefahren, die die Funktion des infizierten Systems betreffen. In dieser Situation liegt eine besondere Gefährdung der betroffenen informationstechnischen Systeme, die bei herkömmlichen Maßnahmen der Telekommunikationsüberwachung nicht vorliegt.

Ein weiterer Aspekt tritt hinzu: Internettelefonie ist häufig mit der Übertragung von Videoaufnahmen der Gesprächsteilnehmer gekoppelt. Die Überwachungsmaßnahme betrifft dann zusätzlich zu den akustischen Signalen auch die Bildsignale. Auch darin liegt ein im Vergleich zur herkömmlichen Telefonie weitergehender Eingriff.

Besondere Schranken für solche Maßnahmen sind also grundsätzlich angemessen. Je kürzer eine solche Maßnahme andauert, desto kürzer ist auch die angesprochene Gefährdungs- und Eingriffssituation. Vor diesem Hintergrund ist eine zweimonatige Anordnungshöchstdauer zu begrüßen.

Der LfDI hatte ergänzend empfohlen, die Verlängerung solcher Maßnahmen auf jeweils einen Monat zu beschränken. Bei der Regelung der Online-Durchsuchung nach dem Polizeigesetz ist dies der Fall. Dort sind nach der ersten maximal dreimonatigen Anordnung Verlängerungen nur für jeweils einen weiteren Monat vorgesehen. Außerdem regte er an, die Zahl der zulässigen Verlängerungsanordnungen zu begrenzen. Des Weiteren hat er zu bedenken gegeben, ob nicht ein Gleichlauf der Fristenregelungen für die Quellen-TKÜ mit der Online-Durchsuchung sachlich sinnvoll wäre. Dieser Gleichlauf könnte etwa so aussehen, dass auch bei der Online-Durchsuchung die Anordnungshöchstfrist beim ersten Mal auf zwei Monate begrenzt wird und dass es dort in Bezug auf die Verlängerungsanordnungen bei der einmonatigen Frist bleibt, die dort derzeit schon gilt. Diese Einmonatsfrist für Verlängerungen könnte auch bei der Quellen-TKÜ vorgesehen werden.

Diesen ergänzenden Anregungen ist der Gesetzgeber nicht gefolgt. Im Rahmen der vorgesehenen Evaluation der neuen Regelung wird zu prüfen sein, ob diese Vorschläge des LfDI möglicherweise doch umgesetzt werden sollen.

3.4.2 Datenschutz im Strafvollzug – Landesjustizvollzugsdatenschutzgesetz

Der Schutz persönlicher Daten von Strafgefangenen, ihren Besucherinnen und Besuchern und sonstiger Betroffenen im Bereich des Justizvollzugs musste auf Landesebene neu geregelt werden, weil die Regelungskompetenz für den Strafvollzug vom Bund auf die Länder übergegangen war. Dies Neuregelung geschah durch das Landesjustizvollzugsdatenschutzgesetz, das am 1. Juni 2013 in Kraft getreten ist (vgl. Art. 3 LJVollzDSG). Seine Regelungen wurden auf der Grundlage eines vom LfDI erstellten Regelungsentwurfs in enger Abstimmung mit dem zuständigen Ministerium erarbeitet und sind daher nachdrücklich zu begrüßen.

Diese Regelungen gelten für alle Vollzugsformen; Spezialvorschriften für den Jugendstrafvollzug oder die Untersuchungshaft sind deshalb die Ausnahme. Das Gesetz schafft damit einen einheitlichen Datenschutzstandard und hebt sich deshalb im bundesweiten Vergleich von den übrigen Vollzugsgesetzen der Länder positiv ab.

In zahlreichen Fortbildungsveranstaltungen wurden die Bediensteten im Justizvollzug über den Inhalt dieser Neuregelungen und das ihnen zugrunde liegende Datenschutzverständnis unterrichtet. Dies erfolgte Hand in Hand mit Handlungsempfehlungen für den Justizvollzugsalltag.

3.4.3 Änderung des Schulgesetzes und Entwurf einer Schulstatistik-Verordnung

Aus datenschutzrechtlicher Sicht war in dem von der Landesregierung vorgelegten Entwurf zur Änderung des Schulgesetzes von Bedeutung, dass darin die Grundlage für die Einführung eines dauerhaften Kennzeichens geschaffen werden sollte. Ein solches Kennzeichen ist Voraussetzung dafür, dass in Verbindung mit dem von der Kultusministerkonferenz beschlossenen allgemeinen Kerndatensatz über die Verknüpfung von jährlichen Einzeldatensätzen der Verlauf von Schullaufbahnen nachvollzogen und statistisch ausgewertet werden kann.

Auf Empfehlung des LfDI wurde die einschlägige Vorschrift im Gesetzgebungsverfahren um

- einen Eingangssatz zum Zweck der Schulstatistik und
- eine Verordnungsermächtigung

ergänzt.

Ein erster Diskussionsentwurf für eine Landesverordnung zur amtlichen Schulstatistik liegt dem LfDI vor. Darin sollen insbesondere die Grundzüge des Verfahrens, die Erzeugung des Kennzeichens und die Erhebungs- und Hilfsmerkmale geregelt werden.

3.4.4 Landesgesetzliche Umsetzung des Krebsfrüherkennungs- und -registergesetzes des Bundes

Das Krebsfrüherkennungs- und -registergesetz des Bundes sieht u.a. vor, dass die Bundesländer zur Qualitätssicherung der medizinischen Versorgung bis Ende 2017 flächendeckend klinische Krebsregister mit einheitlichen Rahmenvorgaben einrichten. In den neuen Bundesländern sind solche Register bereits weit verbreitet.

Da zur Förderung der patientenbezogenen Zusammenarbeit im Behandlungsprozess und für Follow up-Untersuchungen ein umfassenderer Umgang mit Klardaten und sonstigen personenbezogenen Daten der Betroffenen notwendig sein wird als dies bisher bei epidemiologischen Krebsregistern der Fall war, ist es deshalb zu begrüßen, dass das Ministerium für Soziales, Arbeit, Gesundheit und Demografie gemeinsam mit dem LfDI bereits jetzt auf der Grundlage eines ersten Arbeitsentwurfs zur landesrechtlichen Umsetzung des Bundesgesetzes, die wichtigsten Datenschutzfragen, die im Zusammenhang mit der Einrichtung eines Krebsregisters stehen, erörtert hat.

3.4.5 Verordnung zur Ausführung des Landesgesetzes über die Geodateninfrastruktur

Das Landesgesetz über die Geodateninfrastruktur war am 23. Dezember 2010 vom Landtag verabschiedet worden und daraufhin bereits Gegenstand des letzten Tätigkeitsberichts (vgl. 23. Tb., Tz. I-2.3.2). Auf der Grundlage von § 14 Abs. 1 dieses Gesetzes wird derzeit eine Verordnung erarbeitet, die u.a. Näheres über den Datenschutz regeln soll. So wird der Entwurf insbesondere eine datenschutzrechtliche Regelung zum Betrieb des Geoportals RLP enthalten, über das der Öffentlichkeit der Zugang zu Metadaten, Geodaten und Geodatendiensten grundsätzlich eröffnet werden soll. Die Regelung geht zurück auf eine Anregung des LfDI, mit der den unterschiedlich hohen Anforderungen für den Zugang von öffentlichen und nichtöffentlichen Stellen zu Geodaten Rechnung getragen werden soll.

Die Verordnung wird voraussichtlich im dritten Quartal 2014 verkündet.

3.4.6 Landeskinderschutzgesetz

In einem aufwändigen Prozess ist das bereits im Jahre 2008 in Kraft getretene Landesgesetz zum Schutz von Kindeswohl und Kindergesundheit evaluiert worden. Entsprechend der gesetzlichen Vorgaben war der LfDI an der Erstellung des Evaluationsberichtes, der im Januar 2011 dem Landtag vorgelegt wurde, beteiligt. Zu den aus aus dem Bericht zu ziehenden datenschutzrechtlichen Schlussfolgerungen hat sich der LfDI zeitnah und ausführlich geäußert (vgl. 23. Tb., Tz. II-5.1.1). Aber erst im Februar 2012 sind die Evaluationsergebnisse – jedenfalls zum Teil – in einem ersten Entwurf zur Änderungen des Kinderschutzgesetzes aufgegriffen worden. Der LfDI hatte Gelegenheit, frühzeitig zu diesem Entwurf Stellung zu nehmen. Nach mehreren Gesprächen mit dem zuständigen Ministerium war eine Reihe von datenschutzrechtlichen Verbesserungen vereinbart worden:

- Der in § 6 Abs. 1 LKindSchuG enthaltene Katalog der an die Zentrale Stelle zu übermittelnden Meldedaten soll deutlich reduziert werden. Nicht mehr übermittelt werden sollen hinsichtlich der Kinder, die zu einer der in § 7 Abs. 3 LKindSchuG enthaltenen Früherkennungsuntersuchung anstehen, deren frühere Anschriften (Nr. 4), der Tag des Auszugs (Nr. 5) und deren Sterbetag und Sterbeort (Nr. 7). Zudem soll bezüglich der gesetzlichen Vertreter deren Geburtstag nicht mehr übermittelt werden.

- In den Mitteilungen der Zentralen Stelle an die zuständigen Gesundheitsämter über nicht vorliegende Untersuchungsbestätigungen (§ 8 Abs. 1 Satz 2 LKindSchuG) soll auf Informationen zu früheren ebenfalls nicht bestätigten Früherkennungsuntersuchungen verzichtet werden. In der Praxis hatten diese Angaben für die Gesundheitsämter keinen besonderen Erkenntniswert, so dass eine Übermittlung nicht erforderlich ist.

- Die bislang in § 9 Abs. 1 LKindSchuG enthaltene regelhafte Verpflichtung der Gesundheitsämter zur Unterrichtung des zuständigen Jugendamtes, wenn keine Bestätigung für die Durchführung einer vorgesehenen Früherkennungsuntersuchung vorliegt, soll aufgegeben werden. Statt dessen soll den Gesundheitsämtern in diesen Fällen ein Ermessensspielraum eingeräumt werden. Diese sollen dann einzelfallbezogen entscheiden, ob das zuständige Jugendamt über die fehlende Untersuchungsbestätigung unterrichtet werden soll oder ob ggf. mangels bestehender Anhaltspunkte für eine Kindeswohlgefährdung auf eine entsprechende Mitteilung verzichtet werden kann.

- Die in § 10 Abs. 1 und Abs. 2 LKindSchuG enthaltenen Speicherfristen für die bei der Zentralen Stelle und den Gesundheitsämtern festgelegt werden. Unabhängig vom Vorliegen oder Fehlen einer Untersuchungsbestätigung sollen die bei der Zentralen Stelle vorhandenen personenbezogenen Daten spätestens ein Jahr nach der Unterrichtung der gesetzlichen Vertreter (§ 7 Abs. 1 LKindSchuG) gelöscht werden.

  Die maximale Speicherdauer für die den Gesundheitsämtern von der Zentralen Stelle gemeldeten Fälle, bei denen kein weiterer Handlungsbedarf der Gesundheitsämter besteht, soll auf 18 Monate verkürzt werden. Damit soll die bisherige Speicherpraxis der Gesundheitsämter, auch solche Fälle, in denen trotz Meldung durch die Zentrale Stelle tatsächlich eine Früherkennungsuntersuchung durchgeführt wurde (sog. falschpositive Fälle), bis zu drei Jahre aufzubewahren, reduziert werden.

- Im Schulgesetz soll die in § 3 Abs. 2 Satz 3 normierte Pflicht der Schulen, bei gewichtigen Anhaltspunkten für die Gefährdung des Wohls einer Schülerin oder eines Schülers auf die Inanspruchnahme erforderlicher weitergehender Hilfen hinzuwirken, sofern eine Abhilfe durch schulische Maßnahmen nicht möglich ist, durch Verweisung auf § 4 des Gesetzes zur Kooperation und Information im Kinderschutz konkretisiert werden.

Trotz dieser Vereinbarungen wurde im Berichtszeitraum lediglich die Änderung des Schulgesetzes umgesetzt. Der Gesetzentwurf zur Änderung des Landeskinderschutzgesetzes selbst befindet sich nach Auskunft der Landesregierung im Frühjahr 2014 immer noch in der Ressortabstimmung. Ein Inkrafttreten der Änderungen noch im Laufe des Jahres 2014 werde jedoch angestrebt. Seit der Vorlage des Evaluationberichtes werden dann womöglich vier Jahre vergangen sein.

Auch wenn der Gesetzentwurf dann womöglich wesentliche datenschutzrechtliche Anliegen umsetzen wird, geschieht dies letztlich doch nur mit erheblicher Verspätung. Obwohl der Verfassungsgerichtshof in seiner Entscheidung vom 28. Mai 2009 (Az. B 45/08) die Verfassungsmäßigkeit der in dem Landeskinderschutzgesetz enthaltenen Eingriffe in das informationelle Selbstbestimmungsrecht ausdrücklich unter den Vorbehalt der Evaluationsergebnisse gestellt hatte, hat sich an den gesetzlichen Bestimmungen zum Einladungs- und Erinnerungsverfahren bis heute nichts geändert. Und obwohl der Verfassungsgerichtshof in seiner damaligen Entscheidung eindeutig feststellte, dass die durch den LfDI bereits in der mündlichen Verhandlung vorgetragenen und von der Landesregierung eingeräumten Defizite bei der praktischen Umsetzung des Gesetzes nur vorübergehend hinzunehmen seien, sind auch fünf Jahre danach immer noch keine der vom LfDI im Zusammenhang mit der Evaluation eingeforderten Korrekturen umgesetzt.

Aus datenschutzrechtlicher Sicht ist dies kritikwürdig. Die Landesregierung hat mit ihrem Verhalten die verfassungsgerichtlichen Vorgaben zum Schutz des informationellen Selbstbestimmungsrechts nicht beachtet. Dafür gab und gibt es keine zureichenden Gründe.

3.4.7 Rundfunkbeitragsstaatsvertrag

Im vorherigen Tätigkeitsbericht wurden die Anforderungen an ein datenschutzgerechtes Verfahren beim Einzug der Rundfunkbeiträge nach dem Rundfunkbeitragsstaatsvertrag geschildert (vgl. 23. Tb., Tz. II-1.1). Der LfDI hatte dargelegt, dass er in Verhandlungen mit den Vertreterinnen und Vertretern der Rundfunkanstalten darauf hingewirkt habe, in den jeweils durch die Rundfunkanstalten zu erlassenden Satzungen nach § 9 Abs. 2 Rundfunkbeitragsstaatsvertrag die datenschutzrechtlichen Anliegen zu berücksichtigen.

Diese Satzungen sind zwischenzeitlich mit im Wesentlichen gleichem Inhalt durch alle Landesrundfunkanstalten erlassen worden (z.B. Satzung des SWR über das Verfahren zur Leistung der Rundfunkbeiträge vom 3. Dezember 2012, GVBl. 2012, S. 418). Es konnte erreicht werden, dass darin die wesentlichen Anliegen des Datenschutzes Ausdruck gefunden haben. Von den neun Anforderungen, die im vorherigen Tätigkeitsbericht genannt worden sind, haben nur folgende keinen Niederschlag in diesen Regelungen gefunden.

- Es erfolgt keine Unterrichtung der Betroffenen „von Amts wegen“ darüber, welche Daten die Rundfunkanstalten von welchen Stellen ohne Beteiligung der Betroffenen erhoben haben. Die Betroffenen haben allerdings die Möglichkeit, diese Informationen im Wege eines Auskunftsantrages gegenüber der beitragserhebenden Stelle zu erlangen.
- Das Schwärzen irrelevanter Informationen auf den Leistungsbescheiden der Sozialbehörden, die zum Zweck der Beitragsermäßigung bzw. Beitragsbefreiung der Beitragserhebungsstelle vorzulegen sind, wird nicht ausdrücklich zugelassen.

Alle übrigen aus Datenschutzsicht formulierten Forderungen sind erfüllt worden. Dies wertet der LfDI als Erfolg. Es bleibt ein Anliegen, die in der Satzung enthaltenen datenschutzfreundlichen Regelungen nicht nur auf der Ebene der Satzungen, sondern im Staatsvertrag selbst zu verankern. Außerdem bleiben die o.g. noch unberücksichtigten Anliegen auf der Agenda. Im Rahmen der Erörterungen, die sich an die vorgesehene Evaluation des Staatsvertrages (vgl. LT-Drs. 16/556) anschließen werden, wird der LfDI auf diese Anliegen zurückkommen und für ihre Erfüllung eintreten.

In diesem Zusammenhang ist zu erwähnen, dass ein im Land ansässiges Straßenbauunternehmen eine Verfassungsbeschwerde gegen das Landesgesetz zur Ratifizierung des Rundfunkbeitragsstaatsvertrags (Landesgesetz zu dem Fünfzehnten Rundfunkänderungsstaatsvertrag, GVBl. 2011, 385) beim Verfassungsgericht des Landes erhoben hat (Az. VGH B 35/12). Die Beschwerdeführerin hat darin u.a. auch Datenschutzfragen thematisiert. Im Zuge dieses Verfahrens hat das Verfassungsgericht dem LfDI Gelegenheit zur Stellungnahme gegeben und ihn auch zur mündlichen Verhandlung geladen. Der LfDI hat in einer ausführlichen schriftlichen Stellungnahme und auch mündlich in der Verhandlung zum Ausdruck gebracht, dass mit dem Datenschutzstandard, der nunmehr erreicht worden ist, dem verfassungsrechtlich Gebotenen Genüge getan wird. Die noch zu konstatierenden datenschutzrechtlichen Defizite würden aus seiner Sicht nicht zur Verfassungswidrigkeit des angegriffenen Landesgesetzes führen. Eine Entscheidung des Verfassungsgerichts wird für Mai 2014 erwartet.

3.4.8 Fazit

Die Auffassung, vor allem im Interesse eines sog. freien Internets möglichst wenig zu regulieren mag unter netzideologischen und wirtschaftlichen Gesichtspunkten möglicherweise Sinn geben; sie entspricht aber ganz und gar nicht den Interessen der Bürgerinnen und Bürger. Der Staat darf sich nicht zurückziehen und den Bürgerinnen und Bürgern empfehlen, sich in digitalen Zeiten selbst zu helfen. Er muss sich – ganz im Gegenteil – schützend vor sie und ihr Grundrecht stellen, und d.h., für einen effektiven rechtlichen Datenschutzrahmen sorgen.

Das gilt schon für diejenigen, die in der Lage wären, sich zumindest ansatzweise selbst zu helfen. Es gilt aber erst recht und umso mehr für jene, die das von vornherein nicht oder nur sehr unzureichend können. Und das sind vor allem Kinder, die bereits millionenfach im Netz unterwegs sind und staatlichen Schutz dringend benötigen. Er wird ihnen bis heute nicht ausreichend gewährt.

Es wird lange dauern, bis sich im transatlantischen Verhältnis ein vergleichbares Datenschutzniveau entwickelt haben wird. Jedenfalls ist bis jetzt von der angekündigten Bill of Rights für den Datenschutz nichts zu sehen.

Schneller wird es auf europäischer Ebene möglich sein, die Digitalisierung unserer Gesellschaft zu reglementieren und die damit verbundenen Gefahren einzuhegen. Aber die europäische Datenschutz-Grundverordnung wird kaum vor 2018 zur Anwendung kommen, wobei zu hoffen bleibt, dass sich die Mitglieder der Europäischen Union überhaupt auf eine solche Grundverordnung verständigen können. Sie ist dringend erforderlich.

Solange es diese Verordnung nicht gibt, muss der nationale Gesetzgeber „einspringen“. Es gibt genügend Vorschläge, die zügig umgesetzt werden könnten.

Im Windschatten dieser Diskussion wird der Landesgesetzgeber vor allem für hinreichende bereichsspezifische Datenschutzgesetze für die öffentliche Verwaltung zu sorgen haben. Dies beginnt beim Polizeigesetz, endet beim Kinderschutzgesetz und schließt viele vergleichbare Regelungen mit ein. Die Erfahrung zeigt, dass dies in aller Regel gelingt. Aber es gibt auch Ausnahmen, wie das Kinderschutzgesetz zeigt.

II. Arbeitssschwerpunkte des LfDI

1. Information und Beratung

Zu den Aufgaben des LfDI und seiner Mitarbeiterinnen und Mitarbeiter gehört – neben der Beratung des Landtags und der Landesregierung (vgl. § 24 Abs. 4 LDSG) – in immer größerem Umfang die Information und Beratung der Bürgerinnen und Bürger, aber auch der Behörden des Landes und der Kommunen sowie vieler Wirtschaftsunternehmen. Information und Beratung gehen dabei oft ineinander über, ohne dass das eine mit dem anderen deckungsgleich wäre. Während die Beratung sehr häufig auf entsprechende Nachfragen zurückgeht oder die Folge von Eingaben und Beschwerden ist, erfolgt die Information in der Regel völlig unabhängig von solchen Anlässen. Sie geschieht in erster Linie durch Informationsveranstaltungen, Publikationen und Presseerklärungen, während die Beratung u.a. Gegenstand regelmäßiger Konsultationsgespräche etwa mit Wirtschaftsunternehmen sein kann oder Folge von entsprechenden Eingaben.

1.1 Veranstaltungen

1.1.1 Eigene Veranstaltungen

Der LfDI führte im Berichtszeitraum erneut zahlreiche Veranstaltungen durch, mit denen er Bürgerinnen und Bürger, aber auch Beschäftigte der Verwaltungen und privater Datenverarbeiter informiert und für datenschutzrechtliche Themen sensibilisiert hat.

Einen festen Platz im Veranstaltungskalender des LfDI hat mittlerweile das jährlich stattfindende **Speyerer Forum zur digitalen Lebenswelt**. Unter der wissenschaftlichen Leitung von Prof. Dr. Hermann Hill und Prof. Dr. Mario Martini von der Universität Speyer und dem LfDI bereiten die Tagungen aktuelle Themen unserer digitalen Informationsgesellschaft auf. So stand das Forum 2012 im Zeichen von „Facebook, Google & Co. – Chancen und Risiken“. 2013 hieß es „Gemeinsam für den transparenten Staat!“. Vor und mit einem großen Auditorium referierten und diskutierten Expertinnen und Experten aus Politik, Verwaltung, Wissenschaft und Zivilgesellschaft. Die Ergebnisse werden in einer Schriftenreihe veröffentlicht.

Im Rahmen öffentlicher Veranstaltungen wird auch der **Datenschutzpreis** verliehen, was im Berichtszeitraum mittlerweile bereits zum vierten Mal geschehen ist, wobei namhafte Fachleute zu verschiedenen digitalen Fragenstellungen einleitend referieren und die Preisträger sodann die Möglichkeit erhalten, ihre Arbeiten vorzustellen.

Dieser Preis, der gemeinsam mit dem Ministerium für Bildung, Wissenschaft, Weiterbildung und Kultur in den Kategorien „Recht und Sozialwissenschaft“ und „Technik und Informationsfreiheit“ sowie in einer Sonderkategorie verliehen wird, hat mittlerweile einen festen Platz in der Datenschutzlandschaft von Rheinland-Pfalz. Dies zeigt auch die steigende Zahl hochkarätiger Bewerbungen.

Wissenschaftspreis des LfDI
Informationen zum Wissenschaftspreis:
http://www.datenschutz.rlp.de/wissenschaftspreis/
Wissenschaftspreis 2012 – Preisträger und Arbeiten:
http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2013043002

Vor dem Hintergrund der Snwoden-Enthüllungen hat der LfDI sein Angebot zum Selbstdatenschutz durch sog. **„Crypto-Sessions“** ergänzt. In Zusammenarbeit mit dem Landesfilmdienst/Institut für Medienpädagogik Mainz und dem Chaos Computer Club Mainz/Wiesbaden hat er mehrere solcher Workshops durchgeführt.

Die Crypto-Sessions waren öffentlich und richteten sich an interessierte Bürgerinnen und Bürger. Gezeigt wurde dabei, wie man sich mit Verschlüsselung gegen unerwünschtes Lauschen und Datensammeln zur Wehr setzen kann. Nicht alles soll vertraulich bleiben, manches aber vielleicht doch. Ob unverfänglich oder nicht, spielt dabei keine Rolle. Ausschlaggebend ist der Wunsch der Nutzerinnen und Nutzer nach Vertraulichkeit.

Konzept der Crypto-Sessions:
In drei Workshops wird Schritt für Schritt gezeigt, wie mit frei erhältlichen Lösungen E-Mailinhalte verschlüsselt, Dateien sicher auf Online-Speichern

abgelegt und Datenspuren im Internet vermieden werden können:

Workshop 1: „Digitales Kauderwelsch“
E-Mailverschlüsselung mit GnuPG

Workshop 2: „My Eyes Only”
Dropbox & Co sicher nutzen mit TrueCrypt und 7Zip

Workshop 3: „Deine Spuren im (digitalen) Sand“
Datenspuren im Internet vermeiden

Die Teilnehmerinnen und Teilnehmer können dabei auf ihren eigenen Geräten und bei Bedarf angeleitet und unterstützt durch Moderatoren den Einsatz von Verschlüsselungslösungen ausprobieren und einen Blick in die gar nicht so komplizierte Welt der Verschlüsselung werfen.

Datenschutz ist immer häufiger auch **Verbraucherdatenschutz**. Deshalb arbeitet der LfDI auch eng mit dem Ministerium für Justiz und Verbraucherschutz und der rheinland-pfälzischen Verbraucherzentrale zusammen. Dies fand in mehreren gemeinsamen Veranstaltungen seinen Ausdruck. Dazu zählen eine Aufklärungsveranstaltung zum Thema „Smartphones und Apps“ im August 2012 (vgl. Tz. III-8.2.3) sowie der Verbraucherdialog „Mobile Payment“ im Jahr 2013 (vgl. Tz. III-8.2.1).

In Fortsetzung des im Juni 2011 begonnenen Dialogs mit den Krankenhäusern im Lande führte der LfDI im September 2012 einen **Workshop zum datenschutzgerechten Einsatz von Krankenhausinformationssystemen (KIS)** durch. Hintergrund der Veranstaltung war die im Frühjahr 2011 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu der Thematik veröffentlichte Orientierungshilfe (OH KIS; vgl. Tz. II-7.1). An der Veranstaltung nahmen neben zahlreichen Vertreterinnen und Vertretern der betroffenen Krankenhäuser und Träger auch die Krankenhausgesellschaft Rheinland-Pfalz sowie der Bundesverband Gesundheits-IT (bvitg) teil.

Die Landesseniorenvertretung führte in Kooperation mit dem LfDI im August 2012 die **Fachtagung „Silver Surfer – Sicher online im Alter“** durch: Ein Drittel der deutschen Internetnutzerinnen und -nutzer über 45 Jahren nutzt bereits das Internet und die komplette Bandbreite der darin angebotenen Dienste. 32 Prozent der „Generation 50+“ ist in sozialen Netzwerken aktiv. Smartphones und Tablet-Computer sind nicht nur bei jungen Menschen beliebt. Die sog. „Silver Surfer“ stellen eine wachsende Gruppe der Internetnutzerinnen und -nutzer dar. Medienbildung, Medienkompetenz und damit auch Datenschutz ist somit ein Thema, das nicht nur auf die junge Generation beschränkt werden darf.

Diese Veranstaltungen stehen beispielhaft für die Reihe von Informationsveranstaltungen, die der LfDI im Berichtszeitraum durchgeführt hat. Sie werden ergänzt durch eine Vielzahl von externen Veranstaltungen, an denen er bzw. seine Mitarbeiterinnen und Mitarbeiter als Referenten teilgenommen haben.

1.1.2 Externe Veranstaltungen

Die Bandbreite der externen Veranstalter, die auf den LfDI und seine Mitarbeiterinnen und Mitarbeiter zurückgegriffen haben, reicht vom Bundesministerium der Verteidigung und dem hiesigen Innenministerium, der Deutschen Richterakademie in Trier über diverse Hochschulen, wie z.B. die Deutsche Universität für Verwaltungswissenschaften in Speyer, die Universitäten in Trier, Koblenz-Landau, Frankfurt und Mannheim bis zu diversen Kammern, wie den Industrie- und Handelskammern und den Rechtsanwaltskammern in Koblenz und Zweibrücken. Aber auch das ist nur ein Ausschnitt aus dem Kreis der Veranstaltungen mit Beteiligung des LfDI.

Die dabei behandelten Themen betrafen aktuelle Fragen des Internets und seines mobilen Zugangs, Aspekte der IT-Sicherheit, die europäische Datenschutz-Grundverordnung, das in der parlamentarischen Beratung letztlich gescheiterte Beschäftigtendatenschutzgesetz und immer wieder Fragen um das Thema „Datenschutz als Bildungsaufgabe“, worauf im Einzelnen noch näher eingegangen wird (vgl. Tz. II-2). Spezielle Themen, wie der Forschungsdatenzugang im Bildungswesen, gaben Anlass, sich mit bis dahin nur beiläufig behandelten Datenschutzfragen intensiver auseinanderzusetzen.

Mit seiner Vortragstätigkeit verfolgt der LfDI insbesondere das Ziel, die mitunter schwierige Arbeit der betrieblichen Datenschutzbeauftragten zu unterstützen. Deshalb hielten die Mitarbeiterinnen und Mitarbeiter des LfDI zahlreiche Vorträge auf den sog. Erfahrungsaustauschkreisen der betrieblichen

Datenschutzbeauftragten (ERFA-Kreise) in Koblenz, Trier, Ludwigshafen und Mainz. Hinzu kommen Vorträge auf der Ebene der Bundesvereinigungen der Datenschutzbeauftragten, also bei den Jahrestagungen des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD e.V.) und der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.).

Weitere Anfragen erreichten den LfDI von Seiten der Gewerkschaften und von arbeitnehmernahen Verbänden, hier stand das Thema Beschäftigtendatenschutz im Mittelpunkt. Beratungs- und Vortragstätigkeit leistete der LfDI insbesondere für die Vereinte Dienstleistungsgewerkschaft (ver.di), für den Bundesvorstand des Bundes der Gewerkschaften (DGB) sowie für verschiedene Technologieberatungsstellen (tbs).

1.2 Publikationen

Die Arbeit des LfDI spiegelt sich auch in zahlreichen Publikationen wider. So wurde insbesondere im Bildungsbereich ein eigener Flyer zur Datenschutzrelevanz bei Facebook mit dem Titel: „Was Du über Facebook wissen solltest“ erarbeitet. Dieser richtet sich vornehmlich an Jugendliche und wurde mit einer Stückzahl von 10.000 Exemplaren gedruckt, wobei eine Neuauflage bereits in Planung ist.

Parallel zur Veröffentlichung der Internetjugendseite des LfDI „www.youngdata.de“ wurden verschiedene Informationsflyer und Werbematerialien produziert. Hierzu gehörten 1.000 Flyer, die über den Inhalt der neuen Homepage informierten, 500 Plakate für Schulen in Rheinland-Pfalz und 2.000 Werbeflyer in Visitenkartenform (vgl. Tz. II-3.1).

Weiterhin wurde ein Flyer „Mit Sicherheit gut behandelt“ im Rahmen der gleichnamigen Initiative des LfDI und der Kassenärztlichen Vereinigung Rheinland-Pfalz aufgelegt (vgl. Tz. II-3.3).

Der elektronische Praxisratgeber „Selbstdatenschutz“ ergänzte offline das Internetangebot des LfDI zum Selbstdatenschutz und diente als Material für die Crypto-Sessions des LfDI. Die Crypto-Sessions des LfDI wurden mit eigenen Plakaten beworben (vgl. Tz. II-1.1.1).

Ein Tutorial „Datenspuren im Internet“ ist abrufbar im Internetangebot des LfDI.
(vgl. http://www.datenschutz.rlp.de/de/selbstds.php?submenu=datenspuren)

Schließlich arbeitete der LfDI an der Publikation „Silver Surfer“ der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz mit (vgl. Tz. II-1.1.1).

1.3 Pressearbeit

Um die Öffentlichkeit über die aktuellen Entwicklungen im Bereich des Datenschutzes zu informieren und für Datenschutzfragen zu sensibilisieren, war und ist eine intensive Presse- und Medienarbeit zwingend erforderlich. Sie ist eine der wesentlichen Bedingungen dafür, dass sich die Menschen in unserer digitalisierten Welt zumindest ansatzweise noch behaupten und am Ende vielleicht auch gegen die digitale Ausbeutung ihrer Privatsphäre zur Wehr setzen können.

Die zahlreichen Stellungnahmen in diversen Rundfunk- und Fernsehanstalten, insbesondere im Südwestrundfunk, dokumentieren das immer noch steigende öffentliche Interesse am Datenschutz. Um ihm gerecht zu werden, hat der LfDI aber vor allem auch seine Pressearbeit ausgeweitet. Dies kommt nicht zuletzt in den zahlreichen Presseerklärungen zum Ausdruck, die auf unterschiedlichen Wegen ihre Adressaten erreichen, nicht zuletzt auch über die Webseite des LfDI, in der unter „Aktuelles“ sämtliche Presseerklärungen aufgelistet werden.

Die Zahl der Presserklärungen verdeutlicht die Entwicklung auf diesem Feld. Waren es im Jahre 2005 gerade einmal sechs Presseerklärungen aus der Feder des LfDI, so sind es mittlerweile pro Jahr über 50 Presseerklärungen.

Mittlerweile lässt sich auch die Resonanz entsprechender Meldungen jedenfalls ansatzweise nachvollziehen. Es ist keine Seltenheit, dass Presseerklärungen des LfDI von „heise.de“ aufgegriffen und deren Meldungen dann intensiv im Netz diskutiert werden. Oft sind es bis zu 1.000 persönliche Beiträge, die als Reaktion auf einzelne Meldungen des LfDI gepostet werden.

Und noch eines darf nicht unterschätzt werden: Im Rückblick bieten diese Presserklärungen auch einen interessanten Überblick über die Entwicklung des Datenschutzes in den vergangenen Jahren.

1.4 Beratungen aufgrund von Eingaben

Die Zahl der Eingaben im öffentlichen und privaten Bereich ist im Berichtszeitraum erheblich angestiegen. Den LfDI erreichten in den Jahren 2012 und 2013 rund 2.000 schriftliche Eingaben. Dazu kamen mehr als 7.000 telefonische Anfragen. Da die personellen Kapazitäten nicht im selben Maß angestiegen sind, führte dies zwangsläufig zu längeren Bearbeitungszeiten. Im Einzelnen stellt sich die Entwicklung wie folgt dar:

1.4.1 Im öffentlichen Bereich

Eingaben zu Datenschutzfragen im öffentlichen Bereich werden zunehmend auf elektronischem Weg an den LfDI gerichtet. Häufig geschieht dies über das Kontaktformular im Internetangebot des LfDI (https://www.datenschutz.rlp.de/de/kontaktform.php). Im Jahr 2012 waren dies 100 Anfragen, im Jahr 2013 120 Anfragen. Ebenso häufig erfolgt die Kontaktaufnahme per E-Mail über die Adresse „poststelle@datenschutz.rlp.de“. 2012 entschieden sich 130 Personen für diesen Weg, 2013 waren es 150. Hinzu kommen die Eingaben auf dem herkömmlichen Postweg: 2012 ca. 300, 2013 ca. 350. Zusammengenommen befassten sich also rund 1.150 schriftliche Eingaben im Berichtszeitraum mit Datenschutzfragen aus dem öffentlichen Bereich. Hinzu kamen mehrere Tausend telefonische Informationswünsche und sonstige Anfragen.

Der LfDI sieht es als eine seiner wichtigsten Aufgaben an, die Fragen von Bürgerinnen und Bürgern zum datenschutzkonformen Verhalten der Behörden zu beantworten. Allerdings versteht er sich nicht nur als Beratungsorgan, sondern auch als Einrichtung des „vorgezogenen Rechtsschutzes“, als kostengünstige und effiziente Alternative zum formellen Rechtsweg (der normalerweise darin besteht, Widerspruch einzulegen und Klage beim Verwaltungsgericht zu erheben). Sein Ziel ist es, den Betroffenen zu ihrem Recht zu verhelfen und ggf. die Verwaltungen zu einem datenschutzkonformen Verhalten gegenüber den Bürgerinnen und Bürgern zu bewegen.

Die Themenpalette dieser Anfragen und Eingaben ist vielgestaltig: Es wird beispielsweise gefragt, ob Geburtstage von Gemeindebürgerinnen und -bürgern im Amtsblatt veröffentlicht werden dürfen (vgl. Tz. III-7.2.1), ob die GEZ-Nachfolgeorganisation (der „ARD ZDF Deutschlandradio Beitragsservice“) rechtmäßig Meldedaten erhalten darf, ob die Polizei Daten rechtmäßig speichert (vgl. Tz. III-4.1), ob die Ausländerbehörde im Falle des Besuchs visapflichtiger Ausländerinnen und Ausländer zu weitgehende Datenerhebungen durchführt, ob Lehrkräfte Handyfotos der Schülerinnen und Schüler machen dürfen (vgl. Tz. III-6.1.5) und vieles andere mehr.

Die Beantwortung der entsprechenden Fragen ist nur selten ohne Beteiligung der betroffenen Verwaltungen möglich. Oft wird der LfDI erst durch Eingaben auf Verfahrensdefizite aufmerksam. Da der LfDI aus Kapazitätsgründen systematische und anlasslose Kontrollen von Verwaltungsbehörden nicht mehr so häufig durchführen kann wie in früheren Jahren, gewinnen die Eingaben nicht nur zahlenmäßig, sondern auch mit Blick auf das Datenschutzniveau im Lande immer mehr an Bedeutung.

1.4.2 Im privatwirtschaftlichen Bereich

Die Vielzahl der Datenschutzskandale der vergangenen Jahre – Deutsche Telekom, Deutsche Bahn, Lidl und Co. – haben zu der Einsicht geführt, dass das Grundrecht auf informationelle Selbstbestimmung heute besonders durch die Privatwirtschaft gefährdet wird. Zwar hat der staatliche Datenschutz seinen Ursprung im Schutz der Bürgerinnen und Bürger vor übermäßigem behördlichen Informationsinteresse – das Gefährdungspotential des privaten Sektors für das Grundrecht auf informationelle Selbstbestimmung ist jedoch unbestreitbar (vgl. 23. Tb., Tz. II-2.1). Auch die Enthüllungen zum unermesslichen Datenhunger der NSA, also eines staatlichen Geheimdienstes, stellen diese Einschätzung nicht in Frage. Sie betonen sie sogar, wenn man berücksichtigt, dass die NSA in wesentlichen Bereichen an den Datensammlungen von Privatunternehmen anknüpft: an die Verkehrsdatensammlungen privater Telekommunikationsfirmen, an die

Datenspeicher von Facebook, Amazon und Co. Das Wort des ehemaligen Präsidenten des Bundesverfassungsgerichts, Prof. Dr. Hans-Jürgen Papier, der vor der Gefahr eines „Super-GAUs des Datenschutzes“ in der Privatwirtschaft warnte, hat daher immer noch Bestand und Berechtigung.

Dies zeigt auch die Entwicklung der Eingaben von Bürgerinnen und Bürgern im privatwirtschaftlichen Bereich. Im Berichtszeitraum waren es rund 4.000 Eingaben und Anfragen. Rund 800 erfolgten in schriftlicher Form, mehr als 3.000 wurden fernmündlich an den LfDI herangetragen. Das ist im Vergleich zu den Jahren 2010 und 2011 ein weiterer Anstieg. Seinerzeit waren es rund 700 schriftliche Anfragen und ca. 3.000 mündliche Eingaben und Anfragen. Mit jährlich ca. 2.000 schriftlichen und fernmündlichen Eingaben und Anfragen aus dem privatwirtschaftlichen Bereich sind beim LfDI allerdings auch die Kapazitätsgrenzen erreicht.

Schwerpunkte der Eingaben sind wie in den letzten Jahren auch die Bereiche Arbeitnehmerdatenschutz, Videoüberwachung, Internetnutzung, Adresshandel, Wirtschaftsauskunfteien sowie Fragen zur Tätigkeit der betrieblichen Datenschutzbeauftragten.

Generell ist – wie schon im vergangenen Berichtszeitraum (vgl. 23. Tb., Tz. II-2.1) – festzustellen, dass sich die Datenschutzprobleme im Bereich der Privatwirtschaft parallel zur exponentiellen Entwicklung der Kommunikationstechnik in immer kürzeren Zeiträumen steigern. Riesige Datenbestände mit teils sensiblen, in jedem Falle aber umfassenderen und damit höchst aussagekräftigen Informationen entstehen bei immer mehr privaten Unternehmen – Big Data ist keineswegs beschränkt auf Amazon oder Google. Die Miniaturisierung von Speichern macht das unbefugte Kopieren und Übermitteln immer leichter, damit werden auch missbräuchliche Datenverwendungen in immer neuen Dimensionen möglich. Die neuen Gefahren von Big Data im Internet, also durch eine lückenlose Erfassung und Auswertung des Nutzungsverhaltens, aber auch durch Identitätsdiebstähle, Phishing oder virtuellen Exhibitionismus sind ständige Begleiter aller Nutzerinnen und Nutzer. All das spiegelt sich in den Eingaben und Anfragen der Bürgerinnen und Bürger.

Im privatwirtschaftlichen Bereich beschränkt sich die Beratungstätigkeit des LfDI aber nicht nur auf die Verbraucherinnen und Verbraucher und die Arbeitnehmerinnen und Arbeitnehmer, sondern erstreckt sich zunehmend auch auf die Unternehmen selbst.

1.5 Beratungen von Unternehmen

Die Beratung von Unternehmen ist keine „Nebenpflicht“ des LfDI, sondern steht gemäß § 38 Abs. 1 Satz 2 BDSG im Zentrum seiner Tätigkeit. Dort heißt es: Die Aufsichtsbehörde „berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse“.

Dies bedeutet für die Arbeit des LfDI zweierlei: Zum einen gibt es einen Rechtsanspruch der Unternehmen mit Sitz in Rheinland-Pfalz, vom LfDI – kostenfrei! – in allen Fragen um den Datenschutz informiert und unterstützt zu werden. Zum anderen muss diese Beratungsleistung konstruktiv erbracht werden. Es genügt also gerade nicht, dass die Aufsichtsbehörde den anfragenden Unternehmen erklärt, was aus Gründen des Datenschutzes alles nicht geht. Vielmehr ist der LfDI verpflichtet, im Interesse der Unternehmen nach Wegen zu suchen, wie das unternehmerische Geschäftsmodell mit dem geltenden Datenschutzrecht in Einklang gebracht werden kann. Dies schließt natürlich im Einzelfall nicht aus, dass allzu verwegenen Geschäftsideen im Ergebnis datenschutzrechtliche Vorschriften entgegenstehen. In aller Regel wird der LfDI jedoch Lösungsmöglichkeiten suchen und finden, wie das Unternehmen seine Ziele datenschutzkonform umsetzen kann. Zu einer solchen Beratungsleistung ist der LfDI verpflichtet – und im Rahmen seiner personellen Möglichkeiten auch gerne bereit.

Gerade weil die Leistungsfähigkeit des LfDI bei seiner Beratungstätigkeit begrenzt ist, verfolgt der LfDI seit 2009 das Ziel, durch engen Kontakt zu Großunternehmen in Rheinland-Pfalz seinen Aufgaben gerecht zu werden. Daher steht der LfDI mit einem halben Dutzend von „Global Playern“, die es in Rheinland-Pfalz vor allem in den Bereichen Chemie, Pharmazeutika, Logistik, Versicherungen und Medizintechnik durchaus gibt, in besonders engem Kontakt. Dies bedeutet, dass sich Mitar-

beiterinnen und Mitarbeiter des LfDI in der Regel zu Quartalsgesprächen mit diesen Unternehmen treffen, aktuelle und übergreifende Datenschutzfragen aus dem Unternehmen erörtern und umgekehrt über rechtliche und rechtspolitische Entwicklungen aus dem Datenschutz in Deutschland und Europa berichten.

Die Vorteile einer solchen Vorgehensweise liegen auf der Hand: Datenschutzfragen können sehr frühzeitig – idealerweise noch vor Implementierung neuer Geschäftsprozesse – erörtert und entschieden werden; die Unternehmen erfahren frühzeitig von der Position der Datenschutzbehörden zu relevanten Rechtsfragen; umgekehrt wird der LfDI in Kenntnis gesetzt von unternehmerischen Entwicklungen, die häufig auch in anderen Unternehmen relevant werden, was gleichzeitig die Beratungskompetenz des LfDI steigert.

Von solch einem intensiven Austausch haben alle Beteiligten – keineswegs nur die beratenen Großunternehmen – etwas. Er ist von Vorteil für die Kundinnen und Kunden, Geschäftspartnerinnen und -partner und Beschäftigte der Großunternehmen, aber ebenso für alle anderen „verantwortlichen Stellen“ in Rheinland-Pfalz, die auf die wachsende Beratungskompetenz des LfDI vertrauen können.

2. Bildung und Erziehung

2.1 Allgemeines

Seit mehreren Jahren sieht der LfDI eine seiner Hauptaufgaben in der digitalen Aufklärung und darin, den Datenschutz auch als Bildungsaufgabe zu verstehen und wahrzunehmen.

Denn die um sich greifende Digitalisierung unseres Lebens stellt unsere Gesellschaft und jeden Einzelnen vor tiefgreifende und völlig neue Herausforderungen, die – wie bereits eingangs dargestellt – (vgl. Tz. I-1) mit der exzessiven Erhebung, Sammlung und Nutzung von persönlichen Daten und Information verbunden sind und deshalb sehr viel mit dem Datenschutz zu tun haben. Diese Entwicklung gefährdet unsere Privatsphäre, beeinträchtigt unsere Freiheit und stellt unsere Möglichkeit, selbst über die Preisgabe unserer Daten zu entscheiden, fundamental in Frage.

Will man die Menschen befähigen, sich gleichwohl halbwegs souverän im Netz zu bewegen und zumindest partiell die Verfügungsgewalt über ihre Daten zu behalten oder wieder herzustellen, sind entsprechende Gegenstrategien in unterschiedlichen Handlungsfeldern vonnöten. Zu ihnen gehören auch die Erziehung und die Bildung, und zwar aller Generationen, vornehmlich aber der jungen Generation, also der Kinder und Jugendlichen.

In diesem Zusammenhang geht es um die Vermittlung von digitalen Informationen und Wissen, auch um die Förderung eines wachen Bewusstseins, das auch zu Verhaltensänderungen bewegen soll. Es geht darum, die Menschen zu einem verantwortungsvollen Umgang mit den eigenen Daten und zu einem rücksichtsvollen Umgang mit den Daten anderer zu veranlassen.

Allerdings sind Wissensdefizite, fehlendes Risikobewusstsein, digitale Sorglosigkeit und leichtfertiges, ja auch rücksichtsloses Verhalten vor allem im Netz an der Tagesordnung, auch und vor allem in der jungen Generation, der „Generation Internet“ oder „Generation Facebook“, wie man sie verschiedentlich bezeichnet.

Deshalb ist es zuvorderst die Aufgabe der Schulen, die jungen Menschen in die Lage zu versetzen, selbstbewusst, selbstbestimmt und selbstkritisch von den Möglichkeiten und Chancen des Internet Gebrauch zu machen.

Im Kontext der digitalen Medienbildung werden gerade die Datenschutzbeauftragten im Bund und in den Ländern eine größere Rolle übernehmen müssen als dies bisher der Fall ist. Das gilt für den schulischen, aber auch für den außerschulischen Bereich, und das gilt für die Generation „Facebook“ ebenso wie für die „Silver Surfer“.

Die Datenschutzbeauftragten werden vor allem deshalb eine größere Rolle übernehmen müssen, weil niemand so sehr für diese Aufgabe prädestiniert ist wie sie und weil andere potentielle Wissensvermittler mit dieser Aufgabe jedenfalls zum Teil offensichtlich überfordert sind. Denn mehr als andere Behörden, Stellen und Betriebe verfügen gerade die Datenschutzbeauftragten aufgrund ihrer Aufgabenstellung und der täglichen Befassung mit dem Internet und seinen Angeboten über den Fachverstand und das Fachwissen, das sie befähigt, die sich in zeitlicher Hinsicht zum Teil überschlagenen digitalen Entwicklungen und Angebote richtig einzuordnen, zu bewerten und daraus die notwendigen Rückschlüsse und Ratschläge abzuleiten. Dieses Wissen und das damit einhergehende Problembewusstsein ist in diesem Umfange und in dieser Tiefe bei den Schulen, den Hochschulen oder den Volkshochschulen nicht vorhanden.

Deshalb hatte die Kultusministerkonferenz recht, als sie die Schulen vor drei Jahren in ihrem Beschluss über die digitale Medienbildung aufforderte, externen Sachverstand in den Unterricht zu holen. Rheinland-Pfalz ist in der glücklichen Lage, dass dies nicht nur von allen Fraktionen des Landtags so gesehen wird, sondern dass diese daraus auch die notwendigen haushaltsrechtlichen Konsequenzen gezogen haben und immer noch ziehen. Damit wird der Datenschutzbeauftragte in Rheinland-Pfalz in die Lage versetzt, den Datenschutz aktiv als Bildungsaufgabe wahrzunehmen.

Natürlich ist der LfDI keine Bildungseinrichtung, aber er ist in der Lage, die Schulen, Hochschulen, und Volkshochschulen, soweit es um digitale Frage-

stellungen geht, bei der Wahrnehmung ihrer Bildungsaufgabe substanziell zu unterstützen.

2.2. Medienkompetenz und Datenschutzkompetenz

Die Diskussion über die Förderung der Medienkompetenz von jungen Menschen wird seit vielen Jahren geführt, Dementsprechend ist auch manches auf diesem Gebiet erreicht worden. Einschlägige Untersuchungen belegen aber auch die Defizite, die es bereits in der Vorinternetzeit gegeben hat und die bis heute fortbestehen. Durch die allseitige Inanspruchnahme des Internet sind diese Defizite nicht kleiner geworden. Im Gegenteil.

Umso mehr ist es zu begrüßen, dass die Landesregierung mit dem Landesprogramm „Medienkompetenz macht Schule“ frühzeitig versucht hat, sowohl im schulischen wie im außerschulischen Bereich, Kinder und Jugendliche, aber auch die älteren Generationen in digitalen Fragen fitzumachen und zu ertüchtigen. Der Landtag hat dies in seiner Entschließung „Medienkompetenz macht Schule“ Ende der vergangenen Jahres zurecht gewürdigt.

Wie umfassend und vielfältig die entsprechenden Bemühungen in Rheinland-Pfalz waren und immer noch sind, lässt sich vor allem aus der Antwort der Landesregierung auf die Große Anfrage sämtlicher im Landtag vertretenen Fraktionen über die „Maßnahmen zur Förderung der Medienkompetenz“ entnehmen. Diese Antwort stellt eine Bestandsaufnahme aller rheinland-pfälzischen Maßnahmen auf dem Gebiet der Medienkompetenz dar. Sie ist auch für andere Bundesländer beispielgebend und auch unter Datenschutzgesichtspunkten richtungsweisend. Denn sie bestätigt mehrfach, dass Datenschutzkompetenz wesentlicher Teil von Medienkompetenz ist. Aufgrund der digitalen Entwicklung unserer Gesellschaft gilt dies heute mehr denn je. Deshalb ist Medienkompetenz mittlerweile in erster Linie digitale Medienkompetenz, sodass Datenschutzfragen in diesem Zusammenhang einen immer breiteren Raum einnehmen.

Vor diesem Hintergrund empfiehlt es sich, die Antwort der Landesregierung unter verschiedenen Gesichtspunkten noch einmal zu thematisieren, ggf. auch im parlamentarischen Raum, da diese Antwort bisher weder im Plenum noch im zuständigen Ausschuss behandelt worden ist. Dabei sollten sowohl inhaltliche wie organisatorische Aspekte näher beleuchtet werden.

Die Regierungsantwort beschränkt sich – wie bereits gesagt – auf eine – durchaus beeindruckende – Bestandsaufnahme der rheinland-pfälzischen Medienkompetenzmaßnahmen. Es sollte allerdings auch sichergestellt werden, dass diese Maßnahmen die richtigen Themenstellungen behandeln.

So sind – um dies an einem Beispiel festzumachen – Jugendliche, vor allem aber auch Kinder, im Netz zunehmend versteckter und kaschierter Werbung ausgesetzt, der sie – selbst wenn sie offen erfolgte – kaum noch auszuweichen imstande sind, was mit gewichtigen Gefahren verbunden ist, da die entsprechenden Werbemaßnahmen zunehmend personalisiert erfolgen, also auf die konkrete Lebenssituation der Kinder abgestimmt sind. Allerdings ist offenbar nicht gewährleistet, dass diese besonderen Risiken und Gefahren auch im Rahmen der diversen Medienkompetenzmaßnahmen gebührend behandelt werden.

Wie gesagt: Dies ist nur ein Beispiel, das deutlich machen soll, dass es nicht nur auf eine breite Maßnahmenpalette ankommt, sondern vor allem auf die richtige Themenwahl und die richtigen Unterrichtsinhalte. Hinzu kommt, dass die Bestandsaufnahme der rheinland-pfälzischen Medienkompetenzmaßnahmen nicht erkennen lässt, dass diese untereinander abgestimmt und koordiniert sind. Angesichts der angedeuteten inhaltlichen Fragestellungen und der immer knapper werdenden Haushaltsmittel erscheint aber genau dies erforderlich. Es ist sicherzustellen, dass die richtigen Prioritäten gesetzt werden, dass die Maßnahmen sich ergänzen und dass die jeweils aktuellen Entwicklungen aufgegriffen werden. Dies setzt organisatorische Rahmenbedingungen und Strukturen voraus, die hinreichende Koordinierung und inhaltliche Priorisierung sicherstellen. Die Antwort der Landesregierung auf die Große Anfrage zur Medienkompetenz geht darauf nicht näher ein. Das ist bedauerlich und sollte nachgeholt werden.

2.3 Schulfach „Internet“

Wie in anderen Bundesländern wird auch in Rheinland-Pfalz bisher digitale Medienbildung als Querschnittsthema verstanden und deshalb nicht einem besonderen Schulfach zugeordnet. Trotz aller Bemühungen ist es der Landesregierung bisher aber nicht gelungen, die Folgen der umfassenden Digitalisierung unseres Lebens im schulischen Unterricht auf diesem Weg nachhaltig und im notwendigen Umfange zu behandeln. Allerdings ist dies in anderen Bundesländern nicht anders.

Auch die Richtlinie Verbraucherbildung (vgl. Tz. II-2.5) und die Einführung des MedienkomP@sses (vgl. Tz. II-2.6) haben dies bisher nicht vermocht, schon gar nicht in flächendeckender Weise. Es stellt sich deshalb die Frage, ob das Bildungskonzept, soweit es um digitale Fragestellungen geht, nicht überarbeitet werden sollte. Der Beschluss der Kultusministerkonferenz „Medienbildung in der Schule“ vom 8. März 2013 enthält unter Ziffer 3.1 hierzu folgende Feststellung:

> „Medienbildung als Lernen mit Medien und Lernen über Medien ist in den Lehr- und Bildungsplänen der Länder zwar durchgängig ausgewiesen, allerdings unterscheiden sich Art, Umfang und Ausführlichkeit der Angaben deutlich. Wünschenswert wären die Aktualisierung und Akzentuierung der Medienbildung in den einzelnen Fächern und die Formulierung eigener fächerübergreifender Kriterien zur Medienbildung. Bereits vorliegende kompetenzorientierte Konzepte zur schulischen Medienbildung können dazu zusätzlich hilfreiche Orientierung bieten. Die dort formulierten Kriterien sollten auf Landesebene in den Fächern und Lernbereichen der Lehr- und Bildungspläne konkret verankert und auf der Ebene der einzelnen Schule in Form eines Medienbildungskonzeptes oder Medienbildungsplans konkretisiert werden.“

Ob diese Vorgaben in Rheinland-Pfalz hinreichend realisiert worden sind, sei dahingestellt. Mehr denn je stellt sich stattdessen die Frage, ob den grundlegenden Herausforderungen unserer digitalen Zeit, die mit revolutionären technologischen Veränderungen einhergehen, die wiederum alle Lebensbereiche und jeden Einzelnen erfassen, mit dem bisherigen Bildungskonzept noch hinreichend begegnet werden kann.

Die Schulen haben den gesetzlichen Auftrag, ihre Schülerinnen und Schüler zu einem selbstbestimmten und selbstverantwortlichen Leben zu erziehen. Da die digitale Technologie die Möglichkeiten zur Selbstbestimmung und Selbstverantwortung zunehmend untergräbt, muss gerade in den Schulen mehr unternommen werden, um die Schülerinnen und Schüler auf diesen Prozess vorzubereiten.

Dies gilt vor allem auch deshalb, weil es dem Gesetzgeber immer schwerer fällt, für diese globale technologische Entwicklung die notwendigen rechtlichen Rahmenbedingungen zu schaffen.

Mehr denn je sind die Menschen deshalb darauf angewiesen, sich selbst helfen zu können. Angesichts der Komplexität der digitalen Technologie und der großen Intransparenz vieler digitaler – vor allem netzbasierter – Angebote, bedarf es dazu besonderer Fähigkeiten und Kenntnisse. Dabei genügt es nicht, sich auf die Vermittlung allgemeiner und grundlegender Informationen zu beschränken. Die Schülerinnen und Schüler benötigen konkretes Wissen und das heißt vor allem, dass sie über die jeweils aktuellen Entwicklungen unterrichtet sein müssen. Das kann nicht „nebenbei“ geleistet werden. Das ist aufwändig, und zwar in zeitlicher und inhaltlicher Hinsicht.

Hinzu kommt, dass die digitale Entwicklung in atemberaubender Geschwindigkeit voranschreitet und unser staatliches und gesellschaftliches Leben ebenso rasant umgestaltet. Das geschieht in einem bisher nicht bekannten Tempo und so schnell, dass wir heutzutage kaum noch die Zeit dazu haben, die Gesellschaft darauf vorzubereiten, so wie die Gesellschaft kaum noch die Zeit findet, über diese Entwicklung und die damit verbundenen Probleme nachzudenken. Will man diese speziellen Herausforderungen überhaupt noch Herr werden, müssen die notwendigen Grundlagen bereits in der Schule gelegt werden, und zwar auf nachhaltige Art und Weise. Freiwillige Angebote, die weder prüfungs- noch notenrelevant und lehrplanmäßig nur sehr vage ausgestaltet sind, genügen in keiner Weise, vor allem dann nicht, wenn sie nicht mit einer klaren Fächerzuteilung verbunden sind.

Jedenfalls sind die digitalen Herausforderungen so groß, dass die Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestags für die Bundesregierung ein Internetministerium und für das Parlament einen Internetausschuss gefordert hat. Die Landesregierung hat aus denselben Gründen einen Landesrat für digitale Entwicklung und Kultur eingerichtet. Auch die Parteien rüsten sich mit netzpolitischen Arbeitskreisen und netzpolitischen Kongressen für die digitale Zukunft. Das ist alles sinnvoll und richtig.

Notwendig ist es dann aber auch, dass man die Bürgerinnen und Bürger, vor allem die junge Generation, fit für das Netz und die digitale Welt macht. Dafür genügen keine Medienführerscheine und auch kein Medienkompass. Sie sind – wie die „Frankfurter Allgemeine Zeitung“ in ihrem Leitartikel vom 20. April 2013 zu Recht schrieb „nur ein Tropfen auf den heißen Stein“. Notwendig ist es vielmehr, endlich über ein Schulfach „Internet“ nachzudenken. Das würde auch dem Umstand Rechnung tragen, dass digitale Medienkompetenz von allen Fachleuten nach dem Lesen, dem Schreiben und dem Rechnen als vierte Kulturtechnik bezeichnet wird. Daraus müssen die notwendigen bildungspolitischen Konsequenzen gezogen werden.

Notwendig ist dies nicht nur, um sich gegenüber Facebook und Google, Apple und Microsoft zu behaupten, digitale Medienkompetenz ist vielmehr auch Voraussetzung dafür, dass die Internetangebote, die der Staat im Allgemeinen und das Land im Besonderen im Rahmen von E-Government und Open Data-Strategien seinen Bürgerinnen und Bürgern macht, von diesen auch genutzt werden. Von diesen Angeboten werden aber nur diejenigen Gebrauch machen, die sich souverän im Netz bewegen und sich dort sicher fühlen.

Ohne eine nachhaltige digitale Aufklärung wird dies nicht zu erreichen sein. Ein eigenes Schulfach ist dafür ein Schritt in die richtige Richtung. Entsprechende bildungspolitische Leitentscheidungen, die Überarbeitung der Lehrpläne und eine adäquate Ausbildung der Lehrerinnen und Lehrer müssen damit einhergehen.

2.4 KMK-Beschluss „Verbraucherbildung an Schulen“

Dieser Beschluss stammt vom 12. September 2013 und listet eine Reihe einschlägiger Themen und Handlungsfelder auf, die letztlich vor allem auf Finanz-, Ernährungs- und Medienkompetenz hinauslaufen. Diese Handlungsfelder sollen unter dem Stichwort „Verbraucherbildung“ intensiv im schulischen Unterricht behandelt werden.

So begrüßenswert dieser Beschluss vor allem auch im Kontext mit dem KMK-Beschluss „Medienbildung in der Schule“ vom 8. Februar 2012 ist, so fragwürdige sind seine Ausführungen zum Themenfeld „Medien und Information“. Es wird nicht klar, welcher Mehrwert damit verbunden sein soll, wenn angesichts einer umfassenden Digitalisierung unserer Gesellschaft der maßgebliche KMK-Beschluss sich auf die Feststellung beschränkt:

- Informationsbeschaffung und -bewertung
- Datenschutz und Urheberrecht
- Mediennutzung

seien im Unterricht vertiefend zu behandeln.

Man fragt sich, was die Schulen zum Thema „Datenschutz“ vermitteln sollen, findet dazu aber in dem sechsseitigen Beschluss keinen einzigen Hinweis. Tatsächlich wird dieses Thema an keiner anderen Stelle auch nur angedeutet. Selbst bei den externen Institutionen, die für eine Unterstützung der Schulen in diesem Zusammenhang vorgeschlagen werden, finden sich zwar die Verbraucherzentralen, aber nicht die Datenschutzbeauftragten. Dass in unserer digitalen Zeit Verbraucherschutz ganz wesentlich Verbraucherdatenschutz ist, ist offenbar noch nicht bei der KMK angekommen.

2.5 Richtlinie Verbraucherbildung

Im Jahre 2010 hatte das Bildungsministerium eine Richtlinie über Verbraucherbildung in Schulen erlassen und in diesem Zusammenhang auch den Datenschutz als Kernkompetenz ausgewiesen. In der Richtlinie ist die Rede davon, dass keine Zuordnung der Kernkompetenzen zu einzelnen Fächern erfolge; dies bleibe den Rahmen(lehr)-

plänen der jeweiligen Fächer sowie den schuleignen Arbeitsplänen vorbehalten.

Auf Nachfrage des LfDI erklärte das Bildungsministerium, dass in den Lehrplänen der Sekundarstufe I für die Bereiche „Erdkunde, Geschichte, Sozialkunde“ sowie „Gesellschaftslehre“ der Datenschutz stärker als bisher verankert worden sei. Durch das in der Realschule plus gültige Unterrichtsprinzip „Informatorische Bildung“ spiele der Kernbereich Datenschutz in dieser Schulform bereits jetzt eine vertiefte Rolle.

Bei dem ergänzenden Modellprojekt „Verbraucherbildung an allgemeinbildenden Schulen“ handelt es sich nach Auskunft des Bildungsministeriums um ein Gemeinschaftsprojekt des Ministeriums für Bildung, Wissenschaft, Weiterbildung und Kultur, des Ministeriums der Justiz und für Verbraucherschutz und des Ministeriums für Umwelt, Landwirtschaft, Ernährung, Weinbau und Forsten, in dem modellhaft erprobt wird, inwieweit sich die Richtlinie Verbraucherbildung an unterschiedlichen Schulen verschiedener Schularten in schuleigene Arbeitspläne umsetzen lässt. Wesentlicher Baustein dieses Projekts soll eine zwölfmonatige Qualifizierung von Lehrkräften zu allen Kernbereichen der Verbraucherbildung sein, die von der Universität Koblenz-Landau als Online-Schulung mit Präsenzphasen über die Plattform „Moodle“ durchgeführt werde.

Der LfDI hat seine Unterstützung bei der Weiterbildung der Lehrkräfte im Rahmen des Modellprojektes zugesagt. Dementsprechend werden die Koordinatorinnen des Projekts zum Themenbereich „Kryptografie“ fortgebildet.

All diese Bemühungen dürfen jedoch über eines nicht hinwegtäuschen. Auch drei Jahre nach Inkrafttreten der Richtlinie befindet man sich noch immer in einer Erprobungsphase. Von einer flächendeckenden Vermittlung von Datenschutzinhalten als Teil der Verbraucherbildung kann nach wie vor keine Rede sein.

Hinzu kommt, dass die Qualifizierung der Lehrkräfte auf freiwilliger Basis erfolgt und angesichts der ansonsten bestehenden Belastungen im Schulalltag nur spärlich nachgefragt wird. Bislang konnten daher nur knapp 40 Lehrkräfte im Sinne der Richtlinie qualifiziert werden, was angesichts von ca. 40.000 Lehrkräften im Land noch nicht einmal als ein „Tropfen auf den heißen Stein“ angesehen werden kann.

Will man der Richtlinie Verbraucherbildung zum Durchbruch verhelfen, dann kommt man nicht umhin, den Bereich der digitalen Datenschutz- und Medienbildung auch als verpflichtenden Bestandteil der Lehrerausbildung und der Lehrerfortbildung vorzusehen.

2.6 MedienkomP@ss

Im Berichtszeitraum wurde seitens der Landesregierung die Einführung des sog. MedienkomP@sses vorangetrieben. Bei dem MedienkomP@ss handelt es sich um einen Kompetenznachweis für die Schülerinnen und Schüler, in dem sie ihre über die Schuljahre gesammelten Medienerfahrungen dokumentieren. 2013 wurde der MedienkomP@ss an 17 Pilotschulen der Primarstufe modellhaft erprobt. Es ist geplant, dass ab dem Schuljahr 2014/2015 grundsätzlich alle Schülerinnen und Schüler der Klassenstufen eins bis sechs den MedienkomP@ss erwerben können. Es handelt es also um ein – nicht verpflichtendes Angebot.

Als Basis dient dabei ein Medienkonzept für Lehrkräfte, dessen Kompetenzraster die Grundlage für die Unterrichtsplanung ist. Es zeigt auf, welche Kompetenzen erworben werden und welche konkreten Möglichkeiten zur Umsetzung es gibt. Auf der Medienplattform des OMEGA-Servers werden dazu passende Unterrichtsbeispiele für Lehrkräfte zur Verfügung gestellt.

Der LfDI hat das Projekt seit dessen Start kontinuierlich begleitet und unterstützt: Den Pilotschulen wurden Schülerworkshops des LfDI vorrangig zugeteilt und von den pädagogischen Fachkräften des LfDI wurden praktische Methoden der Vermittlung von Datenschutzthemen für den Regelunterricht in der Grundschule entwickelt. Die Konzepte stehen nunmehr in digitaler Form auf dem OMEGA-Server des Pädagogischen Landesinstituts zum Download bereit.

Der MedienkomP@ass wird aus Datenschutzsicht begrüßt. Allerdings kommt er verspätet. Die Enquete-Kommission „Verantwortung in der medialen Welt“ hatte seine Einführung bereits im Jahre 2011 empfohlen. Er kommt auch allzu zögerlich und ohne den nötigen Nachdruck. Dafür mag es nachvollziehbare Haushaltsgründe geben. Doch ändern diese nichts an den daraus resultierenden konzeptionellen Defiziten.

2.7 Schülerworkshops

Aufgrund der großen Nachfrage wurden die seit September 2010 an rheinland-pfälzischen Schulen angebotenen Schülerworkshops „Datenschutz und Datenverantwortung“ auch im Berichtszeitraum fortgesetzt. Die Resonanz bei Schülerinnen und Schülern bei Lehrkräften und der Schulleitung war durchweg positiv, meist wurden unmittelbar nach Ende der Workshops Folgetermine vereinbart.

Im Zeitraum 2010/2011 waren 282 Workshops durchgeführt worden. Mit 946 Workshops im Berichtszeitraum 2012/2013 hat sich die Zahl mehr als verdreifacht. Die Durchführung der Schülerworkshops ist für die Schulen nach wie vor kostenlos; die Finanzierung wurde vor allem durch Unterstützung des Ministeriums für Justiz und Verbraucherschutz, des Ministeriums für Bildung, Wissenschaft und Kultur sowie des Ministeriums der Finanzen sichergestellt.

Insgesamt wurden für das Kalenderjahr 2012 76.900 und für 2013 124.852 Euro verausgabt. Mit diesen Mitteln hat der LfDI im Berichtszeitraum jetzt knapp 1.000 Workshops durchgeführt und auf diese Weise rund 30.000 Schülerinnen und Schüler für den Umgang mit persönlichen Daten im Internet sensibilisiert.

Die Workshops werden von externen Referentinnen und Referenten nach einer eingehenden Schulung durch den LfDI und unter seiner Aufsicht und Anleitung durchgeführt. Waren 2012 noch 20 Honorarkräfte im Einsatz, so hat sich die Zahl mittlerweile auf 30 erhöht. Durch regelmäßige Treffen und die Nutzung eines gemeinsamen Internetforums im Internetangebot des LfDI ist ein gegenseitiger Austausch sichergestellt.

Als aufgrund der Rückmeldungen der Referentinnen und Referenten deutlich wurde, dass ältere Schülerinnen und Schüler an der Thematik Smartphones und Apps besonders interessiert sind, bildete der LfDI die Honorarkräfte in einem gesonderten Seminar entsprechend fort und stellte ihnen die notwendigen Arbeitsmaterialien zur Verfügung. Nach dem NSA-Skandal fand eigens für die Honorarkräfte eine Crypto-Session statt, um diese auch in Fragen der Verschlüsselung von E-Mails und Dateien fortzubilden.

Da nach den Erfahrungen der Referentinnen und Referenten bereits beim Wechsel auf weiterführende Schulen Mobiltelefone und damit auch Datenschutzfragen bei der Nutzung von „Facebook“ und „WhatsApp“ aktuell werden, wurden unter präventiven Gesichtspunkten auch die vierten Klassen der Grundschulen in das Workshopkonzept mit einbezogen. Hierfür entwickelten pädagogische Fachkräfte von „medien+bildung.com“, die zum LfDI abgeordnet sind, ein eigenes didaktisches Konzept. Auch für Justizvollzugsanstalten wurden spezifische Workshops entwickelt und zielgruppengerichtet durchgeführt.

Der LfDI versteht sich dabei stets als Kooperationspartner des Landesprogramms „Medienkompetenz macht Schule“. Als im Juni des vergangenen Jahres der 1.000. Schülerworkshop zugeteilt werden konnte, besuchten Staatssekretärin Beate Reich vom Ministerium der Justiz und für Verbraucherschutz und Bildungsstaatssekretär Hans Beckmann gemeinsam mit dem LfDI diesen „Jubiläumsworkshop“ in Sinzig. Als besondere Anerkennung empfand der LfDI den Besuch eines Schülerworkshops durch Ministerpräsidentin Malu Dreyer im Februar 2014.

Es steht außer Frage, dass der LfDI mit diesen Workshops dazu beiträgt, die jungen Menschen zu sensibilisieren und nachdenklicher zu machen, und sie darin unterstützt da und dort auch umzudenken und digitale Fragen neu zu bewerten. Laut JIM-Studie 2012 war die Behandlung von Medienthemen im Unterricht immerhin für 28 Prozent der Schülerinnen und Schüler Anlass für eine Verhaltensänderung. Die Workshops haben sicherlich ihren Teil dazu beigetragen.

Gleichwohl ist die Nachhaltigkeit dieser Workshops notwendigerweise begrenzt, denn nur ausnahmsweise kommen Schülerinnen und Schüler in den Genuss eines zweiten oder gar eines dritten Workshops. In aller Regel bleibt es bei einem Datenschutzworkshop und nicht selten war das dann auch schon alles, was den Schülerinnen und Schülern in ihren Schulen an datenschutzrelevantem Wissen und datenschutztechnischen Fähigkeiten und Fertigkeiten vermittelt wird.

Gleichwohl ist der LfDI außerordentlich dankbar dafür, dass seine Behörde – mit den Stimmen der regierungstragenden Fraktionen – die notwendigen Haushaltsmittel zur Verfügung gestellt wurden, um das Schülerworkshopprojekt auch in den beiden kommenden Jahren weiterzuführen. In Kooperation mit dem erziehungswissenschaftlichen Zweig der Johannes Gutenberg-Universität Mainz wird dabei im Rahmen einer Masterarbeit eine wissenschaftliche Begleitung sichergestellt werden.

2.8 Medienscouts und Juniorbeirat

Im Rahmen des Landesprogramms „Medienkompetenz macht Schule“ engagierte sich der LfDI auch weiterhin bei der Aus- und Weiterbildung der schulischen Medienscouts im Land.

Hierzu fanden im Rahmen des „Safer Internet Day“ 2012 und 2013 Schulungen und Workshops für Medienscouts und begleitende Lehrkräfte durch Mitarbeiterinnen und Mitarbeiter des LfDI statt. Referiert wurde über datenschutzkonformes Verhalten in sozialen Netzwerken und technische Möglichkeiten der Browsersicherheit. Darüber hinaus gaben die pädagogischen Fachkräfte des LfDI konzeptionelle Anregungen zur Implementierung von Datenschutzthemen in die Medienkompetenzförderung der Schülerinnen und Schüler.

Auch der Juniorbeirat tagte im Berichtszeitraum wiederholt. Wie bereits im Datenschutzbericht 2010/2011 (vgl. 23. Tb., Tz. I-4.10) erläutert, setzt sich der Juniorbeirat aus interessierten Schülerinnen und Schülern vorrangig aus dem Mainzer Umland zusammen, die an ihren Schulen als Medienscouts aktiv sind. Die Mitarbeiterinnen und Mitarbeiter des LfDI beantworten in den Sitzungen rechtliche, technische und pädagogische Fragen, die den Medienscouts bei ihrer Tätigkeit begegnet sind. Auf Wunsch erfolgen zu ausgewählten Themen auch spezielle Schulungen. So wurden die Medienscouts hinsichtlich Smartphones, Apps, Cookies und Browsersicherheit fortgebildet. Alle Mitglieder des Juniorbeirates erhalten über das Internetangebot des LfDI Zugang zu einem eigenen Internetforum, in dem sie in einer geschlossenen Benutzergruppe Fragen stellen, Informationen aufnehmen und sich untereinander austauschen können.

Auch der LfDI profitiert von den Sitzungen des Juniorbeirats: Viele der hier diskutierten Themen sind bei der Gestaltung der neuen Jugendhomepage „www.youngdata.de“ mit eingeflossen (vgl. Tz. II-3.1). Vom LfDI erstellte Informationsmaterialen wurden im Juniorbeirat „vorgeprüft“. Auf diese Art und Weise wurde die Öffentlichkeitsarbeit des LfDI – soweit sie die Zielgruppe Jugendliche betrifft – durch die „Expertinnen und Experten“ des Juniorbeirats evaluiert.

2.9 Veranstaltungen

Wie in Jahren 2010 und 2011 hat der LfDI auch im Berichtszeitraum wieder in einer Reihe von Veranstaltungen dafür geworben, den Datenschutz auch als Bildungsaufgabe zu verstehen und dabei im Einzelnen dargelegt, welche Bildungsinhalte damit verbunden sein müssen. Im Rahmen einer vom Landesdatenschutzbeauftragten Mecklenburg-Vorpommerns im Jahre 2012 durchgeführten Fachtagung „Datenschutz – Fortschrittsbremse oder Bildungschance“ konnte der LfDI zum Thema „Datenschutz und Bildung“ referieren. Ein entsprechender Vortrag war außerdem Teil eines Fachkongresses des IT-Planungsrats im Jahre 2013. Dieses Thema wurde im Übrigen auch immer wieder im Rahmen von Schulveranstaltungen aufgegriffen, etwas bei einer gemeinsam mit dem Vorstandsvorsitzenden der Schufa, Dr. Michael Freytag, durchgeführten Veranstaltung in der Mainzer Maria Ward-Schule. Mit 120 Abiturientinnen wurde intensiv über „intelligenten Verbraucherdatenschutz“ diskutiert.

2.10 Arbeitskreis Datenschutz und Bildung

Um Fragen der digitalen Medien- und Internetkompetenz länderübergreifend und unter Einbeziehung der Bundesebene behandeln und die jeweiligen Erfahrungen austauschen zu können, hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länger bereits vor Jahren einen Arbeitskreis „Datenschutz und Bildung“ eingerichtet und dem LfDI den Vorsitz übertragen.

Dieser Arbeitskreis tagte im Berichtszeitraum insgesamt viermal. Unter dem Vorsitz des LfDI konnte die Vernetzung untereinander und mit externen Partnerinnen und Partnern weiter verbessert werden. Hervorzuheben sind Vorträge von MdB Tabea Rößner als Mitglied der Enquete-Kommission des Deutschen Bundestages „Internet und digitale Gesellschaft“, von Prof. Dr. Birgit Stark, Johannes Gutenberg-Universität Mainz, zur „Googleisierung der Informationssuche“ und von Prof. Dr. Horst Niesyto von der Pädagogischen Hochschule Ludwigsburg zur Thematik „Pflichtfach Medienkompetenz“.

2.11 Fortbildungsmaßnahmen

Auch bei der **Lehrerfortbildung** war die Mitarbeiterinnen und Mitarbeiter des LfDI wieder aktiv. So wurden für das Pädagogische Landesinstitut Schulleitungen, Jugendmedienschutzberaterinnen und -berater und sonstige interessierte Lehrkräfte – je nach Bedarf – in rechtlicher, technischer und pädagogischer Hinsicht in Datenschutzfragen geschult. Weitere Fortbildungen wurden im Rahmen des „Safer Internet Day“ und anlässlich der „iMedia“ durchgeführt.

Der LfDI führt bereits seit vielen Jahren über kommunale Bildungsträger Fortbildungen für **behördliche Datenschutzbeauftragte** durch. Hinzu kamen im Berichtszeitraum Inhouseschulungen bei der Finanz-, Sozial- und Vermessungsverwaltung und beim Landesbetrieb Liegenschafts- und Baubetreuung.

Im Rahmen der Medienkompetenzförderung hat der LfDI für das Pädagogische Landesinstitut schulische Medienkoordinatorinnen und -koordinatoren über die Datenschutzaspekte bei Smartphones und Apps informiert.

Fortbildung fand aber nicht nur im schulischen Bereich statt.

In Kooperation mit dem Justizministerium und der Rechtsanwaltskammer Koblenz sowie der Pfälzischen Rechtsanwaltskammer in Zweibrücken wurden Fortbildungsveranstaltungen für **alle Bereiche der Justiz** angeboten und durchgeführt. In fast 20 Seminaren wurden, abgestimmt auf die jeweiligen Aufgaben- und Tätigkeitsbereiche, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte, Geschäftsstellenbedienstete, Referendarinnen und Referendare sowie Rechtsanwältinnen und Rechtsanwälte in Angelegenheiten des rechtlichen und technischen Datenschutz fortgebildet. Daneben erfolgten mehrere Workshops zu datenschutzrechtlichen Fragestellungen in überregionalem Rahmen bei der Deutschen Richterakademie. Für den kommenden Berichtszeitraum liegen bereits weitere Anfragen zur Fortführung dieser Aktivitäten vor. Schließlich war der LfDI maßgeblich an der Durchführung eines mehrtägigen Seminars für Richterinnen und Richter aus dem ganzen Bundesgebiet an der Deutschen Richterakademie in Trier beteiligt.

Im Rahmen der Twinning- und TAIEX-Programme der Europäischen Union haben zwei Mitarbeiter des LfDI als Short-Time-Experts in Mazedonien und in Montenegro die dortigen Datenschutzinstitutionen beraten. Teil dieser Programme war auch die Information der albanischen Datenschutzbeauftragten über die Rolle der behördlichen und betrieblichen Datenschutzbeauftragten.

3. Webseiten und Apps

Information und Beratung, Bildung und Erziehung erfolgten nicht nur auf althergebrachte Weise, sondern auch in digitaler Form, nämlich im Internet und dort in einigen – auch neuen – Webseiten, die allgemeine Datenschutzfragen ebenso behandeln wie bereichsspezifische und an ältere Generationen ebenso adressiert sind, wie an Jugendliche.

3.1 Young Data

Der LfDI hat sein Internetangebot im November 2013 um eine spezielle Jugendhomepage für den Datenschutz ergänzt. Sie enthält Informationen zum Selbstdatenschutz bei der Nutzung von Facebook, WhatsApp, Youtube, Spielkonsolen, Smartphones und anderen Anwendungen, klärt über die Gefahren von Cybermobbing auf und bietet Hintergrundinformationen zum Datenschutz im Allgemeinen. Folgende Überlegungen waren für den Aufbau dieser Seite maßgeblich:

Nach einer Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet gehen zwei Drittel der führenden Repräsentantinnen und Repräsentanten aus Politik, Wirtschaft, Medien, Zivilgesellschaft sowie Wissenschaft und Forschung davon aus, dass die Sicherheit der Internetnutzerinnen und -nutzer in erster Linie von ihrer Medienkompetenz abhängt. 93 Prozent der Befragten meinen dann aber auch, dass zu allererst jede Bürgerin bzw. jeder Bürger selbst dafür zu sorgen habe, sich verantwortungsvoll und souverän im Netz bewegen zu können. Erst dann folgen die Bildungsangebote in den Schulen mit 81 Prozent, der Berufsschulen und Hochschulen mit 74 Prozent und der Wirtschaftsunternehmen mit 66 Prozent.

Die Eltern tauchen in dieser Rangliste erst gar nicht mehr auf, was deutlich macht, dass sie mit der Bewältigung der digitalen Herausforderung vielfach selbst überfordert und deshalb häufig weit von der Rolle als digitales Vorbild entfernt sind.

Je weniger aber Eltern, Schulen, Hochschulen, Volkshochschulen und Wirtschaftsunternehmen ihrer digitalen Bildungsaufgabe im notwendigen Umfange nachkommen, desto mehr ist jede oder jeder Einzelne tatsächlich selbst für den Auf- und Ausbau ihrer bzw. seiner digitalen Souveränität zuständig. Angesichts der großen Herausforderungen und Risiken, die mit dem Netz und seinen vielfältigen Angeboten verbunden sind, ist dies zwar völlig unangemessen, aber es ist in gewisser Weise trotzdem Realität.

Wer sich im Netz bewegt, muss sich also die digitalen Regeln selbst aneignen, muss selbst ein Gespür für die Risiken und Gefahren entwickeln, muss sich selbst weiterhelfen können. Selbstdatenschutz ist deshalb der Schlüssel zur Datensicherheit und zum Datenschutz. In Zeiten, in denen weder der nationale Gesetzgeber noch die Europäische Union noch die Weltgemeinschaft in der Lage ist, die Bürgerinnen und Bürger durch eine digitale Rechtsordnung hinreichend zu schützen, führt an Selbstdatenschutz kein Weg vorbei.

Vor diesem Hintergrund muss und soll unsere neue Webseite „www.youngdata.de“ in erster Linie gesehen und verstanden werden. Sie ist ein Informationsangebot für alle, die sich etwas Orientierung im Netz wünschen, die nach Ratschlägen suchen, die sie nicht in ihrer Schule, nicht ihrem Betrieb und auch nicht von ihren Freundinnen und Freunden erhalten. Auch wenn natürlich auch die sog. „Silver Surfer“ eingeladen sind, die Seite zu besuchen, richtet sie sich doch in erster Linie an Jugendliche.

Dem entsprechend ist sie auch jugendgerecht gestaltet. Sie ist mit zahlreichen Cartoons, Videos und Fotos angereichert. Sie verfügt über 15 Hauptmenüpunkte, 60 Unterpunkte, elf eigens kreierte Cartoons, mehr als 100 Fotos und Grafiken, über 60 Videos, mehr als 200 weiterführende Links und Dutzende von Datenschutztipps. Selbstverständlich bedient sie sich auch einer jugendgerechten Sprache.

Sie bietet allen Interessierten etwas: den eilig Suchenden die schnelle Information und den wissbegierigen Onlinerinnen und Onlinern den digitalen Rundumblick. So gesehen verstehen wir „www.youngdata.de“ immer als Hilfestellung für alle, die mit einem guten Gewissen und dem notwendigen Sachverstand im Netz unterwegs sein wollen.

Dass sich „www.youngdata.de“ dabei vor allem an Jugendliche wendet, hängt damit zusammen, dass sie wie keine andere Generation im Netz unterwegs sind und auch die mobilen Zugangsmöglichkeiten nutzen. 72 Prozent der 12- bis 19-Jährigen haben ein eigenes Smartphone, und drei Fünftel von ihnen gehen damit mehrmals in der Woche ins Netz oder nutzen den mobilen Zugang zu ihrer Community. Jugendliche sind aber zugleich auch anfälliger als andere Generationen für die Versprechungen des Netzes und gehen sorgloser mit den bequemen und einfachen Bedienungsmöglichkeiten um. Mit anderen Worten: Die Faszination für die generationsspezifischen Angebote verdrängen gerade bei ihnen häufig das gesunde Misstrauen.

Der digitale Schutzschirm, den „www.youngdata.de“ aufspannt, hat einen großen Durchmesser. Die Informationen reichen von allgemeinen Informationen über das Internet bis zu speziellen Tipps für den Umgang mit Facebook, Google, WhatsApp, den Konsolen und den Smartphones. Der Schwerpunkt liegt also eindeutig auf der privatwirtschaftlichen Seite und betont damit die Rolle der Nutzerinnen und Nutzer als Verbraucherinnen und Verbraucher, insbesondere im digitalen Umfeld. Selbstverständlich behandelt die Seite nicht nur die Frage, wie man mit den eigenen Daten umgehen sollte; auch der Umgang mit den Daten anderer wird unter dem Begriff „Cybermobbing“ thematisiert. Auch in Rheinland-Pfalz gibt es keine mobbingfreie Schule.

Aber es werden auch Informationen zum Datenschutz im staatlichen Bereich vermittelt und damit die Rolle der jungen Menschen als Staatsbürgerinnen und Staatsbürger thematisiert. Das betrifft ihr Umfeld in der Schule ebenso wie den Staatstrojaner, die Vorratsdatenspeicherung und die aktuellen Enthüllungen des früheren NSA-Mitarbeiters Edward Snowden.

Last but not least findet sich auf dieser Seite auch Wissenswertes zur Informationsfreiheit, zur Open Data-Bewegung und zu dem in Arbeit befindlichen rheinland-pfälzischen Transparenzgesetz. Wer testen will, ob sie oder er fit für die digitale Welt ist, bekommt dafür erste Anhaltspunkte bei dem einen oder anderen Datenschutzquiz.

„www.youngdata.de“ wurde am 20. November 2013 freigeschaltet. Die öffentliche Resonanz war groß und durchweg positiv. Das gilt für die Presseberichterstattung, für die Rückmeldungen aus den Schulen und auch für die Stellungnahmen von Einrichtungen, die sich besonders mit Datenschutzfragen befassen, wie etwa „klicksafe“, die als Medienpartner gewonnen werden konnte.

Auch die Zahl der Seitenbesuche ist durchaus positiv. Seit dem 20. November 2013 waren rund 35.000 Besuche auf „www.youngdata.de“ zu verzeichnen. Wurde die Verbindung vom Desktop hergestellt, dauerte der Besuch im Schnitt sieben Minuten, vom Smartphone aus vier Minuten, was auch damit zusammenhängt, dass die Seite für den mobilen Zugriff noch nicht optimiert wurde. Allerdings wird dieses Defizit im laufenden Jahr behoben werden.

„www.youngdata.de“ befindet sich derzeit in seiner ersten Entwicklungsstufe. Dazu gehört, dass wir mit diesem neuen Angebot natürlich auch unser Schülerworkshop-Projekt ergänzen wollen. Aus diesem Grund spielt „www.youngdata.de“ bei der Durchführung dieser Workshops eine große Rolle. Weitere Entwicklungsstufen sollen folgen. Wir werden die Seite, ihre Gestaltung und ihren Inhalt in den nächsten Wochen auch mit den Kolleginnen und Kollegen im Bund und in den Bundesländern diskutieren und nach Wegen suchen, wie sich auch die übrigen Datenschutzbeauftragten in dieses Projekt einbringen können. Ziel ist es, die Seite zu einer Webseite aller Datenschutzbeauftragten des Bundes und der Länder auszubauen, damit die Seite aktuell gehalten und die Werbung für diese Seite verbreitert werden kann.

Schließlich werden derzeit E-Learning-Szenarien für Lehrkräfte der Mittel- und Oberstufen entwickelt. Mit ihrer Hilfe sollen diese in die Lage versetzt werden, eigene Unterrichtseinheiten zum Datenschutz in ihren Schulen durchzuführen. Was ist das Ziel? Die Seite soll besucht und gelesen werden, und zwar von so vielen Menschen wie möglich. Wir wünschen uns also hohe „Klickzahlen“.

3.2 Apps für „www.youngdata.de“

Innerhalb des Berichtszeitraums wurden in Kooperation mit Herrn Prof. Dr. Bernhard Schiefer vom Fachbereich Informatik und Mikrosystemtechnik der FH Kaiserslautern (Standort Zweibrücken) insgesamt drei Master- und Bachelorarbeiten zum Thema Datenschutz angestoßen.

Im Rahmen der Masterarbeit „Entwicklung einer plattformunabhängigen mobilen App zur Sensibilisierung von Jugendlichen für Datenschutzprobleme“ entstand eine mobile App, die Informationen zum Thema Datenschutz bereithält sowie über ein Quiz verfügt. Ursprünglich war vorgesehen, dass sich die Nutzerinnen und Nutzer innerhalb der App mit den dort aufbereiteten Inhalten auseinandersetzen und ihr Wissen mit Hilfe des integrierten Quiz überprüfen können. Mit Blick auf die für Jugendliche entwickelte Internetseite „www.youngdata.de“ regte der LfDI an, das Quiz weiter auszubauen Künftig soll die Zielgruppe mit Hilfe des Quiz in die Lage versetzt werden, selbst ihr Wissen zu verschiedenen Datenschutzthemen zu prüfen. Das Ergebnis in Form einer plattformunabhängigen App soll im Laufe des Jahres 2014 im Rahmen der Schülerworkshops zum Einsatz kommen, um die Schülerinnen und Schüler auch außerhalb der eigentlichen Workshops zur Auseinandersetzung mit dem Thema Datenschutz zu bewegen.

Bei der Masterarbeit „Konzeption und Implementierung einer Applikation zur Analyse von potentiellen Datenschutzschwachstellen von Nutzeraccounts bei Facebook“ war die Ausgangsidee die Entwicklung einer Webseite bzw. einer App, welche die Facebook-Privatsphäreneinstellungen der Nutzenden analysiert und Hinweise zur Verbesserung gibt. Aufgrund verschiedener grundlegender Hürden bei der Umsetzung wurde die Applikation in Form einer Erweiterung für den Browser „Chrome“ realisiert. Ist diese installiert und die Person in Facebook eingeloggt, so werden die aktuellen Privatsphäreeinstellungen des Facebook-Zugangs ausgelesen. Hierzu werden keinerlei Zugangsdaten benötigt, da die laufende Facebook-Sitzung verwendet wird, um die entsprechenden Einstellungsseiten aufzurufen und auszuwerten. Die Ergebnisse der Auswertung werden übersichtlich in Form eines Tachos dargestellt. So wird den Nutzerinnen und Nutzern angezeigt, wo Defizite bestehen und Verbesserungen an den Einstellungen vorgenommen werden sollten. Es ist geplant, das Produkt künftig unter einer Open-Source-Lizenz zur Verfügung zu stellen.

Bei der Bachelorarbeit „Konzeption einer mobilen Applikation zur Unterstützung der Aufklärung im Bereich Datenschutz und Informationsfreiheit“ geht es um das grafisch aufbereitete Konzept eines Detektivspiels. Es ist storybasiert und dreht sich um das Verschwinden einer Schülerin. Durch das richtige Beantworten verschiedener Fragen zum Thema Datenschutz in sozialen Netzwerken (hier Facebook) haben die Spielerinnen und Spieler die Möglichkeit, einzelne Personen zu verhören. Hierdurch erhalten sie wichtige Tipps, die zur Täterin oder zum Täter führen. Für den LfDI war der spielerische Ansatz in Hinblick auf die jugendliche Zielgruppe von besonderem Interesse. An der praktischen Umsetzung des Konzeptes wird derzeit noch gearbeitet.

3.3 Neue Webseite zur IT-Sicherheit und zum Datenschutz in Arztpraxen

Wie schon in der Vergangenheit (vgl. 23. Tb., Tz. II-5.2.4) häuften sich auch in diesem Berichtszeitraum wieder die Eingaben und Anfragen im Bereich der niedergelassenen Ärzteschaft. Schwerpunkte waren Fragen zur Praxisorganisation einschließlich der Einbindung externer Dienstleister, die Ausgestaltung der Räumlichkeiten von Arztpraxen und der Umfang einer zu gewährenden Einsicht in die Behandlungsdokumentation. Nach den Erkenntnissen des LfDI bestehen bei der Ärzteschaft verbreitet Informationsdefizite über die Anforderungen an einen sicheren Einsatz von Informationstechnologie im Praxisbetrieb sowie die Auswirkungen der ärztlichen Schweigepflicht auf den Praxisalltag.

Der LfDI hat Anfang 2013 gegenüber der Kassenärztlichen Vereinigung Rheinland-Pfalz und der Landesärztekammer ein gemeinsames Vorgehen angeboten, um die IT-Sicherheit und den Datenschutz in den rheinland-pfälzischen Arztpraxen nachhaltig zu verbessern. Anders als die Kassenärztliche Vereinigung Rheinland-Pfalz nahm die Landesärztekammer jedoch trotz diverser konstruktiver Gespräche und einer großen inhaltlichen

Übereinstimmung in der Zielrichtung eines möglichen Vorhabens von einer formellen Zusammenarbeit Abstand. Dies ist aus Sicht des LfDI sehr zu bedauern.

Nach dem Ausscheiden der Landesärztekammer hielten der LfDI und die Kassenärztliche Vereinigung Rheinland-Pfalz gleichwohl an dem angestrebten Projekt fest. Auf der Grundlage eines gemeinsam entwickelten Konzepts wollen beide Partner im Rahmen der Initiative „Mit Sicherheit gut behandelt“ ab dem Jahresbeginn 2014 die Ärztinnen und Ärzte bei ihrer Verpflichtung, im Praxisbetrieb eine angemessene IT-Sicherheit und einen effektiven Datenschutz zu gewährleisten, umfassend unterstützen. Ziel ist es insbesondere, die Praxisinhaberinnen und -inhaber allgemein für die Thematik zu sensibilisieren und über bestehende rechtliche Vorgaben zu informieren. Darüber hinaus sollen Hilfestellungen gegeben werden, mögliche Handlungsdefizite in der eigenen Praxis zu erkennen und durch geeignete Lösungen zu beseitigen.

Kernstück der Initiative ist die Bereitstellung einer zentralen Webseite zum Thema IT-Sicherheit und Datenschutz in der Arztpraxis (http://www.mit-sicherheit-gut-behandelt.de/). Darin werden verschiedene Themenbereiche im Zusammenhang mit dem Betrieb einer Arztpraxis wie z.B. die Praxisorganisation, die digitale Arztpraxis, die Behandlungsdokumentation oder der Praxisverkauf datenschutzrechtlich aufbereitet. Weiterführende Informationen, Materialien, Handlungsempfehlungen oder Checklisten werden über Weblinks erschlossen und den Nutzerinnen und Nutzern zugänglich gemacht.

Daneben ist geplant, im Rahmen regionaler Veranstaltungen Ärztinnen und Ärzten und Beschäftigten in Praxen vor Ort Gelegenheit zu geben, sich über die Thematik zu informieren und einen Dialog mit den Aktionspartnern aufzubauen. Über Impulsbeiträge in dem Mitteilungsblatt der Kassenärztlichen Vereinigung Rheinland-Pfalz sollen zudem themenspezifisch konkrete Inhalte aufgegriffen und erörtert werden.

Flankiert werden soll die Aktion durch eine frühzeitige Einbindung der Heilberufskammern und der Hersteller von Praxis-IT.

Der LfDI erhofft sich mit der Initiative eine deutliche Verbesserung des Datenschutzes und der IT-Sicherheit im Bereich der niedergelassenen Ärztinnen und Ärzte.

3.4 Die Webseite des LfDI

Das Internetangebot des LfDI wurde und wird kontinuierlich ausgebaut. Beispielhaft zeigt sich dies an der neuen Rubrik „Selbstdatenschutz“ (http://www.datenschutz.rlp.de/de/selbstds.php), die praxisnah erläutert, wie die Preisgabe von Daten vermindert werden kann.

Die auf dieser Webseite bereitgestellten Informationen fanden regenregen Zuspruch, was sich auch aus den Zugriffszahlen ergibt. So sind an einem durchschnittlichen Tag über 220 Besuche zu verzeichnen. Der überwiegende Teil der Zugriffe erfolgt aus der Landes- und Kommunalverwaltung. Interesse fanden vor allem die Bereiche Aktuelles, Materialien und Orientierungshilfen, die FAQs sowie der Bereich des Selbstdatenschutzes.

4. Kontakte und Kooperationen

Es ist im Interesse des Datenschutzes, wenn der LfDI zur bestmöglichen Wahrnehmung seiner Aufgaben den Kontakt und die Zusammenarbeit mit anderen Stellen und Einrichtungen sucht, die dem Datenschutz verpflichtet sind. Zum Teil ist er dazu gemäß § 24 Abs. 4 LDSG sogar gesetzlich verpflichtet. Im Folgenden werden einige Kooperationspartner, die im Berichtszeitraum eine größere Rolle gespielt haben, und die Art der Zusammenarbeit dargestellt.

4.1 medien+bildung.com

„medien+bildung.com“ ist eine gGmbH, zu deren Hauptgesellschafter u.a. die rheinland-pfälzische Landeszentrale für Medien und Kommunikation (LMK) gehört. Zu ihren aktuellen Themenschwerpunkten gehören neben der kulturellen Medienbildung u.a. der Bereich der digitalen Innovation und damit alle angesagten Internetplattformen.

Mit „medien+bildung.com“ besteht seit 2010 eine enge Kooperation, die u.a. auch die Abordnung von Mitarbeitern zum LfDI einschließt. Derzeit teilen sich zwei „medien+bildung.com“-Mitarbeiter eine Planstelle beim LfDI. Beide sind Medienpädagogen, beide waren maßgeblich am Aufbau von „www.youngdata.de“ beteiligt. Auch die konzeptionelle Weiterentwicklung dieser Seite und den darauf aufbauenden E-Learning-Szenarien fällt in ihre Zuständigkeit, die im Übrigen auch die Fortentwicklung der den Schülerworkshops zugrunde liegenden pädagogischen Konzepte umfasst.

Die Kooperation mit „medien+bildung.com“ erstreckt sich im Übrigen auch auf den Ideenwettbewerb für innovative Medienbildung in Rheinland-Pfalz, mit dem zeitgemäße pädagogische Reaktionen auf mediale Entwicklungen gefördert werden.

4.2 Verbraucherzentrale Rheinland-Pfalz

Da der Datenschutz – wie schon mehrfach erwähnt wurde – zunehmend auch als Verbraucherdatenschutz verstanden werden muss, liegt es für die Datenschutzbeauftragten nahe, einen möglichst engen Schulterschluss mit den Verbraucherzentralen zu suchen. In Rheinland-Pfalz sind wir auf diesem Weg schon ein gutes Stück vorangekommen. Denn zwischen dem LfDI und der rheinland-pfälzischen Verbraucherzentrale mit Ulrike von der Lühe an der Spitze wird auf einigen Themenfeldern bereits eine gute Zusammenarbeit gepflegt. Sie schließt Veranstaltungen ebenso ein wie gemeinsame Publikationen. Auch der vom Verbraucherschutzministerium organisierte „Verbraucherdialog“ bindet sowohl die rheinland-pfälzische Verbraucherzentrale wie den LfDI mit ein. Dass in Rheinland-Pfalz im Koalitionsvertrag von „Rot-Grün“ vereinbart wurde, „die enge Zusammenarbeit zwischen Daten- und Verbraucherschutz“ und „ein koordiniertes Vorgehen“ zu fördern, ist ein richtiges Signal, das vom LfDI – auch in der Praxis – nachdrücklich unterstützt wird.

4.3 Chaos Computer Club

In einer Zeit der digitalen Umgestaltung unserer Gesellschaft ist es auch notwendig, den Kontakt und die Zusammenarbeit mit zivilgesellschaftlichen Einrichtungen zu pflegen, die Fragen des Datenschutzes und der Datensicherheit kompetent zu beantworten wissen. Dazu gehört sicherlich der Chaos Computer Club, zu dem der LfDI immer wieder Möglichkeiten der Zusammenarbeit sucht. Diese gibt es mittlerweile auf verschiedenen Ebenen. Mit Dr. Constanze Kurz, Sprecherin des Chaos Computer Club, gibt es regelmäßige Kontakte, übrigens auch im Bereich der Informationsfreiheit, im Übrigen aber auch auf dem Gebiet des Datenschutzes, was sich u.a. immer wieder auch in gemeinsamen Veranstaltungen ausdrückt. Im Übrigen hat der LfDI gemeinsam mit dem Chaos Computer Club Mainz-Wiesbaden einige unserer Crypto-Sessions durchgeführt. Ohne den Sachverstand des Chaos Computer Club wären diese Crypto-Sessions, von denen oben bereits die Rede war, nicht so erfolgreich verlaufen.

4.4 Beirat für den Datenschutzpreis

Der rheinland-pfälzische Datenschutzpreis (vgl. Tz. II-1.1.1) wird in Abstimmung mit einem Beirat vergeben, den der LfDI vor mehreren Jahren eingesetzt

hat. Ihm gehören u.a. Vertreterinnen und Vertreter der Landesregierung, der Hochschulen, der Kirchen, der Rundfunkanstalten und aus dem Bereich der Wirtschaft an.

Aktuell sind dies Prof. Dr. Walter Rudolf, ehemaliger Landesbeauftragter für den Datenschutz Rheinland-Pfalz als Vorsitzender, sowie

- Timo Ahland, Boehringer Ingelheim Pharma GmbH & Co. KG,
- Christoph Bach, Datenschutzbeauftragter des Zweiten Deutschen Fernsehens,
- Prof. Dr. Frank Bomarius, Fraunhofer-Institut für Experimentelles Software Engineering,
- Wolfgang Faller, Direktor der Landeszentrale für politische Bildung,
- Prof. Dr. Rüdiger Grimm, Universität Koblenz-Landau,
- Prof. Dr. Armin Herb, Datenschutzbeauftragter des Südwestrundfunks,
- Prof. Dr. Paul Müller, Technische Universität Kaiserslautern,
- Prof. Dr. Dr. h.c. Rainer Pitschas, Deutsche Hochschule für Verwaltungswissenschaften,
- Carsten Pörksen, Landtagsabgeordneter,
- Dr. Thomas Posern, Beauftragter der Evangelischen Kirchen in Rheinland-Pfalz,
- Prof. Dr. Gerhard Robbers, Universität Trier,
- Pia Schellhammer, Landtagsabgeordnete,
- Herbert Schneiders, Landtagsabgeordneter und
- Prof. Dr. Maria Wimmer, Universität Koblenz-Landau.

Der Beirat unterstützt die Vergabe des Preises durch eine Jury und dadurch, dass die Beiratsmitglieder die Vielfalt und Themenbreite ihrer jeweiligen Bereiche in die Vergabe einbringen. Angesichts der zunehmenden Durchdringung nahezu aller Lebensbereiche mit Informationstechnik bedarf es einer verstärkten Sensibilisierung für datenschutzrechtliche Belange und Bemühungen um eine zeitgemäße Umsetzung des Datenschutzes. Hier leistet der Beirat einen wichtigen Beitrag.

Neben der Vergabe des Datenschutzpreises behandelt der Beirat auch allgemeine Fragen des Datenschutzes. Die Breite der von den Beiratsmitgliedern repräsentierten Themen ist dabei von besonderem Wert für die Arbeit des LfDI. Angesichts einer zunehmenden Verflechtung datenschutzrechtlicher Fragen mit unterschiedlichsten Aspekten in Wirtschaft und Gesellschaft stellt die im Beirat bestehende Möglichkeit, Datenschutzfragen losgelöst von den Rahmenbedingungen einer Aufsichts- und Kontrollbehörde offen und ohne Vorbehalte zu diskutieren, einen unschätzbaren Vorteil dar.

Der LfDI möchte sich daher bei den Mitgliedern des Beirats für die stets rege und wohlwollende Unterstützung des Datenschutzpreises im Besonderen und der Arbeit des LfDI im Allgemeinen bedanken. Aufgrund von Veränderungen in Funktion und Amt von Beiratsmitgliedern stehen mehrere Neubesetzungen an. Der LfDI wird sich dabei weiterhin darum bemühen, dass die unterschiedlichen Aspekte der rheinland-pfälzischen Wirtschaft und Gesellschaft im Beirat ihren Niederschlag finden.

4.5 Behördliche und betriebliche Datenschutzbeauftragten

Der LfDI sieht nach wie vor einen Schwerpunkt seiner Arbeit in der Vernetzung der behördlichen und betrieblichen Datenschutzbeauftragten:

Im Berichtszeitraum wurden die regelmäßigen Treffen mit den Datenschutzbeauftragten der obersten Landesbehörden (der Ministerien, des Rechnungshofs und der Landtagsverwaltung) fortgeführt. Jeweils zum Ende des Jahres wurde ein Treffen durchgeführt. Dabei standen Themen der Internetnutzung und des Beschäftigtendatenschutzes im Vordergrund. Im Übrigen ging es insbesondere um folgende Themen

- Facebook- und Twitterauftritte der Behörden,
- Webanalyse-Tools,
- Umgang mit Nutzerdaten der Besucherinnen und Besucher von Webseiten,
- Protokollierungsschranken bei der Internetnutzung am Arbeitsplatz,
- Verhaltensregeln für Beschäftigte im Internet („Internet Guidelines“).

Außerdem wurde die Rechtsentwicklung auf nationaler und europäischer Ebene thematisiert.

Im Berichtszeitraum kamen die Datenschutzbeauftragten der Kommunen bereits zum sechsten und siebten Mal zusammen. Auf dem Programm standen das Verfahrenskonzept und die Systemarchitektur sowie die rechtlichen Rahmenbedingungen des elektronischen Personenstandsregisters, eine Einführung in das Landesinformationsfreiheitsgesetz sowie die Nutzung von mobilen Endgeräten. In Fortführung der Crypto-Sessions des LfDI wurde ein Workshop zum Einsatz von Verschlüsselungslösungen durchgeführt (vgl. Tz. II-1.1.1). Weiterhin erhielten die Teilnehmerinnen und Teilnehmer der Tagung u.a. ausführliche Informationen zu Sicherheit und Datenschutz im Kommunalen Netz.

Ebenso trafen sich die Datenschutzbeauftragten der Hochschulen sowie der Justiz, um mit dem LfDI, aber auch untereinander aktuelle Fragestellungen aus der täglichen Datenschutzpraxis zu erörtern. Im Anschluss an die Treffen mit der Justiz ergaben sich vielfältige Fortbildungsaktivitäten (vgl. Tz. II-2.11).

Der regelmäßige Austausch mit den behördlichen Datenschutzbeauftragten ist allerdings nicht auf die jährlich wiederkehrenden Treffen beschränkt. Diese Treffen haben vielmehr Netzwerke entstehen lassen, die für die einzelnen Datenschutzbeauftragten jederzeit auch für datenschutzrechtliche Alltagsfragen aktiviert werden können. Für die kommunalen Datenschutzbeauftragten wird dies noch dadurch unterstützt, dass ihnen auf der Homepage des LfDI ein Forum zur Diskussion konkreter datenschutzrechtlicher Problemstellungen gegeben wird.

Mit den kirchlichen Datenschutzbeauftragten wurde ein Treffen im Jahr 2012 vereinbart; aus Kapazitätsgründen konnte 2013 kein Folgetreffen stattfinden. Für 2014 allerdings ist ein weiteres Treffen geplant. Wegen der vielfältigen Zuständigkeiten der kirchlichen Datenschutzbeauftragten (für kirchliche Kindergärten, Schulen, Krankenhäuser, sonstige soziale Einrichtungen) ergeben sich immer wieder Fragen, die sich dort in gleicher Weise wie im staatlichen Bereich stellen. Die Aufgabe des LfDI, auf möglichst gleiche Datenschutzstandards in den unterschiedlichen Bereichen hinzuwirken (§ 24 Abs. 7 Satz 1 LDSG), erfordert möglichst kontinuierliche Kontakte auch mit den kirchlichen Datenschutzbeauftragten.

Auch die Kontakte zu den Erfahrungsaustauschkreisen, sog. Erfa-Kreise, der betrieblichen Datenschutzbeauftragten wurden weiter intensiviert, durch eigene Informationsveranstaltungen u.a. in Mainz, Koblenz und Ludwigshafen wurde die Netzwerkbildung in diesem Bereich weiter gefördert.

5. Feststellungen und Kontrollen

Landes- und Bundesdatenschutzgesetz verpflichten den LfDI dazu, die Einhaltung von Datenschutzbestimmungen durch Behörden, Unternehmen und Vereine zu überwachen. Bis zu einem gewissen Grad und Umfang ist dies auch dadurch möglich, dass der LfDI Beschwerden von Bürgerinnen und Bürgern in konkreten Einzelfällen nachgeht. Das bedeutet aber nicht, dass in den Bereichen, in denen es keine Beschwerden gibt, datenschutzrechtlich alles in Ordnung wäre. Eine solche Vermutung wäre realitätsfern.

Es ist deshalb notwendig, dass der LfDI von Amts wegen und ohne Ankündigung immer wieder Vor-Ort-Kontrollen und sog. örtliche Feststellungen durchführt. Traditionell bestand darin einer seiner Arbeitsschwerpunkte. Die Digitalisierung unserer Gesellschaft, die zu einem rasanten Anstieg von Eingaben und zu vermehrten digitalen Bildungsanstrengungen geführt haben, hat allerdings auch zur Folge, dass die personellen Kapazitäten und Freiräume für solche anlasslosen Kontrollen schmäler werden. Sie waren im Berichtszeitraum deshalb nicht mehr in dem Umfange möglich, wie dies wünschenswert gewesen wäre.

Trotzdem hat der LfDI auch 2012 und 2013 noch eine Reihe solcher Kontrollen durchgeführt, und zwar insbesondere in folgenden Bereichen:

- in Krankenhäusern
- in Hotelbetrieben
- bei Finanzämtern
- beim Verfassungsschutz
- beim Landesbetrieb Daten und Information.

Neben diesen öffentlichen Einrichtungen wurden natürlich auch Unternehmen der Privatwirtschaft kontrolliert.

Insgesamt handelt es sich um über 100 Kontrolltermine. Regelmäßig sind bei solchen Kontrollen vor Ort sowohl die juristischen Referentinnen und Referenten wie die technischen Mitarbeiter der Dienststelle gefordert. Das begründet einen erheblichen personellen Aufwand für die Erledigung entsprechender Aufgaben.

Insgesamt war es aus Sicht des LfDI möglich, noch im nennenswerten Umfang im Bereich der örtlichen Feststellungen und Kontrollen tätig zu werden. Jedenfalls das absolut Notwendige wurde erledigt.

Für die Ergebnisse dieser Kontrollen ist auf die jeweiligen Abschnitte des Tätigkeitsberichts zu verweisen, in denen die Kontrollergebnisse im sachlichen Zusammenhang dargestellt werden.

6. Debeka

Im Sommer 2013 erhielt der LfDI erstmals konkrete Hinweise darauf, dass es im Vertriebsbereich des rheinland-pfälzischen Versicherers, der deutschlandweit führend im Bereich privater Krankenversicherungen ist, zu erheblichen Datenschutzproblemen gekommen sei. Es wurde der Vorwurf erhoben, das Versicherungsunternehmen und dessen Mitarbeiterinnen und Mitarbeiter hätten Daten von potentiellen Neukundinnen und -kunden widerrechtlich angekauft und innerhalb des Unternehmens zum Abschluss von Versicherungsverträgen weiterverkauft.

Darüber hinaus wurde der Verdacht geäußert, dass es im sog. „Tippgeber-System“ des Versicherungsunternehmens zu weiteren systematischen Datenschutzverstößen gekommen sei. Über Jahrzehnte hinweg habe der Versicherer ein bundesweites Netz von sog. Tippgeberinnen und -gebern insbesondere in öffentlichen Verwaltungen aufgebaut und die öffentlich Bediensteten für Hinweise auf Abschlussmöglichkeiten honoriert. Es bestehe dabei der Verdacht, dass Tippgeberinnen und -geber dienstlich erlangte Daten von potentiellen Neukundinnen und -kunden an das Versicherungsunternehmen ohne wirksame Einwilligung der Betroffenen weitergegeben haben.

Diesen Vorwürfe, die vor allem auch in den Medien erhoben wurden, wird derzeit nachgegangen, wobei es um verschiedene Verantwortlichkeiten geht. Die erhobenen Vorwürfe richten sich nämlich nicht nur gegen das Unternehmen, dessen Vorstandsmitglieder und einzelne Außendienstbeschäftigte, sondern auch gegen einzelne Tippgeberinnen und -geber aus der Beamtenschaft des Landes Rheinland-Pfalz und anderer Länder. Damit stellt sich auch die Frage, wie die Dienstvorgesetzten dieser Beamtinnen und Beamten bzw. Beschäftigte des öffentlichen Dienstes mit der Kundenakquise des Versicherungsunternehmens umgegangen sind.

Die Frage, ob andere Versicherungsunternehmen sich auch datenschutzrechtlich fragwürdiger Vertriebssysteme bedienen oder bedient haben, kann vom LfDI nicht beantwortet werden. Diese Versicherungsunternehmen unterliegen nicht seiner Zuständigkeit.

6.1 Aktivitäten gegenüber der Debeka

Auf der Grundlage der erhobenen Verwürfe hat der LfDI Anfang November 2013 zunächst ein aufsichtsbehördliches Verfahren gemäß § 38 Abs. 3 BDSG gegen das Versicherungsunternehmen eingeleitet. Neben dem LfDI haben auch die Staatsanwaltschaft Koblenz und die Bundesanstalt für Finanzdienstleistungsaufsicht eigene Untersuchungen und Ermittlungen aufgenommen.

Neben dem Vorwurf des illegalen Datenhandels beschäftigt sich der LfDI insbesondere mit der Struktur des Vertriebssystems des Versicherungsunternehmens und geht der Frage nach, ob dieses Verstöße gegen Datenschutzbestimmungen möglicher Weise zumindest begünstigt hat. Das Auskunftsverfahren mündete im Dezember 2013 in ein Ordnungswidrigkeitenverfahren gegen das Versicherungsunternehmen und seine Vorstandsmitglieder.

Neben den dargelegten mutmaßlichen Verstößen gegen Datenschutzbestimmungen durch das Unternehmen bejaht der LfDI damit einen Anfangsverdacht, dass der Vorstand der Debeka vorsätzlich oder fahrlässig ihm obliegende Aufsichtspflichten verletzt haben könnte. Es geht dabei insbesondere um die Frage, ob der Vorstand alles ihm Mögliche getan hat, um zu verhindern, dass es im Rahmen der Neukundengewinnung zu strafbaren oder mit Bußgeld bedrohten Verletzungen von Datenschutzgesetzen durch Außendienstbeschäftigte des Versicherungsunternehmens einerseits und durch die Tippgeberinnen und -geber andererseits gekommen ist. Geprüft wird hier eine Verletzung der §§ 130 und 30 OWiG.

Der Vorstand des Versicherers hat bislang die Aufklärungsarbeit des LfDI aktiv unterstützt und deutlich gemacht, dass zukünftig datenschutzrechtliche Fragen mit der gebotenen Sensibilität behandelt werden. Der LfDI führt seit Ende 2013 darüber hinaus mit dem Versicherer konstruktive Gespräche über notwendige Veränderungen im Vertriebssystem; diese Gespräche dauern über den Berichtszeitraum hinaus weiter an. Der LfDI rechnet mit einem einvernehmlichen Abschluss dieser gemeinsamen Bemühungen um eine Modifikation des Vertriebssystems.

6.2 Aktivitäten in Bezug auf die Landesregierung und einzelne Tippgeberinnen und -geber

Darüber hinaus hat der LfDI gegen einzelne Tippgeberinnen und -geber Ordnungswidrigkeitsverfahren eingeleitet. Gegenstand der Ermittlungen ist ein Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG und in diesem Zusammenhang das fahrlässige oder vorsätzliche unbefugte Erheben oder Verarbeiten von nicht allgemein zugänglichen Daten. Es besteht, wie bereits ausgeführt, in einer Reihe von Fällen der Verdacht, dass durch Tippgeberinnen und -geber dienstlich erlangte personenbezogene Daten ohne Einverständnis der potentiellen Versicherungskundinnen und -kunden genutzt und an die Debeka weitergegeben wurden. Für den Fall, dass sich diese Verdachtsfälle bestätigen, wäre mit der Verhängung von Bußgeldern gegen die betroffenen Beschäftigten des öffentlichen Dienstes zu rechnen.

Gleichzeitig hat der LfDI den Dialog mit den Dienstherren aufgenommen. Insbesondere mit der Landesregierung und dem Ministerium des Inneren, für Sport und Infrastruktur besteht eine enge Zusammenarbeit. Es ist das Bestreben aller Beteiligten, Datenschutzverstöße aufzuklären und mit Blick auf die Zukunft durch klare Strukturen zu verhindern. Zu diesem Zweck hat das Ministerium des Inneren, für Sport und Infrastruktur – nach Klarstellung der datenschutzrechtlichen Unzulässigkeit der Nutzung dienstlich erlangter Informationen für Werbezwecke – erfragt, wie viele Beamtinnen und Beamte mit einer Nebentätigkeitsgenehmigung als Tippgeberinnen und -geber tätig geworden sind.

Auch insoweit sind die Entwicklungen zum Ende des Berichtszeitraums noch im Fluss. Für die einzelnen Dienstherren sind dabei neben datenschutzrechtlichen Bestimmungen beamtenrechtliche Vorgaben wie das Nebentätigkeitsrecht, aber auch Fragen des Wettbewerbsrechts relevant.

7. Sonstige Arbeitsschwerpunkte des LfDI

7.1 Datenschutz und IT-Sicherheit in Krankenhäusern

Seit 2009 steht der datenschutzgerechte Einsatz von Krankenhausinformationssystemen im Fokus der Datenschutzaufsichtsbehörden in der Bundesrepublik. Bei diesen IT-Systemen handelt es sich um Verfahren, die Behandlungsprozesse in Krankenhäusern durch die Bereitstellung patientenbezogener Informationen unterstützen. Hierzu gehören administrative Angaben, wie z.B. zur Krankenversicherung oder zu den Angehörigen der Patientinnen und Patienten, insbesondere aber medizinische Daten. Die in Krankenhausinformationssystemen enthaltenen Daten dienen der Verwaltung und Dokumentation der stationären Behandlungsfälle und werden somit von einer Vielzahl der in einem Krankenhaus tätigen Beschäftigten zu unterschiedlichen Zwecken (z.B. Aufnahme, ärztliche Behandlung und Pflege, Therapie, Abrechnung, seelsorgerische Betreuung, Qualitätssicherung, Controlling) genutzt. Da zur Erfüllung dieser einzelnen Aufgaben jeweils unterschiedliche Informationen von den verschiedenen Organisationseinheiten im Krankenhaus benötigt werden, müssen die Systeme bereits Funktionalitäten beinhalten, die eine differenzierte Gewährung von Zugangsrechten erlauben. Zugleich sind die Krankenhausbetreiber verpflichtet, derartige Instrumente dann auch tatsächlich einzusetzen.

Bereits im März hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe für den datenschutzgerechten Einsatz dieser Systeme vorgelegt. Zahlreiche Rückmeldungen von Krankenhausbetreibern und Herstellern von Krankenhausinformationssystemen, aber auch die Ergebnisse eines in Rheinland-Pfalz durchgeführten Referenzprojektes belegen die Notwendigkeit und Praxistauglichkeit dieser Orientierungshilfe, die gleichwohl behutsam weiterzuentwickeln ist. Eine Arbeitsgruppe der Datenschutzbeauftragten, in der auch der LfDI mitarbeitet, beabsichtigt, bis zum Frühjahr 2014 der Datenschutzkonferenz die notwendige Fortschreibung vorzulegen.

Sehr erfreulich verlief die Beteiligung der Deutschen Krankenhausgesellschaft. Nach anfänglicher Kritik an Zustandekommen und Inhalt der OH KIS konnte mittlerweile ein sehr konstruktiver Dialog zwischen der Arbeitsgruppe und dem Verband erzielt werden. Die Deutsche Krankenhausgesellschaft plant, zeitnah Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der OH KIS zu veröffentlichten und damit das Anliegen des Datenschutzes grundsätzlich zu unterstützen. Ein im Sommer 2013 der Arbeitsgruppe vorgelegter Entwurf zeigt, dass die Vereinbarkeit einer optimalen Patientenversorgung mit dem Schutz des informationellen Selbstbestimmungsrechts der Betroffenen auch seitens der Betreiber anerkannt ist.

Neben seiner Beteiligung an der bundesweiten Arbeitsgruppe legte der LfDI im Berichtszeitraum in besonderem Maße Gewicht darauf, einen datenschutzgerechten Einsatz von Krankenhausinformationssystemen in den seiner Zuständigkeit unterliegenden rheinland-pfälzischen Krankenhäusern sicherzustellen. Hierzu wurden folgende Maßnahmen ergriffen:

■ Abschluss des Referenzprojektes

Das im August 2011 begonnene Referenzprojekt mit dem Landeskrankenhaus (AöR), dem größten rheinland-pfälzischen Krankenhausträger im Bereich psychiatrisch-psychotherapeutischer und neurologischer Leistungen, konnte im April 2012 erfolgreich abgeschlossen werden. Im Ergebnis bestätigte sich, dass die OH KIS für die Beschreibung und Umsetzung der datenschutzrechtlichen Anforderungen an den Einsatz von Krankenhausinformationssystemen grundsätzlich praxistauglich und angemessen ist.

Im Rahmen der Prüfung zeigte sich zudem, dass mit der im Landeskrankenhaus (AöR) betriebenen IT-Lösung ein Großteil der in der Orientierungshilfe vorgegebenen Muss-Anforderungen abgedeckt wird. So wurde beispielsweise zwischen verschiedenen Benutzergruppen und den ihnen zugeordneten Berechtigungen differenziert und die Datenhaltung in Bezug auf die verschiedenen Standorte des Landeskrankenhauses gemäß der Orientierungshilfe ausgestaltet. Gleiches gilt für die Organisation des technischen Betriebs sowie die Administration der Anwendungen und Systeme.

Dennoch wurden auch Defizite bei dem Einsatz des Krankenhausinformationssystems offenkundig: Obwohl das von der Orientierungshilfe geforderte Rollen- und Berechtigungskonzept vorhanden war, entsprach es noch nicht den datenschutzrechtlichen Anforderungen. Die in dem Konzept getroffenen Abgrenzungen waren zu grob, so dass es an einer ausreichend differenzierten Struktur für die Erteilung der Berechtigungen fehlte. Mangels Auswertungskonzept war zudem die Frage ungeklärt, ob, in welchem Umfang und in welcher Weise erzeugte Protokolldaten ausgewertet werden dürfen. Schließlich fand sich im Krankenhausinformationssystem des Landeskrankenhauses (AöR) bislang keine automatisierte Funktion zur Archivierung und Löschung von Patientenakten. Angesichts der Bedeutung dieser Anforderungen ist es Aufgabe des Systemherstellers, zeitnah geeignete Archivierungsfunktionen anzubieten.

http://www.datenschutz.rlp.de/de/aktuell/2012/images/Referenzprojekt_Landeskrankenhaus_Projektbericht_Zusammengfassung.pdf

■ Workshop zur Umsetzung der OH KIS

In Fortsetzung des im Juni 2011 begonnenen Dialogs mit den Krankenhäusern im Lande (vgl. 23. Tb., Tz. I-3.6) führte der LfDI im September 2012 einen Workshop zum datenschutzgerechten Einsatz von Krankenhausinformationssystemen durch. Mit der Veranstaltung in Mainz, an der neben zahlreichen Vertreterinnen und Vertretern der betroffenen Krankenhäuser und Träger auch die Krankenhausgesellschaft Rheinland-Pfalz und der Bundesverband der Gesundheits-IT teilnahmen, sollte der bislang nur schleppend in Gang gekommene Umsetzungsprozess innerhalb der Krankenhäuser einen neuen Impuls erhalten. Die vom LfDI im Rahmen des Workshops mit den Teilnehmern abgestimmten Arbeitshilfen wurden dabei als willkommene und nützliche Materialien allseits begrüßt. Ein Leitfaden zur strukturierten Umsetzung der datenschutzrechtlichen Anforderungen an den Einsatz von KIS einschließlich eines Maßnahmeplans, zahlreiche themenbezogene Checklisten sowie eine Priorisierung der in der Orientierungshilfe enthaltenen Anforderungen sollen den Einrichtungen das konkrete Tätigwerden erleichtern. Im Gegenzug wird von den Krankenhäusern und deren Trägern nun erwartet, zügig die vor Ort eingesetzten Systeme auf ihre Datenschutzverträglichkeit hin zu überprüfen und ggf. festgestellte Unzulänglichkeiten abzustellen.

http://www.datenschutz.rlp.de/downloads/oh/OH_KIS_Materialien_LfDI_RLP.zip

■ Befragungen zum konkreten IT-Einsatz und zum Umsetzungsstand der OH KIS

In einer zweiten Umfrage im Frühjahr 2013 versuchte der LfDI festzustellen, inwieweit die seiner Aufsicht unterliegenden Einrichtungen die von ihnen eingesetzten Systeme inzwischen auf ihre Datenschutzverträglichkeit hin überprüft hatten. Es stellte sich heraus, dass erst mit der Veröffentlichung der OH KIS und den damit verbundenen Aktivitäten des LfDI die weit überwiegende Zahl der befragten Häuser eine Revision der eingesetzten Systeme durchführte. Dabei wurde fast immer ein konkreter Handlungsbedarf festgestellt. Neben der Erstellung oder Überarbeitung technischer Konzepte (z.B. Datenschutzkonzept, IT-Sicherheitskonzept, Rollen- und Berechtigungskonzept, Protokollierungskonzept, Archivierungs- und Löschkonzept) beabsichtigen die Betreiber vermehrt, durch interne Schulungsmaßnahmen und die Kontaktaufnahme mit dem Systemhersteller bestehende Defizite auszuräumen.

■ Örtliche Feststellungen

Die mit der Umfrage gewonnenen Erkenntnisse waren Grundlage für die nun örtlichen Feststellungen des LfDI bei einzelnen Krankenhäusern im Land. Im Rahmen einer bis 2015 angesetzten strukturierten Prüfungsreihe wurden seit September 2013 bislang verschiedene Einrichtungen u.a. das Klinikum Worms und das Gemeinschaftsklinikum Koblenz-Mayen am Standort Kemperhof Koblenz besucht. Dabei ist es jetzt schon ersichtlich, dass trotz der allgemeinen Bereitschaft, die datenschutzrechtlichen Anforderungen zu erfüllen, in der Praxis immer noch gravierende Handlungsdefizite bei dem Betrieb von Krankenhausinformationssystemen bestehen. So fehlt es in Bezug auf die eingesetzten IT-Verfahren regelmäßig systemseitig an der datenschutzrechtlich gebotenen Funktionalität der Löschung. Ohne diese Funktion sind jedoch die

Betreiber nicht in der Lage, gesetzlich vorgegebene Löschverpflichtungen auch zu erfüllen.

Die Krankenhäuser ihrerseits gewähren den einzelnen Organisationseinheiten im Hause oftmals sehr weitgehende Zugangsmöglichkeiten zu den im Krankenhausinformationssystem vorgehaltenen Patientendaten, obwohl dies häufig überhaupt nicht zur Aufgabenerfüllung der einzelnen Beschäftigten erforderlich wäre. Ein Grund hierfür ist vermutlich die nur unzureichende konzeptionelle Vorbereitung für die Vergabe von Zugriffsberechtigungen. Nicht selten wurden Berechtigungen gewährt, mit denen Informationen zu sämtlichen aktuell und in der Vergangenheit in dem Krankenhaus behandelten Patientinnen und Patienten abgerufen werden können. Ein derartiger Zustand steht jedoch in deutlichem Widerspruch zu den datenschutzrechtlichen Vorgaben und kann seitens des LfDI nicht hingenommen werden.

Der Weg zu mehr IT-Sicherheit und Datenschutz beim Einsatz von Krankenhausinformationssystemen ist weit und steinig. Die Datenschutzbeauftragten sind sich des damit verbundenen Aufwandes für die Betreiber und Träger der Krankenhäuser durchaus bewusst. Gleichwohl handelt es sich bei dem der Orientierungshilfe zugrunde liegenden Anliegen nicht um eine überflüssige und zeitraubende Spielerei einiger Aufsichtsbehörden. Das Papier zielt vielmehr auf die schon seit langem bestehende Pflicht der Krankenhäuser, im Rahmen einer stationären Behandlung das Recht der Patientinnen und Patienten auf informationelle Selbstbestimmung einschließlich der Wahrung der ärztlichen Schweigepflicht sicherzustellen. Dies gilt selbstverständlich auch und gerade beim Einsatz moderner Informationstechnologie. Mit der OH KIS und den in diesem Zusammenhang vorgelegten Arbeitshilfen sollen sowohl Betreiber als auch Hersteller der im Krankenhausbereich eingesetzten Systeme leichter erkennen können, welche konkreten Anforderungen an datenschutzgerechte Systeme bestehen und in welcher Weise eventuell vorhandene Defizite erkannt und behoben werden können. Die damit bestehende Chance zu mehr IT-Sicherheit und Datenschutz im digitalen Krankenhausbetrieb sollte nicht ungenutzt verstreichen.

7.2 Datenschutz in Hotels

Immer wieder erreichen den LfDI Hinweise zu Datenschutzverstößen im Hotelgewerbe. Dies hat der LfDI 2012 zum Anlass genommen, in einer breit angelegten Aktion den Datenschutzstandard von Hotels in Rheinland-Pfalz zu untersuchen. Dazu wurden mehr als 100 kleinere und mittlere Hotelbetriebe vor Ort sowie alle 19 in Rheinland-Pfalz ansässigen Hotelketten überprüft.

Gleichzeitig wurde in Kooperation mit dem DEHOGA Rheinland-Pfalz eine Umfrage bei allen Hotelbetrieben im Land durchgeführt. Dabei wurden zehn Fragen an die Hotelbetriebe gerichtet, etwa zum Einsatz von Kundenbindungsprogrammen, zur Erstellung von Kundenprofilen, zum Einsatz von Videoüberwachung sowie zur Ausgestaltung der Meldescheine.

Die Ergebnisse dieser freiwilligen Umfrage wurden vom DEHOGA Rheinland-Pfalz ausgewertet und flossen in eine Orientierungshilfe des LfDI ein, in welcher in Abstimmung mit der DEHOGA die wesentlichen Datenschutzprobleme in Hotels thematisiert und mit Hinweisen und Tipps für die datenschutzgerechte Arbeit verbunden wurden: http://www.datenschutz.rlp.de/downloads/oh/Datenschutz_Hotel.pdf

In dieser Orientierungshilfe werden nicht nur die Rechtsgrundlagen des Datenschutzes im Hotelgewerbe erläutert, sondern auch die persönliche Verantwortlichkeit der Geschäftsleitung für den Umgang mit persönlichen Angaben von Gästen, Beschäftigten und Geschäftspartnerinnen und -partnern dargelegt. Zu den wichtigsten Problemfeldern zählen insbesondere der Umgang mit Meldedaten, die Anfertigung von Kundenprofilen, der Einsatz von Videoüberwachungstechnik sowie Fragen der Datensicherheit. Abgerundet wird diese im April 2013 vorgestellte Orientierungshilfe durch „Tipps für Hotelgäste“, die zum Selbstdatenschutz beitragen sollen und auf die weiteren Unterstützungs- und Informationsmöglichkeiten beim LfDI hinweisen:

Tipps für Hotelgäste

Hoteliers, die sich ihrer Pflicht zum Schutz des informationellen Selbstbestimmungsrechts von Kunden und Mitarbeitern bewusst sind, tragen viel zum „gelebten Datenschutz“ bei. Genauso wichtig sind aber aufgeklärte und selbstbewusste Hotelgäste, die um den Wert ihrer Privatsphäre wissen und nicht in jede datenschutzrechtliche Zumutung blindlings einwilligen.

Hierzu die folgenden Tipps:

1. Datensparsamkeit schützt.
   Persönliche Daten, die ich dem Hotel nicht offenbare, können auch nicht zu meinem Nachteil verwendet werden. Das gilt auch für die Nutzung „kostenloser“ WLAN.
2. Fragen hilft.
   Wenn von mir Angaben verlangt werden, ohne dass gleichzeitig erläutert wird, auf welcher Grundlage gefragt wird und zu welchem Zweck die Daten erhoben werden, dann hilft nur die Nachfrage. Und das Bestehen auf eine Antwort.
3. Streich mal wieder.
   Nur weil ein vorgelegtes Formular viele Antwortfelder vorsieht, muss ich es noch lange nicht komplett ausfüllen. Fragen nach persönlichen Angaben, die ich nicht verstehe oder die ich nicht beantworten will, kann ich getrost streichen. Auf zwingend erforderliche Fragen wird der Hotelier mich hinweisen.
4. Auskunftsrechte nutzen.
   Das BDSG gibt dem betroffenen Gast umfangreiche Rechte gegenüber dem Hotel. Der Gast darf jederzeit und ohne Angabe von Gründen Auskunft über alle Informationen verlangen, die das Hotel über ihn gesammelt hat. Die Verweigerung der Auskunft kann sogar mit einem Bußgeld bestraft werden.
5. Alles auf Anfang: Das Widerrufsrecht ausüben.
   Auch wenn man früher mal eine Einwilligung zur Speicherung persönlicher Daten abgegeben hat, ein einfacher Widerruf lässt ganze Datensammlungen verschwinden. An eine einmal abgegebene Einwilligung ist man für die Zukunft nicht gebunden, ein formloser Widerruf verpflichtet den Hotelier, alle „Datenspuren“ zu beseitigen.
6. Hilfsangebote nutzen.
   Wenn man als Gast unsicher ist, wie man sich verhalten soll oder wenn man meint, der Hotelier geht mit den persönlichen Daten nicht korrekt um, dann hilft der Landesdatenschutzbeauftragte gerne weiter. Ein Anruf genügt.

7.3 Massenhafte Kfz-Kennzeichenerfassungen an Autobahnen

Seit Mitte 2008 waren auf deutschen Autobahnen immer wieder Fahrzeuge beschossen worden. In einem dieser Fälle wurde eine Person verletzt, in einem anderen Fall wurde der Kopf eines Fahrers nur knapp verfehlt.

Über 700 Beschüsse wurden bekannt, bei denen Schusswaffen mit zwei unterschiedlichen Kalibern zum Einsatz gekommen waren. Von den Schüssen waren vor allem die Autobahnen A 61 zwischen Kerpen und Walldorf, die A 6 zwischen Walldorf und Nürnberg, die A 5 zwischen Karlsruhe und Kirchheim, die A 4 zwischen Aachen und Köln und die A 3 zwischen Köln und Nürnberg betroffen.

Die Ermittlungsbehörden hatten trotz intensiver Fahndungsmaßnahmen lange keinen Hinweis auf den oder die Täter. Konkrete Hinweise zur Tatzeit oder dem Tatort ließen sich meist nur schwer rekonstruieren, da die Beschädigungen an den Fahrzeugen oft erst am Ende der Fahrt festgestellt und später angezeigt wurden. Bei den Staatsanwaltschaften Koblenz und Würzburg wurden Sammelverfahren eingeleitet. Das Bundeskriminalamt hatte eine „AG Transporter“ eingerichtet, um die bundesweiten Maßnahmen der Polizei zu koordinieren und die Erkenntnisse auszuwerten. Pressekonferenzen im Jahr 2009 sowie 2012 blieben ebenso erfolglos wie Öffentlichkeitsfahndungen in Rundfunk und Fernsehen. Auch Handzettel und Fahndungsplakate brachten trotz der ausgelobten Belohnung in Höhe von 100.000 Euro keine zielführenden Hinweise.

Mangels anderer Ermittlungsansätze und weil es zuletzt verstärkt zu Beschüssen von Pkws gekommen war – wobei anstatt des Kleinkalibers 5,6 mm nunmehr auch das wesentlich gefährlichere Kaliber 9 mm eingesetzt wurde – hatte das Bundeskriminalamt in Abstimmung mit der Staatsanwaltschaft Koblenz, ab dem 6. Dezember 2012 an sechs Standorten zwischen Nordrhein-Westfalen und Bayern eine stationäre Videoüberwachung von Autobahnabschnitten in beiden Fahrtrichtungen eingerichtet. Die Maßnahme wurde zunächst auf drei Monate beschränkt und später um einen Monat verlängert.

Bei dieser Überwachung wurden von allen an den Kontrollstellen vorbeifahrenden Fahrzeugen Bildaufnahmen gefertigt, auf denen die Kennzeichen zu erkennen waren. Die Fahrzeuginsassen waren auf den Bildern nicht erkennbar. Die Aufnahmen wurden unmittelbar automatisiert ausgewertet. Dabei entstand eine Liste der erfassten Kennzeichen, die wiederum automatisiert ausgewertet werden konnte. Die erhobenen Bilder und Daten wurden vor Ort über einen Zeitraum von zehn Tagen gespeichert und anschließend gelöscht bzw. überschrieben.

Täglich wurden auf diese Weise an allen Kontrollpunkten insgesamt rund 350.000 Kennzeichen erfasst. Das entspricht einer wöchentlichen Anzahl von 2,45 Millionen und monatlich 10,5 Millionen Fahrzeugkennzeichen.

Wurde ein Beschuss auf den überwachten Autobahnabschnitten bekannt, wurde zunächst ein Datenbestand selektiert, der alle zeitlich in Betracht kommenden Fahrzeuge erfasste. Dieser Datenbestand wurde von der regelmäßigen Löschung ausgenommen, um einen Abgleich mit Kennzeichenlisten aus anderen Beschussfällen zu ermöglichen. Mögliche „Kreuztreffer“ sollten z.B. über eine Halterfeststellung und weitere Ermittlungen der Feststellung des Täters dienen. Wurde festgestellt, dass die selektierten Datenbestände der Beschussserie nicht zugeordnet werden können, waren sie zu löschen.

Es gelang mithilfe dieses Verfahrens, den Täter im Juni 2013 zu identifizieren und ihn festzunehmen.

Der LfDI war seitens der rheinland-pfälzischen Justiz zu Beginn der Maßnahme im Dezember 2012 in Kenntnis gesetzt worden. Nach eingehender Prüfung vertrat er die Auffassung, dass es für die durchgeführte Strafverfolgungsmaßnahme keine ausreichend klare und verhältnismäßig ausgestaltete Rechtsgrundlage gibt. Auf die vorhandenen Ermächtigungsgrundlagen der Strafprozessordnung (§§ 100h, 163f StPO) hätte nach Auffassung des LfDI die Maßnahme nicht gestützt werden können. Zum einen waren deren Voraussetzungen nicht erfüllt und zum anderen war der vom Gesetz vorgesehene Richtervorbehalt nicht beachtet worden. Gegen Nichtbeschuldigte dürfen mit richterlicher Anordnung planmäßig angelegte Beobachtungen – sog. Observationen – nur durchgeführt werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass sie mit dem Täter in Verbindung stehen oder eine solche Verbindung herstellen werden (§ 163f StPO). Dies war für die täglich überwachten rund 350.000 Verkehrsteilnehmerinnen und –teilnehmer sicher auszuschließen.

Auf Anregung des LfDI wurde die Maßnahme zur Unterrichtung des Landtags im Rechtsausschuss und in der Datenschutzkommission behandelt. Eine Unterrichtung der Öffentlichkeit erfolgte erst nach Ergreifung des Täters am 21. Juni 2013.

Auch wenn die Fahndung nach dem Autobahnschützen am Ende erfolgreich war, fällt die datenschutzrechtliche Bilanz der Aktion eher zwiespältig aus. Bemerkenswert und positiv ist es, dass der LfDI frühzeitig vom rheinland-pfälzischen Justizministerium und den zuständigen Stellen der Staatsanwaltschaft im Lande über den Einsatz der Kfz-Kennzeichenkontrollstellen unterrichtet und auf dem Laufenden gehalten worden war. Auf diese Weise konnte auch gewährleistet werden, dass über die Datenschutzkommission die Landtagsfraktionen und auch der Rechtsausschuss des Landtags über das staatsanwaltschaftliche Vorgehen informiert waren.

Positiv ist auch, dass die gespeicherten Daten – von einer überschaubaren Zahl von Ausnahmen abgesehen – bereits zehn Tage nach ihrer Speicherung gelöscht wurden, so dass sich der Eingriff in die Grundrechte der Betroffenen in Grenzen gehalten hat. Bemerkenswert ist es schließlich auch, das die Koblenzer Staatsanwaltschaft den Einsatz der Kfz-Kennzeichenüberwachung zeitlich befristete, um so den Verhältnismäßigkeitsgrundsatz zum Tragen zu bringen.

Negativ zu verbuchen ist allerdings, dass es für diese bundesweit erstmals eingesetzte Ermittlungsmethode aus Datenschutzsicht keine hinreichende gesetzliche Ermächtigungsgrundlage gab. § 100h StPO, auf den sich die Staatsanwaltschaft stützte, ist für ganz andere Sachverhalte gedacht, nicht aber für Maßnahmen, bei denen man aus einer unbegrenzten Zahl von Daten völlig unverdächtiger Personen die eine Täterin oder den einen Täter herauszufiltern beabsichtigt. Dies zeigt auch der Vergleich mit der wohl für eine begrenzte Zahl von

Personen parallel durchgeführten Funkzellenüberwachung. Sie kann nur mit Genehmigung eines Richters realisiert werden. Für die komplette Überwachung ganzer Autobahnabschnitte ist dies in § 100h StPO dagegen nicht vorgesehen.

Nicht zu akzeptieren wäre es auch gewesen, wenn die Öffentlichkeit bei erfolgloser Durchführung der Maßnahmen – wie offenbar geplant – nicht informiert worden wäre. Bei derart gravierenden Eingriffen, die zur Speicherung von 60 bis 80 Millionen Datensätzen gänzlich unverdächtiger Personen führte, haben die Betroffenen und hat damit auch die Öffentlichkeit einen Anspruch auf Information. Nur dann auch kann die Rechtmäßigkeit eines entsprechenden staatsanwaltschaftlichen Vorgehens gerichtlich überprüft werden. Es geht nicht an, dass diese Selbstverständlichkeit nicht eindeutig in der Strafprozessordnung geregelt ist. In diesem Zusammenhang ist auf die Ergebnisse der „Regierungskommission zur Überprüfung der Sicherheitsarchitektur- und -gesetzgebung“ hinzuweisen, die diesen Punkt besonders hervorgehoben hat (vgl. Bericht der Regierungskommission vom 28. August 2013), Der LfDI ist nach seinen Erfahrungen in diesem Fall darum bemüht, im Zusammenwirken mit dem rheinland-pfälzischen Justizministerium die dargestellten Defizite zu thematisieren und ggf. durch gesetzgeberische Initiativen zu beseitigen. Die entsprechenden Gespräche haben bereits begonnen.

Was bleibt in diesem Fall also als datenschutzrechtliche Erkenntnis? Die Ermittlungsmaßnahmen werden immer dichter, die Kontrollinstrumente immer engmaschiger. Gleichzeitig wird ihre Streubreite aber immer größer. Millionen von unverdächtigen Personen geraten ins Visier der Ermittlungsbehörde, um eine Verdächtige oder einen Verdächtigen zu finden. Dass dieses Vorgehen effizient sein kann, wissen wir nicht erst seit gestern. Es hat aber auch seinen Preis. Aber auch er kann nur gezahlt werden, wenn die Rechtslage klar und unzweideutig ist. Das war aber bei diesem Sachverhalt gerade nicht der Fall. Das Beispiel zeigt, dass die Strafprozessordnung dem Erfordernis an hinreichend klaren und zeitgemäßen Eingriffsvoraussetzungen nicht mehr gerecht wird. Ähnliches gilt nämlich für den Einsatz von Staatstrojanern, der stillen SMS und von massenhaften Funkzellenabfragen. Der LfDI ist dabei, die entsprechenden Fragen mit den Justizministerien auf Bundes- und auf Landesebene zu erörtern.

7.4 Facebook

Obwohl Facebook mit seinem Firmensitz im Silicon Valley und seiner europäischen Niederlassung in Irland weit entfernt von Rheinland-Pfalz ist, was die Zuständigkeit des LfDI natürlich auch begrenzt, begleitet Facebook doch seine Arbeit wie kaum ein anderes Unternehmen. Die Frage, ob öffentliche Verwaltungen Facebook-Fanseiten nutzen dürfen, ob die Polizei auf dieser Seite öffentlich fahnden darf, ob in den Schulen Lehrerinnen und Lehrer mit ihren Schülerinnen und Schülern befreundet sein dürfen, ist in diesem Bericht gesondert im jeweiligen Kontext dargestellt. Darüber hinaus ging es im Berichtszeitraum aber auch um folgende Facebook-Themen:

7.4.1 Gesichtserkennungsfunktion

Die Datenschutzbeauftragten haben sich nachdrücklich dafür eingesetzt, dass Facebook Personenbilder nur dann biometrisch erfasst und speichert, wenn die abgebildeten Personen zuvor darin eingewilligt haben (vgl. 23. Tb., Tz. I-3.2.3). Facebook hat sich dem lange Zeit verschlossen. Einige deutsche Datenschutzbeauftragte, vor allem der hamburgische, dann aber auch der schleswig-holsteinische und der rheinland-pfälzische Datenschutzbeauftragte, hatten ein förmliches Untersagungsverfahren nach dem Bundesdatenschutzgesetz gegen Facebook eingeleitet. Die Vereinigung der europäischen Datenschutzbeauftragten (die „Art. 29-Gruppe") hat im März 2012 eine förmliche Stellungnahme verabschiedet, in der sie klar gefordert hat, Gesichtserkennungssysteme nur auf der Grundlage der informierten Einwilligung der Abgebildeten einzusetzen.

Im September 2012 ist Facebook dieser Forderung schließlich nachgekommen: Für seine europäischen Nutzerinnen und Nutzer wurde die Praxis eingestellt, wonach Bilder auch ohne jede Kenntnis der Abgebildeten biometrisch erfasst worden sind.

Dies war zwar ein wichtiger Schritt zu mehr Datenschutz bei Facebook. Allerdings ist nicht sicher, ob Facebook seine Pläne zur Nutzung der Gesichts-

erkennungsfunktion auch in Europa nicht erneut aufgreifen wird.

Im Übrigen ändert es nichts an der Tatsache, dass Facebook aufgrund der großen Unbekümmertheit seiner Mitglieder mittlerweile über mehr als 40 Milliarden Fotos verfügt, mit deren Hilfe zwischenzeitlich eine halbe Milliarde Menschen weltweit identifiziert werden konnten. Facebook verfügt also über die weltweit größte biometrische Datenbank. Die Zugriffe des amerikanischen Geheimdienstes auf die Datenbanken von Facebook haben gezeigt, wie schnell auch staatliche Stellen von solchen Datenschätzen für ihre eigenen Zwecken profitieren können.

7.4.2 Heimliche Überwachung von Chats und Nachrichten

Presseberichten zufolge setzt Facebook eine Software gegenüber den eigenen Mitgliedern ein, die in Facebook-Chats und -Nachrichten nach Anhaltspunkten für mögliche Sexualstraftaten sucht. Neben verdächtigen Formulierungen werden dazu bestimmte Aspekte in der Beziehung der beteiligten Facebook-Mitglieder (z.B. das unterschiedliche Alter der Kommunikationspartnerinnen und -partner) herangezogen.

Aus dem Umstand, dass Facebook eine solche Überwachung unter dem Gesichtspunkt möglicher Sexualstraftaten durchführt, lässt sich leicht schlussfolgern, dass eine inhaltliche Überprüfung der Chats auch aus anderen Gründen und unter anderen Gesichtspunkten erfolgt, zumindest erfolgen kann. Über die notwendigen technischen Hilfsmittel verfügt Facebook ganz offensichtlich.

Ein solches Vorgehen ist rechtswidrig. Facebook hat das Telekommunikationsgeheimnis zu wahren, das dem Diensteerbringer untersagt, sich Kenntnis vom Inhalt der Telekommunikation zu verschaffen. Facebook informiert seine Mitglieder nicht über seine entsprechenden Aktivitäten und holt erst recht nicht ihr Einverständnis für eine solche Auswertung ihrer Kommunikation ein. Völlig unklar ist auch, ob und wie lange solche ja lediglich vagen Verdachtsfälle gespeichert bleiben und an wen die Daten weitergegeben werden. Es ist zu befürchten, dass auch deutsche Facebook-Mitglieder in diese Überwachung einbezogen sind. Schriftliche Anfragen deutscher Datenschutzbeauftragter an Facebook, um das Verfahren weiter aufzuklären, sind leider erfolglos geblieben.

7.4.3 Prüfung durch den irischen Datenschutzbeauftragten

Der für die europäische Facebook-Niederlassung in Dublin zuständige irische Datenschutzbeauftragte führte im Herbst 2011 ein Audit durch. Der am 21. Dezember 2011 veröffentlichte Bericht (http://www.europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf) dokumentierte zwar einige besorgniserregende Mängel, die der irische Datenschutzbeauftragte jedoch nicht als Aussage einer fehlenden Rechtskonformität von Facebook verstanden wissen wollte. Der irische Datenschutzbeauftragte hat darauf hingewiesen, dass er im Rahmen des Audits primär einen „best practice approach“ verfolgt habe und der formelle Abschluss des Audits erst nach der Evaluation der bis Mitte des Jahres 2012 mit Facebook vereinbarten Nachbesserungen vorgesehen sei. Der Folgebericht vom 21. September 2012 (http://www.europe-v-facebook.org/ODPC_Review.pdf) benannte einige Verbesserungen und bestätigte im Übrigen die vorläufig gewonnenen Erkenntnisse.

Die in den Berichten beschriebenen Mängel sowie die dort wiedergegebenen Einlassungen Facebooks belegen aus der Sicht des LfDI, dass Facebook häufig hinter anerkannten Datenschutzstandards zurückbleibt. Insbesondere in Bezug auf die Sammlung der Daten von Nicht-Facebook-Mitgliedern und bezüglich der Facebook-Gesichtserkennung vertreten deutsche Datenschutzbeauftragte eine andere Rechtsauffassung als ihr irischer Kollege. Auch erscheint die Vorgehensweise, nur nach dem „Prinzip Hoffnung“ auf Verbesserungen hinzuwirken, ohne wegen deutlicher Rechtsverstöße Sanktionsmittel einzusetzen („best practice approach“), fragwürdig.

Derzeit verfolgt die Studentenorganisation „europe versus facebook“ ihr Anliegen, Facebook zu zwingen, sich an europäisches Datenschutzrecht zu halten, auf dem Rechtsweg in Irland weiter.

7.4.4 Facebook-Fanpages von Behörden

Bei den von Facebook unter der Bezeichnung „Seiten“ oder „Fanpages“ angebotenen Funktionen handelt es sich um Informations- und Kommunikationsdienste, die hinsichtlich ihrer Gestaltung und Funktionalität in weiten Teilen dem Betrieb eines Internetangebots vergleichbar sind. Sie unterfallen damit den Regelungen des Telemediengesetzes; die Pflicht zur Einhaltung der diesbezüglichen datenschutzrechtlichen Anforderungen trifft die jeweilige fanpagebetreibende Stelle.

In der durch Facebook gegenwärtig angebotenen Form ist der Einsatz von Fanpages durch öffentliche Stellen aus datenschutzrechtlicher Sicht mit deutschem Datenschutzrecht (insbesondere dem Telemediengesetz) grundsätzlich nicht vereinbar.

Kernpunkte der datenschutzrechtlichen Kritik an der gegenwärtigen Konzeption der Facebook-Fanpage-Funktion sind die fehlende Widerspruchsmöglichkeit gegen die Verarbeitung von Nutzungsdaten und deren weitere Verwendung in personenbezogener Form, z.B. für personalisierte Werbung.

Der Besuch von Fanpages führt automatisch dazu, dass von den Besucherinnen und Besuchern dieser Seiten Nutzungsdaten erhoben und von Facebook gespeichert und verarbeitet werden. Dazu gehören der Zeitpunkt des Besuches, ggf. das zuvor besuchte Internetangebot und die Facebook bezogene Form der interaktiven Nutzung der entsprechenden Seiten (z.B. Nutzung von Like Buttons und Share Buttons, Kommentierungen, Post, Dokumentenuploads), so dass auf diese Weise sog. Nutzerprofile i.S. von § 15 Abs. 3 TMG entstehen. Diese werden, soweit es sich um angemeldete Nutzerinnen und Nutzer des Netzwerkes handelt, mit demografischen Angaben wie Alter, Geschlecht und Herkunft verknüpft. Mit der Erstellung und dem Betrieb einer Fanpage geht insoweit auch die Beauftragung einer Nutzungsanalyse nach § 15 Abs. 3 TMG einher.

Für Facebook sind diese Nutzungsprofile, soweit es sich bei den Seitenbesucherinnen und -besuchern um angemeldete Facebook-Mitglieder handelt, personenbezogen, während die Betreiber der Fanpages diese Profile nur in aggregierter Form über den Facebook-Statistikdienst „Insights“ erhalten.

Diese Nutzungsdaten werden an Facebook übermittelt, bevor die Betroffenen darüber informiert werden können. Ein entsprechendes Widerspruchsrecht der Nutzerinnen und Nutzer (vgl. § 15 Abs. 3 TMG) ist von Facebook beim Betrieb seiner Fanpages nicht vorgesehen. Aus diesen Gründen hält der LfDI den Betrieb von Fanpages durch öffentliche Stellen für datenschutzrechtlich problematisch. Die Möglichkeit einer umfassenden Einwilligung in die von Facebook vorgegebene Form der Verarbeitung (vgl. § 12 TMG) scheitert an der unzureichenden Information der Nutzerinnen und Nutzer über Art und Umfang der Datenverarbeitung durch Facebook. Die bestehenden Defizite müssen ggf. durch eine geeignete Unterrichtung auf der jeweiligen Fanpage selbst ausgeglichen werden. Auf der anderen Seite ist das berechtigte Interesse der Verwaltungen zu sehen, kostengünstig und schnell Bürgerinnen und Bürger und insbesondere bestimmte Zielgruppen zu informieren, die auf anderen Wegen möglicherweise nicht in vergleichbarem Umfang zu erreichen sind.

Bei einer vom LfDI im Bereich der Landes- und Kommunalverwaltung sowie der Hochschulen Mitte 2012 durchgeführten Erhebung zeigte sich, dass Facebook-Fanpages in der Landesverwaltung nur in sehr überschaubarem Umfang genutzt wurden. Deutlich öfter war dies bei den Kommunen der Fall, von denen ca. 40 Prozent über einen Facebook-Auftritt verfügten; an den Hochschulen wurden Facebook-Seiten durchgängig genutzt.

Die Schwerpunkte dieser Seite lagen in den Bereichen Öffentlichkeitsarbeit, Tourismus, Kultur, Stadt-/Hochschulmarketing, Nachwuchsgewinnung und Jugendpflege. Als Gründe für die Nutzung von Fanpages wurden überwiegend Image-Überlegungen, Wettbewerbsdruck, Bürgererwartungen, die Reichweite der Informationsangebote und die bestehenden Möglichkeiten einer zielgruppenorientierten Ansprache genannt.

Aus Sicht des LfDI ist jedoch darauf hinzuweisen, dass der Staat, seine Organe und seine Amtsträger Facebook nicht in gleicher Weise nutzen dürfen wie Bürgerinnen und Bürger. Diese sind in ihrer Handlungsweise frei, ihr informationelles Selbstbestimmungsrecht erlaubt es ihnen, Facebook zu nutzen oder davon Abstand zu nehmen. Der Staat hingegen hat kein entsprechendes Grundrecht. Im

Gegenteil: Er ist an die Grundrechte gebunden und hat die Gesetze zu beachten, auch und gerade dann, wenn er Facebook nutzen möchte. Diese Gesetze schränken ihn ein, auch wenn dies nicht jedermann wahrhaben möchte.

Nach wie vor sind allerdings wesentliche Rechtsfragen im Zusammenhang mit Facebook und der Nutzung von Fanpages ungeklärt. Die vorliegenden Urteile aus anhängigen Gerichtsverfahren betreffen entweder Sachverhalte, die für diese Frage nicht von Bedeutung sind, oder wurden mit Rechtsmitteln angegangen.

Facebook hat zwei Seiten: die eine Seite ist Ausdruck der Informationsgesellschaft und bringt diese auch voran. Die andere Seite bedroht die Privatsphäre und damit letztlich auch die Würde der Menschen. Daraus ergibt sich ein Schutzauftrag für den Staat. Diesen Auftrag muss der Staat auch bei der Nutzung von Facebook im Allgemeinen und bei der Einrichtung von Facebook-Fanseiten im Besonderen beachten.

Die Umfrage des LfDI hat gezeigt, dass bezüglich einschlägiger Datenschutzfragen jedes Problembewusstsein und in vielen Fällen die notwendige Sensibilität fehlte. Folglich gab es bereits gravierende Defizite bei datenschutzrechtlichen Selbstverständlichkeiten: Insbesondere war die Information der Nutzerinnen und Nutzer über Art und Umfang der Datenverarbeitung (im Rahmen von Datenschutzerklärungen) unzureichend oder fehlte ganz, auch Angaben über die für das Angebot verantwortliche Stelle waren häufig nicht vorhanden (Verstoß gegen die Impressumspflicht).

Am Beispiel der von der Staatskanzlei betriebenen Facebook-Fanseite hat der LfDI Rahmenbedingungen formuliert, unter denen der Betrieb einer Fanpage noch hingenommen werden kann. Diese umfassen u.a.

- die Information der Nutzerinnen und Nutzer,
- die Verringerung von Nutzungsdaten,
- Hinweise für die Nutzerinnen und Nutzer auf Möglichkeiten des Selbstdatenschutzes,
- die Förderung datenschutzfreundlicher Plattformen im Internet.

Ziel ist es dabei, in der ungeklärten rechtlichen Situation anerkannte Datenschutzstandards auch beim Einsatz von Facebook-Fanpages so weit wie möglich wirksam werden zu lassen.

So sieht der LfDI bei Fanpages, die den nachfolgenden Punkten entsprechen, und solange wesentliche Rechtsfragen gerichtlich nicht abschließend geklärt sind, von einem aufsichtsrechtlichen Einschreiten ab:

1. Erforderlichkeitsprüfung

Eine Fanpage auf Facebook sollte nur dann eingerichtet werden, wenn eine Prüfung ergeben hat, dass ohne eine solche Facebook-Präsenz der Verwaltung erhebliche Nachteile drohen bzw. ihre Aufgabenerfüllung ernsthaft beeinträchtigt wäre.

2. Kein Einsatz von Fanpages in den Kernbereichen der Verwaltung

Fanpages kommen nur als Informationsmedium zur Verstärkung der Reichweite kommunaler Informationsangebote insbesondere in den Bereichen Kultur/Veranstaltungen, Tourismus oder Stadtmarketing in Betracht. In Kernbereichen der hoheitlichen oder Leistungsverwaltung (z.B. Ordnungsverwaltung, Sozialverwaltung, Finanzverwaltung) sind Fanpages, die mehr als allgemeine Informationen (z.B. Öffnungszeiten, Ansprechpartner, Kontaktdaten) enthalten, nicht zulässig.

3. Transparenz für die Bürgerinnen und Bürger muss oberstes Gebot sein

Die Bürgerinnen und Bürger sind von der Verwaltung als Anbieter einer Fanpage darüber aufzuklären, welche Gefährdungen ihres Persönlichkeitsrechts durch Facebook bestehen, wenn sie eine gemeindliche Fanpage aufrufen. Zu diesem Zweck ist über die Eingangsseite der Fanpage ein Datenschutzhinweis entsprechend des nachfolgenden Musters (vgl. Kasten „Datenschutzhinweise für den Betrieb einer Facebook-Fanpage“) verfügbar zu machen. Dieser ist individuell anzupassen, wenn besondere Bedingungen bestehen. Auf der Fanpage sollten weiterhin Links zu Webseiten vorhanden sein, die die Datenschutzgefahren von Facebook, die Funktionsweise von Like Buttons und von Facebook-„Insight“ erläutern.

4. Impressum

Wenn eine Verwaltung eine Fanpage betreibt, muss für Besucherinnen und Besucher leicht erkennbar sein, dass sie sich auf einer offiziellen Seite befinden, für die eine öffentliche Stelle die Verantwortung trägt. Es muss auch erkennbar sein, wie diese Stelle schnell und unkompliziert zu erreichen ist (Adresse, Telefonnummer, E-Mail-adresse). Inhaltlich müssen diese Hinweise den Vorgaben aus § 5 TMG entsprechen. Die unmittelbare Erkennbarkeit und leichte Erreichbarkeit ist gegeben, wenn ein entsprechender Hinweis prominent platziert ist, z.B. auf der Hauptseite der Fanpage oder im standardmäßig vorgesehenen Infobereich, und die Informationen nach max. zwei Klicks zur Verfügung stehen.

5. Fanpages primär als Brücke zum Internetangebot der Verwaltung

Aufgrund der eingangs genannten Probleme sollen Inhalte und Funktionen einer Fanpage beschränkt werden, um eine datenschutzrechtlich fragwürdige Verarbeitung von Nutzungsdaten nicht von öffentlicher Seite aus zu initiieren oder zu fördern. Facebook erfährt über die Nutzerinnen und Nutzer und deren Nutzungsverhalten umso mehr, je vielfältiger die Inhalte sind bzw. in Anspruch genommen werden. Dann besteht eine erhöhte Wahrscheinlichkeit, dass die interaktiven Elemente (der Like Button; das Teilen von Informationen etc.) verstärkt genutzt werden. Es sollen keine interaktiven Funktionen vorhanden sein, die über die standardmäßig vorhandenen, nicht abschaltbaren Fanpage-Funktionen (Gefällt mir, Kommentieren, Teilen) hinausgehen. Die primäre Funktion einer Fanpage sollte darin liegen, die Nutzerinnen und Nutzer auf das jeweilige Internetangebot zu führen (Überleitungs- oder Brückenfunktion).

6. Ausgeschlossene Bereiche

Eine Fanpage darf keinesfalls dazu genutzt werden, dass Bürgerinnen und Bürger auf diesem Weg der Verwaltung Mitteilungen zukommen lassen. Dieser Aspekt gilt in besonderem Maß für den gesamten Sozialleistungsbereich einschließlich der Kinder- und Jugendhilfe. Die Betreuten dürfen nicht veranlasst werden, über Facebook gemeindliche Hilfen einzufordern. Die Verwaltung sollte alles tun, um solche Nutzungen zurückzudrängen. Auf der Fanpage ist daher darauf hinzuweisen, dass für die Kommunikation mit der Verwaltung die hierfür allgemein vorgesehenen Wege (Telefon/Telefax, Postweg, E-Mail) oder die ggf. auf der Internetseite angebotenen Funktionen zu nutzen sind.

7. Förderung datenschutzfreundlicher Netzwerke

Es sollte das Ziel aller öffentlichen Stellen sein, datenschutzfreundliche Netzwerke zu fördern (vgl. die entsprechende Forderung aus dem Projekt „Jugendforum“ der Staatskanzlei). Zu diesen gehören vor allem die Netzwerke „Diaspora“ und „Friendica“ (vgl. http://www.youngdata.de/facebook/alternativen/). Jede Facebook-Präsenz sollte also von einem vergleichbaren Angebot auf diesen Netzwerken begleitet sein, um zum Einen das datenschutzpolitische Signal zu geben, dass datenschutzfreundliche Facebook-Alternativen unterstützt werden, und um auch unter Wettbewerbsgesichtspunkten nicht einseitig die bzw. den Falschen zu fördern.

Aus Sicht des LfDI ist dieser Kompromiss jedenfalls so lange akzeptabel, bis die Gerichte in einer unübersichtlichen Rechtslage für die nötige Klarheit gesorgt haben.

Datenschutzhinweise für den Betrieb einer Facebook-Fanpage (Muster)

Beim Besuch dieser Seite erfasst Facebook u.a Ihre IP-Adresse sowie weitere Informationen, die in Form von Cookies auf Ihrem PC vorhanden sind. Diese Informationen werden verwendet, um der (Kommune XY) als Betreiber der Facebook-Seiten statistische Informationen über die Inanspruchnahme ihrer Seiten zur Verfügung zu stellen. Nähere Informationen hierzu stellt Facebook unter folgendem Link zur Verfügung: http://de-de.facebook.com/help/pages/insights.

Welche Informationen Facebook erhält und wie diese verwendet werden, beschreibt Facebook in allgemeiner Form in seinen Datenverwendungsrichtlinien. Diese sind unter folgendem Link verfügbar: http://de-de.facebook.com/about/privacy

In welcher Weise Facebook die Daten aus dem Besuch von Facebook-Seiten konkret für eigene Zwecke verwendet, in welchem Umfang Aktivitäten auf der

Fanpage einzelnen Nutzern zugeordnet werden, wie lange Facebook diese Daten speichert und ob Daten aus einem Besuch der Fanpage an Dritte weitergegeben werden, wird von Facebook nicht abschließend und klar benannt und ist uns nicht bekannt.

Die IP-Adresse wird nach Auskunft von Facebook ausschließlich für statistische Zwecke verwendet, anonymisiert (bei „deutschen" IP-Adressen) und nach 90 Tagen gelöscht.

Wenn Sie als Nutzerin oder Nutzer aktuell bei Facebook angemeldet sind, befindet sich auf Ihrem PC ein Cookie mit Ihrer Facebook-Kennung. Dadurch ist Facebook in der Lage nachzuvollziehen, dass Sie diese Seite aufgesucht und wie Sie sie genutzt haben. Dies gilt auch für alle anderen Facebook-Seiten, die Sie besuchen.

Wenn Sie dies vermeiden möchten, sollten Sie sich bei Facebook abmelden bzw. die Funktion „angemeldet bleiben" deaktivieren, die auf Ihrem Gerät vorhandenen Cookies löschen und Ihren Browser beenden und neu starten. Auf diese Weise werden alle Facebook-Informationen, über die Sie identifiziert werden können, gelöscht. Damit können Sie unsere Facebook-Seite anonym nutzen. Wenn Sie auf interaktive Funktionen der Seite zugreifen (Gefällt mir, Kommentieren, Teilen, Nachrichten etc.), erscheint eine Facebook-Anmeldemaske. Nach einer etwaigen Anmeldung sind Sie für Facebook erneut als Nutzerin/Nutzer erkennbar.

Sie können sich selbstverständlich über die Angebote und Leistungen der (Kommune XY) auch auf deren Internet-Seite informieren. In diesem Fall erhält Facebook keinerlei Informationen. Unser Internet-Angebot finden Sie unter folgender Adresse:

http://www....

Datenschutzaspekte von Facebook-Fanpages

- 23. Tb., Tz. I-3.2.2: http://www.datenschutz.rlp.de/downloads/tb/tb23.pdf
- FAQ „Dürfen Verwaltungen Facebook-Seiten betreiben?": http://www.datenschutz.rlp.de/downloads/misc/FAQ_Facebook-Seiten.pdf
- Arbeitspapier „Facebook-Reichweitenanalyse" des ULD Schleswig-Holstein: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf
- Gutachten „Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook-Fanpages und Social-Plugins" des wissenschaftlichen Dienstes des Deutschen Bundestages: https://www.datenschutzzentrum.de/facebook/material/WissDienst-BT-Facebook-ULD.pdf

Der LfDI hat anlässlich des Presserechtsforums 2013 am 19. Juni 2013 in Frankfurt die wesentlichen datenschutzrechtlichen Kritikpunkte zu Facebook in seiner Rede „Dauerstreit Facebook – Was dürfen Medien, Behörden und Unternehmen noch?" dargestellt (http://www.datenschutz.rlp.de/de/service/reden/20130619_lfdi_-_Rede_Frankfurt.pdf).

7.5 Mit sieben Siegeln: Die AGBs der Internetriesen

Wer bei Amazon oder Ebay kauft, wer bei Facebook Mitglied ist, wer Google nutzt, sollte wissen, was AGBs sind: Es sind die Allgemeinen Geschäftsbedingungen der Unternehmen. Darin steht, welche Rechte und Pflichten die Nutzerinnen und Nutzer diesen Unternehmen gegenüber haben. Dennoch kennt sie kaum jemand. Das hat verschiedene Gründe. Sie liegen häufig in der Verantwortung der Unternehmen:

Die Internetgroßunternehmen (z.B. Microsoft, Facebook, Google, Apple) zeichnen sich dadurch aus, dass sie eine Vielzahl von Diensten anbieten und einen fast noch größeren Erfindungsreichtum zeigen, wenn es um das Formulieren und Verstecken von AGB-Regelungen geht. AGB-Regeln, die sich mit der Verarbeitung von Kundendaten befassen, erscheinen unter ganz unterschiedlichen Namen, darunter „Privacy Policy", also „Datenschutzerklärung". Microsoft z.B. hat mindestens zehn verschiedene Regelwerke, die unter unterschiedlichen Namen an unterschiedlichen Stellen Bestimmungen zum Umgang mit diesen Daten enthalten. Fast niemand findet diese Regeln. Wenn man sie gefunden hat, sind sie zudem unklar. Man

weiß nicht, für welchen Dienst sie gelten und für welchen nicht; nur selten enthalten sie deutliche Formulierungen.

AGBs sind aber dennoch wichtig. Wenn die Nutzerinnen und Nutzer sich mit einem Anliegen an den Internetdienst wenden – vielleicht, um Auskunft darüber zu erhalten, was sie über einen selbst gespeichert haben –, dann berufen sich die Unternehmen auf ihre AGBs.

Immer wieder stellen Bürgerinnen und Bürger auch Fragen an den LfDI, die unter Hinweis auf die AGBs der betroffenen Unternehmen zu beantworten sind. Dabei werden häufig die datenschutzrechtlichen Defizite und Unklarheiten solcher Regelungen deutlich.

Die Verbraucherschutzverbände können vor Gericht gegen Regeln in den AGBs klagen, wenn diese die Nutzerinteressen zu sehr außer Acht lassen. So waren die Verbraucherschützer schon gegen bestimmte Regelungen in den AGBs von Apple, Facebook und Samsung erfolgreich, wie die folgenden Pressemitteilungen der Verbraucherzentrale dokumentieren:

- „Samsung-App-Store: Viele AGB-Klauseln unzulässig“ vom 6. Januar 2013, http://www.vzbv.de/11854.htm
- „Datenklauseln von Apple sind unzulässig“ vom 7. Mai 2013, http://www.vzbv.de/11558.htm
- „vzbv mahnt erneut Facebook ab – App-Zentrum von Facebook erfragt keine Einwilligung zur Weitergabe von Daten“ vom 27. August 2012, http://www.vzbv.de/10146.htm
- „vzbv gewinnt Klage gegen Facebook – Richter erklären Freundefinder und Geschäftsbedingungen für rechtswidrig“, vom 6. März 2012, http://www.vzbv.de/8981.htm

Aber auch die Datenschutzaufsichtsbehörden bemühen sich, datenschutzwidrige AGBs der Datenkraken zu revidieren. Derzeit wird versucht, die AGBs von Google und von Microsoft datenschutzgerechter zu machen (Presseerklärung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, http://www.datenschutz-hamburg.de/news/detail/article/privatsphaere-bestimmungen-von-google-auf-dem-pruefstand-1.html?tx_ttnews[backPid]=1&cHash=bb137b3ed9d122da2135eab01246fd50).

In Bezug auf Microsoft ist die Vereinigung der europäischen Datenschutzbeauftragten aktiv, um Verbesserungen zu erreichen.

Die französische Datenschutzbehörde hat Google wegen seiner datenschutzwidrigen AGBs im Januar 2014 zu einer Geldstrafe von 150.000 Euro verurteilt. Außerdem musste die Suchmaschine auf ihrer französischen Startseite für 48 Stunden folgende Information einblenden:

„Bekanntmachung: Der Sanktionen-Ausschuss der Französischen Datenschutzaufsichtsbehörde (CNIL) hat das Unternehmen Google zu einer Geldstrafe von 150.000 Euro wegen des Verstoßes gegen die Datenschutzbestimmungen des Datenschutzgesetzes verurteilt. Diese Entscheidung ist abrufbar unter: http://www.cnil.fr/linstitution/missions/sanctionner/Google/“

Google hatte versucht, die Auflage, eine Information über seine eigene Verurteilung einzublenden, aus dem Urteil streichen zu lassen. Man hätte sogar – wie Presseberichten zu entnehmen ist – eine höhere Geldstrafe in Kauf genommen, um den Imageschaden abzuwenden. Dieser Versuch ist gescheitert.

Allerdings hat das Gericht über die Verhängung der Geldbuße noch nicht entschieden.

Die Datenschutzbehörden in Europa sind einhellig der Auffassung, dass die Vereinheitlichung der Datenschutzbestimmungen, die Google im März 2012 vorgenommen hatte, gegen das Datenschutzrecht verstößt. Danach kann das Unternehmen in verschiedenen Diensten wie „Gmail“, „Youtube“ oder „Google+“ Nutzerdaten sammeln, kombinieren und weiterverwenden. Google hält dies ebenso wie die dazugehörigen Datenschutzerklärungen für rechtmäßig und hat sich bislang geweigert, datenschutzgerechte Änderungen vorzunehmen.

In Deutschland werden derzeit entsprechende Sanktionen vorbereitet (http://www.datenschutz-hamburg.de/news/detail/article/privatsphaere-bestimmungen-von-google-auf-dem-pruefstand-1.html?tx_ttnews%5BbackPid%5D=1&cHash=bb137

b3ed9d122da2135eab01246fd50). Auch der LfDI wird sich darum bemühen, Google zu einem Einlenken zu bewegen.

7.6 Datenschutz im Anti-Doping-System

Mit dem sehr sensiblen Thema „Datenschutz und Anti-Doping-System“ hat sich der LfDI bereits im letzten Tätigkeitsbericht ausführlich auseinander gesetzt (vgl. 23. Tb., Tz. II- 2.4). Eine Reihe von Spitzensportlerinnen und -sportlern hatte sich im Herbst 2010 an den LfDI mit der Bitte gewandt, sie bei der Wahrung ihrer Persönlichkeitsrechte mit Blick auf Anti-Doping-Kontrollmaßnahmen zu unterstützen. Ihre Unterwerfung unter den Nationalen Anti-Doping-Code der Anti-Doping-Agentur Deutschland (NADA) führe zu einer nicht hinnehmbare Verletzung ihrer Intim- und Privatsphäre.

Die umfangreiche Stellungnahme des LfDI zur Anti-Doping-Kontrollpraxis und zum Nationalen Anti-Doping-Code führte zu einer breiten öffentlichen Debatte über die Angemessenheit der aktuellen Kontrollmaßnahmen, die bis in den Sportausschuss des Deutschen Bundestages hineingetragen wurde. In einer parlamentarischen Anhörung im Oktober 2011 konnte der LfDI seine bisherige Kritik am Doping-Kontrollsystem der NADA erläutern. Er verwies dabei auf die besondere Problematik, dass es sich beim Doping-Kontrollsystem wegen des bestimmenden finanziellen und strukturellen Einflusses des Bundesinnenministeriums auf die NADA um ein „quasistaatliches Überwachungssystem“ handele.

Hierzu führte der LfDI vor dem Bundestag aus: „Die Grundrechte und das deutsche Datenschutzrecht gelten nicht nach Belieben internationaler Organisationen wie der Welt-Anti-Doping-Agentur (WADA), sondern unbedingt. Auch Sportler sind daher keine Grundrechtsträger zweiter Klasse.“

Zwischenzeitlich sind die Bemühungen der Datenschützerinnen und Datenschützer, die Situation der Sportlerinnen und Sportler im Rahmen der Novellierung des WADA-Codes zu verbessern, ergebnislos geblieben. Die Hoffnung, die hohen deutschen und europäischen Datenschutz-Standards in weltweit gültige Sportregelungen zu implementieren, wurde enttäuscht.

Erst in jüngster Zeit gibt es wieder Grund für vorsichtigen Optimismus: Zum einen hat das Landgericht München mit seiner Entscheidung im Schadensersatzprozess der Eisschnellläuferin Claudia Pechstein das weltweite Sportrechtssystem ins Wanken gebracht. Das Landgericht München I erklärte die Schiedsklausel der Athletenvereinbarung zwischen Verbänden und Athletinnen und Athleten im Falle der fünfmaligen Eisschnelllauf-Olympiasiegerin im Februar 2014 für unwirksam. Dies stützt ganz wesentlich die Rechtsauffassung des LfDI, dass sich Anti-Doping-Kontrollmaßnahmen nicht auf Einwilligungserklärungen der Sportlerinnen und Sportler stützen können (Urteil vom 26. Februar 2014, Az. 37 O 28331/12). Eine freie Entscheidung der Betroffenen im Sinne von § 4a Abs. 1 Satz 1 BDSG, sich dem Kontrollsystem zu unterwerfen, liegt – nach dem Maßstab des LG München – nicht vor. Im Rahmen der beruflichen Betätigung als Profisportlerin oder -sportler hängt ihre berufliche Existenz davon ab, bei nationalen oder internationalen Wettkämpfen startberechtigt zu sein. Die Erteilung einer solchen Startberechtigung wird über die beteiligten Vereine bzw. Sportfachverbände von der Unterwerfung unter den Nationalen Anti-Doping-Code abhängig gemacht; die Verweigerung der Teilnahme am internationalen Anti-Doping-Kampf führt notwendig zum Ausschluss von Veranstaltungen im Sportbereich und kommt damit im Ergebnis einem Berufsverbot gleich.

Damit ist erstmals – zumindest mittelbar – gerichtlich bestätigt worden, dass Unterwerfungserklärungen von Athletinnen und Athleten keine wirksame Grundlage von Kontrollmaßnahmen sein können.

Mangels wirksamer Einwilligung sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Anti-Doping-Organisationen damit nur zulässig, soweit sie durch das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift ausdrücklich erlaubt sind. Dieses Bundesdatenschutzgesetz kennt jedenfalls keine solche Erlaubnisnorm.

An dieser Stelle ist allerdings Bewegung in die bisher festgefahrene Debatte um ein Anti-Doping-Gesetz gekommen – ein weiterer Grund zur Hoff-

nung. Hatten insbesondere die Sportverbände bislang eine solche gesetzliche Regelung als Eingriff in die „Selbstregulierung des Sports“ abgelehnt, mehren sich die Stimmen, ein solches Gesetzgebungsverfahren einzuleiten. Im aktuellen Koalitionsvertrag von CDU, CSU und SPD findet sich erstmals die Feststellung:

„Deshalb werden wir weitergehende strafrechtliche Regelungen beim Kampf gegen Doping und Spielmanipulation schaffen. Dazu kommen auch Vorschriften zur uneingeschränkten Besitzstrafbarkeit von Dopingmitteln zum Zweck des Dopings im Sport sowie zum Schutz der Integrität des sportlichen Wettbewerbs in Betracht.“

Im November 2013 folgten dieser Initiative auch die Länder, der Bundesrat beschloss, den Gesetzentwurf von Baden-Württemberg „zur Verbesserung der strafrechtlichen Doping-Bekämpfung“ in den Bundestag einzubringen.

Auch von Seiten des Deutschen Olympischen Sportbundes kommen erste Signale, ein solches Gesetz nicht mehr grundsätzlich abzulehnen. Im Dezember 2013 sprach sich etwa Turn-Präsident Rainer Brechtken, Sprecher der Spitzenverbände im Deutschen Olympischen Sportbund, für die Strafverfolgung von dopenden Athletinnen und Athleten aus.

Für das Anliegen der Datenschützerinnen und Datenschützer könnte sich so die Chance eröffnen, in eine gesetzliche Regelung des Anti-Doping-Kampfs auch Schutzvorschriften zugunsten des informationellen Selbstbestimmungsrechts der Sportlerinnen und Sportler zu integrieren. Dies hatte der LfDI in der Vergangenheit bereits wiederholt verlangt. Ein Anti-Doping-Gesetz ohne entsprechende Einschränkung von Verfolgungsmöglichkeiten wäre jedenfalls offenkundig verfassungswidrig und hätte vor dem Bundesverfassungsgericht keinen Bestand.

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

1. Medien und Telekommunikation

1.1 Nutzung privater E-Mailpostfächer für dienstliche Zwecke

Eine pauschale Weiterleitung dienstlicher E-Mails auf private E-Mailkonten von Bediensteten ist grundsätzlich nicht zulässig. Die Art privater E-Mail-lösungen und die dabei bestehenden Zugriffsmöglichkeiten sind höchst unterschiedlich und entziehen sich in aller Regel der Beurteilung und Einflussnahme des Dienstherrn sowie in Teilen auch der Inhaberinnen und Inhaber der privaten Postfächer. Aus Sicht des LfDI kann damit der nach § 9 Abs. 2 Nr. 4 LDSG geforderte Schutz vor unbefugter Kenntnisnahme nicht verlässlich sichergestellt werden (vgl. 20. Tb., Tz. 21.3.1).

Die Nutzung privater E-Mailkonten von Beschäftigten mit dem Ziel, außerhalb der Dienstzeit oder auf Dienstreisen einen Zugriff auf dienstliche Unterlagen zu eröffnen, begegnet damit datenschutzrechtlichen Bedenken. Soweit entsprechende Anforderungen bestehen, sollte hierfür stattdessen ein gesicherter externer Zugriff auf die dienstlichen Postfächer eingerichtet werden (VPN-Zugang, Terminal-Server-Lösung etc.).

In begründeten Einzelfällen mag die Nutzung privater E-Mailpostfächer fallweise erforderlich sein, etwa bei unvermuteter Abwesenheit und Dringlichkeit einer Rückantwort. Dies muss jedoch auf Ausnahmefälle beschränkt bleiben und darf nicht als allgemeine Form der dienstlichen Kommunikation zugelassen werden. Soweit personenbezogene Daten betroffen sind, sind dabei angemessene Schutzvorkehrungen zur Wahrung der Vertraulichkeit zu treffen (z.B. Verschlüsselung der betroffenen Dokumente).

Die Weiterleitung von Nachrichten ohne Personenbezug ist aus datenschutzrechtlicher Sicht grundsätzlich unbedenklich, es bestehen jedoch Zweifel, ob bei einer routinemäßigen Nutzung in der Praxis eine entsprechende Abschätzung und Differenzierung vorgenommen wird und entsprechende Vorkehrungen getroffen werden.

Im Rahmen einer allgemeinen Regelung sollten damit folgende Punkte berücksichtigt werden:

- Eine pauschale Weiterleitung dienstlicher E-Mails auf private E-Mailkonten von Bediensteten ist grundsätzlich nicht zugelassen; eingehende Nachrichten sind bei Abwesenheit zunächst entsprechend der bestehenden Vertretungsregelungen weiterzuleiten.
- Die Weiterleitung dienstlicher E-Mails zu privaten E-Mailadressen ist nur im Ausnahmefall zulässig und nur, wenn dies aus sachlichen und zeitlichen Gründen zwingend geboten ist. Derartige Ausnahmen bedürfen der Genehmigung.
- Soweit personenbezogene Daten betroffen sind, sind geeignete Maßnahmen zur Wahrung der Vetraulichkeit und Integrität der Daten zu treffen (Verschlüsselung). Für Unterlagen, die im öffentlichen Interesse geheimhaltungsbedürftig sind (Verschlusssachen) gelten die Anforderungen der Verschlusssachenanweisung.
- Die genutzten privaten E-Mailkonten dürfen nur im Zugriff von Beschäftigten der Verwaltung stehen; ein Zugriff weiterer Nutzerinnen und Nutzer (z.B. von Familienmitgliedern) muss ausgeschlossen sein.
- Die weitergeleiteten dienstlichen Nachrichten sind, wenn ihre Speicherung nicht mehr erforderlich ist, unverzüglich zu löschen.

1.2 Public Cloud-Angebote für die Landesverwaltung

Das Cloud Computing hält Einspar- und Effektivitätspotentiale bereit, die auch von Verwaltungen genutzt werden wollen. Der Landesbetrieb Daten und Information (LDI) stellt daher Überlegungen zu künftigen Angeboten von Cloud-Leistungen für die Landesverwaltung an. Angesichts der bestehenden Rahmenbedingungen sowie der beobachtbaren technischen und Marktentwicklung bedarf es nach Einschätzung des LfDI bei Cloud-Leistungen des LDI künftig einer differenzierten Betrachtung.

In der gegenwärtigen Situation profitiert jedes beim LDI betriebene Verfahren von der Sicherheitsinfra-

struktur des rlp-Netzes und dem Sicherheitskonzept des LDI für den Rechenzentrumsbetrieb, auch wenn der Schutzbedarf eines Verfahrens dieses Schutzniveau im Einzelfall nicht erfordern sollte. So begrüßenswert dies aus Sicht des LfDI ist, da es die Verwaltungen in weiten Teilen davon entbindet, ein verfahrensspezifisches Sicherheitskonzept zu erstellen, ist nicht zu verkennen, dass Kostenentwicklungen es erforderlich machen, über ergänzende Angebote nachzudenken. Dies gilt insbesondere dort, wo geringere Anforderungen an die Verfügbarkeit und Integrität von Daten und Funktionalitäten bestehen. Naturgemäß treten bei Verfahren, die keinen Personenbezug und damit vielfach keine besonderen Vertraulichkeitsanforderungen haben, Datenschutzüberlegungen in den Hintergrund. Da in jedem Fall aber Nutzungsdaten entstehen, bleiben auch solche Verfahren nicht gänzlich frei von datenschutzrechtlichen Anforderungen.

Soweit neben den Private Cloud-Leistungen des LDI, bei denen die Kontrolle über die IT-Struktur vollständig in dessen Händen liegt, künftig mit Hilfe eines externen Dienstleisters abgestufte Public Cloud-Leistungen angeboten werden sollen, ist dies aus Sicht des LfDI an die nachfolgend genannten Voraussetzungen zu knüpfen. Verfahren nach § 4 Abs. 4 Satz 2 LDSG, d.h. solche, bei denen Berufs- oder besondere Amtsgeheimnisse betroffen sind, oder die einen Betrieb in hoheitlicher Hand erfordern, sind von diesen Überlegungen allerdings grundsätzlich ausgenommen; diese sollten im Regelfall in der direkten Obhut des LDI betrieben werden.

- Für die Kunden des LDI muss erkennbar sein, wie sich die einzelnen Leistungskategorien hinsichtlich ihres Datenschutz- und Sicherheitsniveaus unterscheiden, damit eine am jeweiligen Schutzbedarf des Verfahrens orientierte Auswahl getroffen werden kann. Von Bedeutung sind hier insbesondere Service Level (Verfügbarkeit, Reaktionszeiten), Update- und Patchmanagement, Betriebssystemhärtung, Sicherheitsüberprüfungen des IT-Personals, Exklusivität der genutzten IT-Struktur, Servermonitoring/Logging sowie die infrastrukturellen Sicherheitsleistungen des LDI (Netz- und Firewallstruktur, Intrusion Detection System, Virenschutz, räumliche und organisatorische Sicherheit). Hier muss deutlich werden, wo im Vergleich zu den LDI-Leistungen nach unten ausgewichen wird. Ziel ist es dabei zu vermeiden, dass Auftragsentscheidungen allein unter Kostengesichtspunkten getroffen werden. Die Konsequenzen einer Entscheidung für ein anderes – niedrigeres – Sicherheitsniveau müssen transparent gemacht werden.
- Von Ausnahmefällen abgesehen, haben die Verfahren der Verwaltung einen mindestens normalen, d.h. niedrigen bis mittleren Schutzbedarf. Anbieter müssen daher nachweisen, dass sie über ein dokumentiertes Sicherheitskonzept verfügen, das an den Vorgaben der Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik orientiert ist. Dessen Umsetzung sollte durch Testate unabhängiger Stellen regelmäßig (vgl. § 4 Abs. 2 Satz 2 Nr. 3 und Satz 5 LDSG) belegt werden. Insoweit bestehende Kontrollpflichten des Auftraggebers (hier der LDI im Verhältnis zum Dienstleister) können in weiten Teilen durch geeignete Testate ersetzt werden; je nach Art und Umfang der Datenverarbeitungen sollte dies allerdings durch eine Prüfung vor Ort ergänzt werden, um das vereinbarte Sicherheitsniveau gegenüber den Auftraggebern des LDI verlässlich vertreten zu können.
- Aus Sicht der auftraggebenden Verwaltung handelt es sich bei dem vom LDI in Anspruch genommenen Dienstleister um einen Unterauftragnehmer. Die Anforderungen zur Auftragsdatenverarbeitung in § 4 LDSG sind demgemäß auf diesen zu übertragen. Neben den bereits angesprochenen technisch-organisatorischen Maßnahmen betrifft dies insbesondere die Geltung der Regelungen des Landesdatenschutzgesetzes und die Möglichkeit einer Kontrolle durch den LfDI (vgl. § 4 Abs. 1 Satz 3 LDSG).
  Dies zieht es nach sich, dass mit dem Dienstleister des LDI vertraglich vereinbart wird, dass dieser die Beschäftigten, die im Rahmen ihrer Tätigkeit Zugriff auf personenbezogenen Daten haben – im Regelfall dürfte es sich dabei um Administrationspersonal handeln –, im Innenverhältnis auf § 8 LDSG verpflichtet.
  Eine förmliche Verpflichtung nach dem Verpflichtungsgesetz ist dann von Bedeutung, wenn Daten nach § 203 StGB betroffen sind. Über die Verpflichtung werden dabei die für Amtsträgerinnen und Amtsträger bestehenden strafrechtlichen Sanktionsmöglichkeiten auf den Auftragnehmer

ausgedehnt. Nach den eingangs genannten Kriterien dürften Public Cloud-Leistungen für derartige Verfahren jedoch nur sehr eingeschränkt in Betracht kommen. In die Ausschreibung sollte gleichwohl eine Anforderung aufgenommen werden, wonach der Auftragnehmer sich einverstanden erklärt, dass bei Bedarf für bestimmte Beschäftigte eine förmliche Verpflichtung nach dem Verpflichtungsgesetz durch den LDI oder eine von ihm beauftragte Stelle vorgenommen werden kann.

- Das Angebot von Cloud-Leistungen, die hinsichtlich ihres Datenschutz- und Sicherheitsniveaus differieren, erfordert seitens der Auftraggeber die Bewertung des Schutzbedarfs eines Verfahrens, damit eine risikoadäquate Vergabeentscheidung getroffen werden kann. Die Entscheidung für ein niedrigeres Sicherheitsniveau muss durch einen entsprechend geringeren Schutzbedarf gerechtfertigt werden können, der auf einer nachvollziehbaren, d.h. begründeten und dokumentierten Abschätzung fußt.

Textmuster für Verpflichtungen:

http://www.datenschutz.rlp.de/downloads/mat/verpflichtung_8ldsg.rtf
http://www.datenschutz.rlp.de/downloads/mat/Muster_Verpflichtungsniederschrift_VerpflG.rtf

1.3 Zwei-Klick-Lösung für Videos

Die Problematik bei der Nutzung sog. Social Plugins, etwa von Facebook, Google+ oder Twitter, ist hinlänglich bekannt: Es werden bereits beim bloßen Aufruf einer Webseite mit solchen Plugins Daten an die Betreiber der Plattformen übermittelt, ohne dass die aufrufende Person darüber informiert wird oder in die Übermittlung, Speicherung und Verarbeitung ihrer Daten eingewilligt hat (vgl. 23. Tb., Tz. I-3.2.1). Ebenso entfällt die Möglichkeit, dem zu widersprechen. Dies geschieht nicht nur im Zusammenhang mit den allgegenwärtigen Plugins der sozialen Netzwerke, sondern auch bei den nicht minder verbreiteten eingebetteten Videos von Plattformen wie Youtube oder Vimeo.

Im Rahmen des Webauftritts von „www.young-data.de“, der wie viele Internetpräsenzen der Landesregierung mit Typo3 realisiert wurde, sind zahlreiche Videos von verschiedenen Plattformen eingebunden. Um diesbezüglich dem Datenschutz gerecht zu werden, wurde im Auftrag des LfDI eine Erweiterung für Typo3 vom Landesbetrieb Daten und Information entwickelt. Diese Erweiterung ermöglicht das komfortable Einbetten von Videos beliebiger Plattformen dergestalt, dass beim Aufrufen einer Webseite mit einem Video nur ein Standbild des Videos als Platzhalter angezeigt wird. Fährt man nun mit der Maus über den Platzhalter, so wird ein Hinweistext eingeblendet, der über die mögliche Datenübertragung an diejenigen, die das Video bereitstellen, informiert. Bis hierhin fand noch keine Datenübermittlung an Dritte statt. Dies ändert sich erst, wenn der Link im Hinweistext angeklickt wird. Dann lädt die Seite das eigentliche Video nach und spielt es ab, wodurch es zur beschriebenen Datenübertragung kommt.

Die Erweiterung wird nach endgültiger Fertigstellung den Verwaltungen des Landes zur Verfügung gestellt.

Social Plugins (z.B. von Facebook, Google oder Twitter findet man mittlerweile auf vielen großen und kleinen Webseiten. Es handelt sich dabei um interaktive grafische Elemente, die das einfache Teilen von Inhalten ermöglichen. So kann man beispielsweise über den Facebook-Like Button auf einer Webseite diese „liken“, ohne dazu Facebook selbst zu besuchen.

1.4 Linkverkürzer „s.rlp.de“

In Zusammenarbeit mit dem LfDI hat die Zentralstelle für IT und Multimedia im Ministerium des Inneren, für Sport und Infrastruktur einen landeseigenen datenschutzkonformen Linkverkürzer, auch Kurz-URL-Dienst genannt, ins Leben gerufen. Hintergrund ist die Problematik, dass bei der Nutzung der bekannten Dienste, wie etwa „bit.ly“, „tinyurl“ oder „goo.gl“, deren Betreiber zahlreiche Nutzerdaten erhalten. Hierzu zählen unter anderem die IP-Adresse, die Quellseite mit dem verkürzten Link und natürlich das Ziel des angeklickten Links. Dies geschieht alles, ohne dass die Nutzerinnen und Nutzer darüber informiert werden, einwilligen oder dagegen Widerspruch einlegen können. Der Nutzen solcher Linkverkürzer ist unbestritten, vor allem

innerhalb von Vorträgen oder bei gedruckten Unterlagen. Damit den Verwaltungen des Landes ein entsprechendes datenschutzkonformes Werkzeug zur Verfügung steht, wurde unter http://s.rlp.de/ ein solcher Dienst eingerichtet. Bei der Nutzung werden keine IP-Adressen der Aufrufenden gespeichert, es findet keine Profilbildung oder sonstige Auswertung statt. Der Aufruf des Dienstes zum Zwecke der Verkürzung eines Links ist derzeit nur aus dem rlp-Netz möglich. Der Aufruf eines verkürzten Links hingegen ist von jedem Internetzugang aus durchführbar.

1.5 Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte – Smart-TVs – bieten neben dem Empfang des Fernsehsignals die Möglichkeit, Internetdienste aufzurufen. Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal von Zuschauerinnen und Zuschauern zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Die Fernsehzuschauerinnen und -zuschauer können häufig nicht erkennen, wer welche Informationen dabei über ihr Nutzungsverhalten verarbeitet. Ihr Datenschutzrecht wird durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Die Datenschutzbeauftragten des Bundes und der Länder sind sich darin einig, dass folgende zentrale Forderungen zu beachten sind:

1. Personenbeziehbare Daten der Nutzerinnen und Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.

2. Unmittelbar bei Beginn der Nutzung müssen die Nutzerinnen und Nutzer erkennbar und umfassend über die Datenerhebung und –verarbeitung informiert werden.

3. Anbieter dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffenen Nutzerinnen und Nutzer dem nicht widersprochen haben. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z.B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzerinnen und Nutzer hinzuweisen. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes. Der Verstoß gegen diese Vorgaben kann mit einem Bußgeld geahndet werden.

4. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Endgeräte und Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. So müssen etwa Web-Dienste im Auslieferungszustand der Endgeräte deaktiviert sein, so dass deren Aufruf und die damit einhergehende wechselseitige Kommunikation per Internet erst nach umfassender Information durch die Nutzerinnen und Nutzer selbst initiiert werden.

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

Der LfDI hat die Rundfunkdatenschutzbeauftragten der im Land ansässigen Fernsehsender auf diese Position hingewiesen. Hersteller und sonstige Unternehmen, die TV-Nutzungsdaten unmittelbar aus dem Betrieb von Smart-TVs verarbeiten, sind offenbar nicht in Rheinland-Pfalz ansässig.

1.6 Adressierung im Internet: IPv6 – The Next Generation

Nachdem Mitte März 2011 die letzte IPv4 Adresse vergeben wurde, ist IPv6 mittlerweile im Massenmarkt angekommen. Laut der kontinuierlichen Statistik von Google (http://www.google.de/ipv6/statistics.html) liegt der Anteil der Nutzerinnen und Nutzer, die über IPv6 auf Google zugreifen, weltweit bei rund 2,5 Prozent und innerhalb Deutschlands bei 6,75 Prozent. Viele Provider vergeben mittlerweile IPv6-Adressen, und zahlreiche Endgeräte und

Betriebssysteme beherrschen das Protokoll (vgl. 23. Tb., Tz. II-1.5).

Damit die durch den Umstieg gebotenen Gestaltungsmöglichkeiten auch den Datenschutz berücksichtigen, wurde im Rahmen der 33. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre eine entsprechende Entschließung gefasst („Die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6)“ vom 1. November 2011, http://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungIntDSK/2011InternetIPv6.pdf;jsessionid=5EC60CE0E481AE77BBC073510F14775F.1_cid344?__blob=publicationFile). Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in zwei Entschließungen entsprechende Anforderungen gestellt: „Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!“ vom 28./29. September 2011; „Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller“ vom 7./8. November 2012.

IPv6-Adresse:	
2001:0db8:85a3:08d3 :	1319:8a2e:0370:7347
Präfix	Interface Identifier

Die letztere gibt Hinweise und Empfehlungen zum datenschutzgerechten Einsatz von IPv6. Neben Anforderungen, die sich primär an die Provider richten, waren dabei insbesondere folgende Punkte von Bedeutung:

- Zur Vermeidung eines Nutzertrackings sollen Adresspräfixe grundsätzlich dynamisch an Endkundinnen und -kunden vergeben werden. Im Falle eines statischen Präfixes sollte auf Wunsch der Kundinnen und Kunden über eine einfache Bedienmöglichkeit am Router oder Endgerät das Adresspräfix gewechselt werden können.
- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahlknoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.
- Privacy Extensions müssen auf Endgeräten implementiert werden und sollten standardmäßig aktiviert sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.
- Zusätzlich sollten die Hersteller von Betriebssystemen benutzerfreundliche Konfigurationsmöglichkeiten einbauen, mit denen Kundinnen und Kunden die Wechselfrequenz des Interface Identifiers festlegen bzw. einen Wechsel vornehmen können.
- Die Datenschutzvorkehrungen bei der dynamischen Adressvergabe sind nur dann wirksam, wenn Präfix und Interface Identifier gleichzeitig gewechselt werden, da Diensteanbieter ansonsten Nutzerdaten anhand des jeweils unveränderten Teils miteinander verketten können.
- IPv6-Adressen müssen ebenso wie IPv4-Adressen als personenbezogene Daten angesehen werden. Da bei IPv6-Installationen Mechanismen zur Adressumsetzung wie Network Address Translation (NAT) oder Proxy eine geringere Rolle spielen werden, ist der Informationsgehalt der Adressen höher als bei IPv4. Individuelle Adressen von Clients werden häufiger in Protokolldaten von Internetdiensten auftauchen. Hinsichtlich der rechtlichen Bedingungen gibt es keine wesentlichen Unterschiede zu IPv4. Sofern diese keine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus zulassen, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten.

1.7 Nutzung von Dropbox

Bei Dropbox handelt es sich um eine Cloud-Anwendung, mit der Online-Speicherplatz bereitgestellt wird. Dies erlaubt es, Daten in der „Wolke“ abzulegen und auf diese online von wechselnden Geräten oder Standorten mobil darauf zuzugreifen oder die Daten Dritten zur Verfügung zu stellen. Andere Lösungen mit vergleichbarem Ansatz sind z.B. „Google Drive“, „Web.De SmartDrive“, „Telekom-Cloud“ etc. Bis zu einem vorgegebenen Speichervolumen ist die Nutzung solcher Dienste meist kostenlos. Dropbox war einer der ersten derartigen Dienste am Markt und verfügt, nicht zuletzt aufgrund der leichten Bedienbarkeit und der Unterstützung zahlreicher Plattformen (Windows, Mac, Android-Smartphones oder -Tablets) über eine große Zahl von Nutzerinnen und Nutzern, auch bei Verwal-

tungen und Unternehmen. Von diesen, aber auch von Bürgerinnen und Bürgern wurde der LfDI wiederholt um Beratung gebeten, ob bzw. wie eine vertrauenswürdige Nutzung gewährleistet werden kann.

Dropbox ist ein US-amerikanisches Unternehmen. In der Vergangenheit gab es verschiedene Vorfälle, die die Sicherheit von Dropbox in Frage stellten; nach aktuellen Untersuchungen gilt der Dienst hinsichtlich der eingesetzten Verschlüsselungsalgorithmen (SSL/AES256) allerdings als hinreichend sicher gegenüber Angriffen. Dabei darf jedoch nicht übersehen werden, dass es sich bei der bei Dropbox eingesetzten anbieterseitigen Verschlüsselung um eine Lösung zum Schutz gegenüber Zugriffen Dritter handelt, Dropbox selbst ist als Betreiber des Dienstes und der zugehörigen Verschlüsslung in der Lage, auf die dort abgelegten Informationen im Klartext zuzugreifen bzw. diese bei entsprechenden Anfragen zur Verfügung zu stellen.

Für die Speicherung von Daten, die ohnehin zur Veröffentlichung vorgesehen oder die ohne besondere Sensitivität sind, begegnet die Nutzung von Dropbox keinen datenschutzrechtlichen Bedenken. Für die Speicherung personenbezogener Daten bedarf es jedoch ergänzender Vorkehrungen in Form einer verschlüsselten Speicherung unter der Kontrolle der Nutzerinnen und Nutzer.

Im Rahmen der vom LfDI durchgeführten Crypto-Sessions (vgl. Tz. II-1.1.1) werden Möglichkeiten für eine sichere und vertrauenswürdige Nutzung von Dropbox und vergleichbaren Cloud-Diensten aufgezeigt.

Zwar erfolgt die Ablage der Daten auf den Dropbox-Servern ebenfalls verschlüsselt, dies steht jedoch unter der vollständigen Kontrolle von Dropbox, die Nutzerinnen und Nutzer haben darauf keinen Einfluss. Dropbox hat damit grundsätzlich die Möglichkeit, inhaltlich auf die Daten zuzugreifen. Des Weiteren stellt sich das Problem eines etwaigen Zugriffs durch staatliche (US-)Stellen (vgl. Orientierungshilfe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Cloud Computing“ http://www.datenschutz.rlp/downloads/oh/ak_oh_cloudcomputing.pdf).

Um dies zu vermeiden, bedarf es in solchen Fällen einer Verschlüsselung der Daten durch die Nutzerinnen und Nutzer vor deren Speicherung auf Dropbox. Je nach Sensitivität der Daten können hier einfache Lösungen (z.B. passwortgesicherte ZIP-Datei) jedoch ausreichend sein. Die Anforderungen sind letztlich denen für den Versand personenbezogener Daten via E-Mail vergleichbar.

Selbstdatenschutz: Dropbox & Co sicher nutzen

PCs, Notebooks, Smartphones und Tablets... eine Vielzahl von Endgeräten steht den Nutzerinnen und Nutzern heutzutage zur Verfügung. Und diese Vielfalt wird ausgenutzt, und nicht nur im Bezug auf einzelne Geräte. Viele Nutzerinnen und Nutzer verfügen über mehrere Geräte und möchten natürlich auch von all diesen verschiedenen Systemen auf gespeicherte Informationen zugreifen. Und da der Zugriff nicht nur zu Hause, sondern auch unterwegs erfolgen soll, werden Daten zunehmend auf Speichersystemen im Internet abgelegt, so dass diese überall und jederzeit erreichbar sind. Doch wie ist es um die Vertraulichkeit bei diesen Speichersystemen bestellt? Kann man sich darauf verlassen, dass die Betreiber dieser – zum Teil kostenlosen – Speichersysteme die Privatsphäre der Nutzerinnen und Nutzer beachten? Um sicherzustellen, dass Unbefugte die in der „Wolke“ gespeicherten Informationen nicht zur Kenntnis nehmen, sollte man diese Daten nur verschlüsselt ablegen. Ähnlich wie bei der E-Mailkommunikation stehen hierzu verschiedene Möglichkeiten zur Verfügung.
Lösungen:

- Truecrypt
- 7-Zip (für Windows)
- 7Zx (für Mac)

(vgl. http://www.datenschutz.rlp.de/de/selbstds.php?submenu=cloud)

Dropbox ermöglicht den Up-/Download von Daten über die Dropbox-Webseite, aber auch die automatische Synchronisation mit einem „Dropbox-Ordner“ auf dem Nutzerendgerät. Hierdurch wird Dropbox Zugriff auf das Nutzersystem, ggf. im internen Netz einer Verwaltung gewährt. Möglichen Missbräuchen ist daher ggf. durch eine entsprechende Konfiguration der Firewall-Systeme zu begegnen.

2. Wirtschaft

2.1 Allgemeines

Der LfDI ist jetzt seit sechs Jahren auch Aufsichtsbehörde für die Datenverarbeitung nicht-öffentlicher Stellen, d.h. er hat seither auch zu prüfen, ob die knapp 200.000 rheinland-pfälzischen Betriebe und Wirtschaftsunternehmen die diversen Vorschriften über den Datenschutz beachten. Es liegt auf der Hand, dass dies nicht flächendeckend und anlasslos, sondern nur stichprobenhaft in wenigen Schwerpunktgebieten möglich ist oder eben bei den Unternehmen, die unter datenschutzrechtlichen Gesichtspunkten bereits in die Kritik geraten sind.

Wollte man alle Unternehmen wenigstens ein Mal auf ihre Datenschutzkonformität hin überprüfen und – was ohnehin illusorisch wäre – pro Tag fünf Unternehmen einer Prüfung unterziehen können, bräuchte man mehr als 130 Jahre, bis dieses Ziel erreicht wäre. Wie gesagt: dies ist nur ein Gedankenspiel, zumal die Unternehmen ab einer bestimmten Größe unter bestimmten Voraussetzungen auch einen eigenen betrieblichen Datenschutzbeauftragten zu bestellen haben.

Natürlich war die Zahl der Unternehmen, die im Berichtszeitraum vom LfDI tatsächlich kontrolliert worden sind, kleiner. Aber es waren insgesamt doch mehr als 130 Unternehmen. Zum Teil konnten die Kontrollen relativ schnell abgeschlossen werden, zum Teil waren und sind sie äußerst arbeits- und zeitintensiv, wie z.B. bei der Aufarbeitung der Debeka-Problematik (vgl. Tz. II-6).

Im nachfolgenden Kapitel wird in erster Linie auf einige datenschutzrechtliche Schwerpunktthemen etwas näher eingegangen, u.a. auf die Videoüberwachung. Andere Fragen zum Datenschutz in der Wirtschaft werden – je nach Sachzusammenhang – an anderer Stelle dieses Berichts erörtert (zu den Eingaben im privatwirtschaftlichen Bereich vgl. Tz. II-1.4.2, zu Beratung von Unternehmen vgl. Tz. II-1.5, zu den betrieblichen Datenschutzbeauftragten vgl. Tz. II-4.5, zur Debeka-Datenproblematik vgl. Tz. II-6).

2.2 Hauptthemen des Datenschutzes in der Wirtschaft

In diesen gut fünf Jahren hat sich durch die rasante technische Entwicklung der Datenverarbeitung viel verändert, weniger an den Hauptthemen des Datenschutzes in der Wirtschaft. Schwerpunkte sind nach wie vor die „Dauerbrenner“ Videoüberwachung (vgl. Tz. III-2.3), Überwachung von Beschäftigten (Tz. I-3.3.1) und – besonders stark seit dem „Jahr der Hacker“ 2011 – die Datensicherheit in Unternehmen (Tz. I-2.5). Was sich verändert hat, ist die Intensität der Datenverarbeitung, sie ist schneller, umfassender, komplexer, insgesamt also „intelligenter“ geworden.

Im Bereich **Videoüberwachung** durch Wirtschaftsunternehmen zeigt sich das etwa daran, dass die technische Qualität der Überwachungskameras (gemessen etwa an Auflösung/Pixelzahl oder der Zoomfähigkeit) und der Überwachungstechnik insgesamt (etwa mit Blick auf die nahezu unbegrenzte Verfügbarkeit von Speicherkapazität und die Zugriffsmöglichkeiten auf Überwachungsmaterial via Internet) einen Quantensprung vollzogen hat. Standen Betreiberinnen und Betreiber von Überwachungsanlagen im ersten Jahrzehnt unseres Jahrtausends noch vor einem unüberschaubaren Datenberg an Überwachungsmaterial, verfügen sie im zweiten Jahrzehnt über Software, welche diese Datenberge „durchschaubar“ und damit nutzbar macht: Die Überwachungssoftware lernt selbständig, ungefährliche Normalsituationen von Gefahrenlagen zu unterscheiden und demgemäß Alarm zu geben. Die „gute alte“ Videokamera wird abgelöst von Drohnen (Tz. III-2.3.4), die nahezu unbemerkt ihre Aufnahmen anfertigen und direkt per Internet übertragen; sie wird ersetzt durch portable Kameras für jedermann in Mobiltelefonen und Smartphones; und sie taucht in Gebieten auf, die bis vor kurzem noch als Rückzugsräume verstanden und geschützt wurden, Stichwort „Wildkameras“ (Tz. III-2.3.3).

Ein ähnliches Bild lässt sich im Bereich **Beschäftigtendatenschutz** zeichnen. Chefinnen und Chefs, die sich noch persönlich um das Befinden, die Nöte und manchmal auch um die Fehltritte ihrer Beschäftigten gekümmert und sich dabei auf ihre Erfahrung und das „untrügliche Bauchgefühl“ verlassen haben, wurden in der letzten Dekade abgelöst vom Unter-

nehmensleiterinnen und -leitern, die ausgeklügelte Screeningverfahren einsetzen, um Fehlverhalten der Belegschaft algorithmisch auf die Spur zu kommen. Sie gehen mit High End-Videotechnologie gegen die Verletzung von Verhaltensvorschriften vor, sie verschaffen sich einen Überblick über die Reisewege ihrer Mitarbeiterinnen und Mitarbeiter, die sie jederzeit durch GPS-Sender orten können und die ihnen via Smartphone rund um die Uhr zur Verfügung stehen. Bewerberprofile rufen sie in den einschlägigen sozialen Netzwerken ab; auch ihre Personalchefinnen und -chefs setzen immer weniger auf Detektivdienste, die „Blaumacher“ noch persönlich verfolgten, vielmehr lassen sie Persönlichkeitsprofile erstellen, die auf die umfassende Analyse der Datenspuren von Beschäftigten im Netz gestützt sind. Dass dabei mit Blick auf die leider nur rudimentären gesetzlichen Regelungen des § 32 BDSG häufig Graubereiche be- und sogar übertreten werden, liegt auf der Hand (vgl. Tz. I-3.3.1).

Das Thema **Datensicherheit in Unternehmen** schließlich hat im Jahre 2013 durch die Enthüllungen Edward Snowdens einen unerhörten Aufschwung erfahren (vgl. Tz. I-2.1; I-2.5). Die Berichte des Whistleblowers haben für Erschütterungen gesorgt, die – positiv betrachtet – für eine erhebliche Steigerung der Bemühungen der Unternehmen um die Sicherheit ihrer Kunden-, Geschäftspartner- und Mitarbeiterdaten (und natürlich zum Schutz ihrer Betriebs- und Geschäftsgeheimnisse) gesorgt haben. Allerdings hat die Berichterstattung über mögliche Wirtschafts- und Industriespionage durch US-amerikanische und britische Geheimdienste und die angebliche Infiltration von VPNs durch das Überwachungsprogramm „XKeyscore“ bei nicht wenigen Unternehmen zu einer resignativen Haltung beigetragen, nach dem Motto: Man kann gegen Unternehmensspionage ohnehin nichts tun! Diese Einstellung wäre jedoch vollkommen unangebracht, der LfDI bemüht sich weiterhin darum, beim Thema Datensicherheit in Unternehmen mit den verantwortlichen Stellen an einem Strang zu ziehen und insbesondere das Thema Verschlüsselung weiter zu propagieren (vgl. Tz. I-2.5).

2.3 Videoüberwachung

2.3.1 Entwicklung

Schon in seinen letzten Tätigkeitsberichten hat der LfDI das Schwerpunktthema Videoüberwachung ausführlich dargestellt und Empfehlungen hierzu ausgesprochen (vgl. 23. Tb., Tz. II-2.2). Tausende Videokameras werden zur Zeit zur Überwachung von Supermärkten und Kaufhäusern, von Einkaufspassagen und Tankstellen, von Bahnhöfen und Sparkassen, von Regionalbahnen und Bussen des öffentlichen Personennahverkehrs in Rheinland-Pfalz eingesetzt. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Insbesondere muss die Videoüberwachung erforderlich sein, und die Interessen der Betroffenen müssen durch entsprechende technische und organisatorische Maßnahmen ausreichend geschützt werden.

Den Vorteilen der Videoüberwachung insbesondere bei der Diebstahlsvorbeugung und ihrem (beschränkten) Nutzen zur Aufklärung von Straftaten stehen nämlich erhebliche Nachteile gegenüber: Zu nennen ist hier insbesondere der Überwachungs- und Anpassungsdruck, der durch die Videoüberwachung entsteht; neben der Gefahr eines allgemeinen Voyeurismus ist durch die Installation von Videoüberwachungsanlagen auch eine Lähmung der Hilfsbereitschaft und des Verantwortungsgefühls in der Bevölkerung zu beobachten. Positive Wirkungen der Videoüberwachung werden häufig dadurch gemindert, dass nur bloße Verlagerungseffekte auftreten, also Straftaten nicht etwa unterbleiben, sondern lediglich von einem an den anderen Ort verschoben werden.

Mittlerweile sind aufgrund der technologischen Fortentwicklung diese Kameras häufig nicht mehr als solche zu erkennen, sondern ähneln kleinen Lampen mit wenigen Zentimetern Durchmesser. Auch trennen uns nur noch ein paar Entwicklungsschritte von einer Videoüberwachung, die Gesichter

erkennen und auf bestimmte „auffällige“ Bewegungen von „Zielpersonen“ reagieren kann. Insbesondere die datenmäßige Vernetzung der Kameras ist in Teilbereichen bereits machbar. Das in früheren Berichten angesprochene Problem der überwachenden Stellen, dass sie in der Flut von Bildern unterzugehen drohten, ist mittlerweile auf technischem Wege gelöst: „Intelligente“ Videoüberwachung ermöglicht es, die Aufzeichnungen so zu steuern und zu filtern, dass nach einer technischen Vorauswahl dem Überwachungspersonal nur noch „relevante“ Bilder präsentiert werden. Damit ist in den letzten Jahren aus einer Videotechnik, die „ins Blaue hinein“ eingesetzt und nur höchst selten vollständig ausgewertet wurde, eine „scharfe“ Videoüberwachung geworden, ein ebenso effektives wie datenschutzrechtlich problematisches Mittel der intensiven Überwachung einer Vielzahl von Betroffenen.

So gesehen stehen wir an einem Scheideweg: Entweder die unkontrollierte und unkontrollierbare Ausbreitung der Videoüberwachung hinzunehmen, die unser Privatleben weiter einschränken und unser Verhalten zunehmend beeinflussen wird, oder aber energisch gegenzusteuern.

Grundlage einer Zurückdrängung der sich epidemisch ausbreitenden Videoüberwachungsanlagen ist die Bestandsaufnahme der aktuellen Situation in Rheinland-Pfalz, die der LfDI bereits in den Jahren 2008 und 2009 durchführte. Bei der breit angelegten, in ihrem Umfang bundesweit einmaligen Umfrage zur Videoüberwachung durch die öffentliche Hand wurden 2.673 öffentliche Stellen in Rheinland-Pfalz befragt, zusammen mit Stichproben im privaten Bereich, etwa bei Tankstellen und Sparkassen, wurden Informationen zu insgesamt mehr als 6.000 Stellen erhoben (vgl. 22. Tb., Tz. 3.2). Auf Basis der gut fundierten Schätzung, dass allenfalls jede zehnte Überwachungskamera sich in öffentlicher Hand befindet, wurde damals für Rheinland-Pfalz von 30.000 bis 50.000 Überwachungskameras ausgegangen.

Diese Zahl ist im Berichtszeitraum mit Sicherheit weiter angestiegen, die Kombination aus Preisverfall und Miniaturisierung der Technik hat zwischenzeitlich dazu geführt, dass von deutlich mehr Überwachungskameras in Rheinland-Pfalz auszugehen ist; dies wird unten anhand der Beispiele „Wildkameras“ und „Drohnen“ belegt und erläutert werden (vgl. Tz. III-2.2.3 und Tz. III-2.2.4).

Die Zunahme der Videoüberwachung spiegelt sich auch im weiteren Anstieg der Nachfragen und Beschwerden zu diesem Thema beim LfDI wider, etwa ein Drittel der mehr als 2.000 Eingaben an den LfDI betreffen den Bereich Videoüberwachung. Bei seinen dann ausgelösten Kontrollen stellt der LfDI oft gravierende Missstände fest. Die häufigsten datenschutzrechtlichen Mängel finden sich im Bereich der Hinweispflichten (vgl. § 6b Abs. 2 BDSG). Häufig fehlen Hinweisschilder ganz, regelmäßig sind sie nicht zur Kennzeichnung des Überwachungsbereichs, sondern unterhalb der Kamera angebracht; in vielen Fällen fehlt zudem der vorgeschriebene Hinweis auf die verantwortliche Stelle.

Regelmäßig fehlen auch Videoüberwachungskonzepte, welche vor Inbetriebnahme der Anlage verpflichtend zu erstellen sind (vgl. § 6b Abs. 1 Nr. 3, Abs. 3 BDSG). Insbesondere fehlt es häufig an der Festlegung bestimmter Zwecke der Videoüberwachung, die eine aufsichtsbehördliche Kontrolle der Rechtmäßigkeit der Videoüberwachung erst ermöglichen.

Wird Videoüberwachung in Form der Aufzeichnung betrieben, finden sich in der Regel Verstöße gegen die Höchstspeicherdauer der Videoaufzeichnung. Eine Überschreitung der maximalen Grenze von 48 Stunden Speicherdauer führt regelmäßig zur Unverhältnismäßigkeit der Videoüberwachung. Im staatlichen Bereich wurden den Behörden Orientierungshilfen an die Hand gegeben, um eine rechtskonforme und zurückhaltende Anwendung der Videoüberwachung zu ermöglichen. Mittlerweile stellen die Aufsichtsbehörden von Bund und Ländern auch für die Videoüberwachung durch private Stellen eine Orientierungshilfe zum Einsatz von Videoüberwachung zur Verfügung.
(http://www.datenschutz.rlp.de/downloads/oh/oh-vue-durch-nicht-oeffentliche-Stellen.pdf)

Noch wichtiger ist es aber, dass die Bürgerinnen und Bürger mit offenen Augen durch ihren Alltag gehen und nicht klaglos akzeptieren, wenn in ihrer Eisdiele, im Schwimmbad, in Toilettenbereichen oder im Zug nach Hause Videokameras installiert werden.

2.3.2 Nachbar überwacht Nachbar

Die Anzahl der Beratungsanfragen aus der Bevölkerung rund um das Thema Videoüberwachung steigt weiterhin. Mittlerweile erreichen den LfDI auch vermehrt Beschwerden über Videoüberwachungsanlagen in der eigenen Nachbarschaft. Entweder zeigt die beanstandete Kamera z.B. auf den Garten der bzw. des Anderen oder aber auf den öffentlichen Verkehrsraum. Die Nachbarinnen und Nachbarn scheinen sozusagen ihre Nachbarschaft zu überwachen – sehr zum Missfallen der Betroffenen. Dabei handelt es sich zwar nicht um eine „Wirtschaftsthematik“, wegen ihrer praktischen Bedeutung für die Arbeit des LfDI soll die „nachbarschaftliche Überwachung“ jedoch an dieser Stelle näher erörtert werden.

Ob die von der Nachbarin oder dem Nachbarn betriebene Videoüberwachung zulässig ist, hängt zunächst von der Anwendbarkeit des Bundesdatenschutzgesetzes (§ 6b BDSG) ab. Das Bundesdatenschutzgesetz greift nur ein, wenn öffentlich zugängliche Räume beobachtet werden und es sich um eine Videoüberwachung zu gewerblichen Zwecken handelt. Liegen diese Voraussetzungen nicht vor, dann ist der LfDI nicht zuständig und kann dem Nachbarn leider nicht weiterhelfen. Das bedeutet allerdings nicht, dass damit die Überwachung zulässig ist. Dann müssen vielmehr an Stelle des LfDI die Zivilgerichte über die Rechtmäßigkeit der Videoüberwachung entscheiden.

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

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

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

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

In vielen Fällen kann der LfDI also auch bei Auseinandersetzungen zwischen Nachbarn weiter helfen. Als Faustregel gilt: Wer fremde Grundstücke oder öffentlichen Verkehrsraum videoüberwacht, verstößt gegen geltendes Recht und kann vom LfDI oder von den Zivilgerichten zum Abbau der Überwachungsanlage verpflichtet werden.

2.3.3 Wildkameras – Der Wald hat tausend Augen

Inzwischen haben Videokameras ihren Weg aus der Nachbarschaft hinaus in den Wald gefunden: In den 3.500 Jagdbezirken in Rheinland-Pfalz sind ca. 20.000 Jägerinnen und Jäger unterwegs. Zur Erleichterung der Jagdausübung werden seit mehreren Jahren Wildkameras eingesetzt. Teilweise werden sie auch zum Schutz jagdlicher Einrichtungen wie Hochsitze, Jagdhütten u.ä. angebracht.

Seit alle großen Discounter diese Kameras zum Preis von unter 100 Euro anbieten, nimmt ihre Verbreitung rasant zu. Nach Schätzungen setzt inzwischen im Schnitt jede Jägerin bzw. jeder Jäger zwischen zwei bis drei solcher Kameras ein. Damit kommt man für Rheinland-Pfalz auf einen

Kamerabestand im fünfstelligen Bereich. Auch nach dem LfDI vorliegenden Verkaufsangaben ist davon auszugehen, dass in Rheinland-Pfalz über 30.000 Wildkameras im Einsatz sind.

Diese digitalen Wildkameras sind technisch gut ausgestattet. Sie werden über einen Bewegungsmelder aktiviert, besitzen Nachtsichtfunktion und speichern wahlweise Fotos oder Videos mit hoher Auflösung (ab fünf Megapixel, z.T. HD-Qualität) auf SD-Karten. Diese sind z.T. von der Kamera getrennt angebracht und werden via WLAN oder SIM-Karte angesteuert. Auch die Übertragung von Bildern per SMS oder MMS ist möglich.

Der steigende Einsatz von Wildkameras in den rheinland-pfälzischen Wäldern wird auch von der Bevölkerung wahrgenommen. Waldbesucherinnen und -besucher, die sich beim Spazieren oder Joggen beobachtet fühlen, wenden sich an die Aufsichtsbehörde. So ist seit Mitte 2012 die Anzahl der Beschwerden über Wildkameras deutlich gestiegen, mittlerweile liegen dem LfDI über 100 Beschwerden gegen Wildkameras vor.

Auf Grundlage umfangreicher Prüfungen ist der LfDI zum Ergebnis gekommen, dass der Einsatz von Wildkameras mit dem Datenschutzrecht (§ 6b BDSG) grundsätzlich unvereinbar ist. Dies gilt unabhängig davon, ob es sich um Privat- oder um Staatswald handelt.

In Rheinland-Pfalz hat jeder das Recht, sich im Wald zu Erholungszwecken frei zu bewegen, auch abseits von Wegen und Pfaden. Vom allgemeinen Betretungsrecht sind nach Landesrecht auch Kirrungen, Suhlen und andere Anlagen umfasst. Die Videoüberwachung in solchen öffentlich zugänglichen Räumen ist in § 6b BDSG geregelt. Danach ist eine Abwägung des Interesses der Waldbesucherinnen und -besucher an einem von Beobachtung unbeschwerten Aufenthalt im Wald einerseits und des Interesses der Jägerinnen und Jäger bzw. Wald-, Feld- und Wiesenbesitzerinnen und -besitzer an einer durch den Einsatz von Videotechnik erleichterten Ausübung der Jagd andererseits vorzunehmen.

Das Recht der Spaziergängerinnen und Spaziergänger, Joggerinnen und Jogger, Pilzsammlerinnen und -sammler und Geocacher auf informationelle Selbstbestimmung und damit darauf, als Waldbesucherin und -besucher in freier Natur unbeobachtet zu sein, verdient nach Ansicht des LfDI hier den Vorrang. Ihr schutzwürdiges Interesse wiegt grundsätzlich deutlich schwerer als das Interesse der Jägerinnen und Jäger, die Effizienz der Jagd und Hege zu steigern und konkrete Angaben zum Wildbestand ohne langwieriges Ansitzen zu erlangen.

Diese Abwägungsentscheidung gilt zwar grundsätzlich, nicht aber ausnahmslos. Zu beachten sind nämlich besondere Fallkonstellationen, wie etwa in solchen Bereichen, zu denen Besucherinnen und Besucher des Waldes keinen Zugang haben, etwa an Wildbrücken. Da solche Wildtierbrücken einem Betretungsverbot unterliegen und daher keinen öffentlich zugänglichen Raum darstellen, sind hier Einzelaufnahmen rechtlich möglich.

Akzeptiert werden können ggf. auch Kameras, die aufgrund ihrer Position für alle offenkundig keine Personen, sondern nur Tiere erfassen können, so. z.B. bei der Dachsbaubeobachtung. Auch können Wildkameras, die von Forschungseinrichtungen zu wissenschaftlichen Zwecken eingesetzt werden, unter bestimmten Voraussetzungen zulässig sein.

Gehen Hinweise auf Wildkameras und deren Betreiberinnen und Betreiber beim LfDI ein, so wird ein Auskunftsverfahren nach § 38 Abs. 3 BDSG eröffnet. Sollten sich die Betreiberinnen und Betreiber auf keinen der o.g. Ausnahmetatbestände berufen können, so kann die Anfertigung von Aufzeichnungen untersagt werden (§ 38 Abs. 5 BDSG). Für den Fall, dass die Betreiberin oder Betreiber der Kamera dem nicht nachkommt, wird ein angemessenes Bußgeld – etwa in Höhe von 5.000 Euro pro Kamera – verhängt.

Zudem kann ein Bußgeld gemäß § 43 Abs. 2 Nr. 1 BDSG in Höhe von bis zu 300.000 Euro verhängt werden, wenn Aufzeichnungen von Wildkameras im Internet verbreitet werden oder ihre Weitergabe an Dritte erfolgt.

Bislang stieß der LfDI bei seinem Vorgehen gegen Wildkameras zwar auf deutlichen Widerspruch des Landesjagdverbandes, nicht aber auf Widerstand

bei den einzelnen Kamerabetreibern. In jedem geprüften Einzelfall konnte eine Lösung gefunden werden, sei es durch Demontieren der Kamera, sei es durch deren Neuausrichtung. Der LfDI hat jedoch auch keinen Zweifel daran, dass solche einvernehmlichen Lösungen nicht immer gefunden werden können. Dann wird es den Gerichten obliegen, über die Abgrenzung und Gewichtung der betroffenen Interessen aller Beteiligten zu entscheiden.

2.3.4 Drohnen

Die Überwachung findet mittlerweile auch aus der Luft statt. Mit Drohnen, also Flugrobotern, die mit Videokameras ausgestattet werden können, lassen sich Bilder und Filme von Veranstaltungen, Wohngebieten oder Landschaften aufnehmen oder sogar in der Zukunft Pakete ausliefern.

Während sich die Landesregierung im Rahmen einer gemeinsamen Fachtagung des rheinland-pfälzischen Ministeriums des Inneren, für Sport und Infrastruktur und des LfDI im September 2013 für größte Zurückhaltung bei deren Einsatz aussprach und erklärte, dass sie derzeit vom Kauf von Drohnen absehe (vgl. Tz. III-4.1.4), sieht dies im privaten Bereich ganz anders aus. Nach den auf der Fachtagung gegebenen Informationen sind in Deutschland allein ca. 300.000 Drohnen, die als Träger von Kameras geeignet seien, bei Privaten in Gebrauch. Eine Videobeobachtung durch unauffällige, überall einsetzbare fliegende Kameras ist somit praktisch für jedermann möglich. Derzeit ist der Einsatz von Überwachungsdrohnen zu Sport- und Freizeitzwecken sogar genehmigungs- und anzeigefrei.

Der LfDI nahm diese Informationen zum Anlass, die Situation der zivilen Drohnen in Rheinland-Pfalz näher zu analysieren. Auf Anfrage beim Landesbetrieb Mobilität (LBM) konnten Einzelheiten zu den Drohnenflügen geklärt werden. Laut LBM ist der Betrieb eines Flugmodells erlaubnisfrei, solange das Gerät unter fünf Kilogramm Gesamtmasse inklusive Lasten wiegt, in einer Entfernung von mehr als 1,5 km zu Flugplätzen aufsteigt (§ 16 Abs. 1 Nr. 1c LuftVO) und nicht zu gewerblichen Zwecken erfolgt. Der LBM stellte fest, dass aus diesem Grund viele Steuernde angeben, Luftbildaufnahmen zum Zwecke des Sports oder der Freizeitgestaltung, also zu rein privaten Zwecken zu machen. Damit würden sie ihr Fluggerät erlaubnisfrei als Flugmodell nutzen.

Der Datenschutz wird bei der Entscheidung über eine Aufstiegserlaubnis insoweit berücksichtigt, als bei einer Einzelaufstiegserlaubnis das Einverständnis der vom Drohnenflug betroffenen Grundstückseigentümerinnen und -eigentümer bzw. Nutzungsberechtigten eingereicht und für eine Allgemeinerlaubnis zudem eine datenschutzrechtliche Erklärung abgegeben werden muss.

Die vom LBM genannten Zahlen zeigen, dass in den letzten drei Jahren die Anzahl der Drohnenflüge in Rheinland-Pfalz erheblich gestiegen ist. Während im Jahr 2011 nur 19 Einzelaufstiegserlaubnisse für den Aufstieg eines unbemannten Luftfahrtsystems erteilt wurden, waren es im Jahr 2012 bereits 68. Im Jahr 2013 stieg die Zahl erneut: 150 Anfragen wurden verzeichnet, 70 Allgemeinerlaubnisse und 23 Einzelaufstiegserlaubnisse erteilt. Gründe für eine Ablehnung bzw. Antragsrücknahme waren bis jetzt lediglich flugfachliche Bedenken seitens der Luftfahrtbehörde. Auch Bedenken der zuständigen Ordnungsämter, die durch den beabsichtigten Aufstieg des unbemannten Luftfahrtsystems eine Gefahr für die öffentliche Sicherheit und Ordnung vermuteten, wurden bei der Entscheidung berücksichtigt. Datenschutzrechtliche Bedenken haben bislang einen Aufstieg nicht verhindert.

Die zunehmende Verbreitung von Drohnen mit Kameras spiegelt sich einerseits in einer Reihe von Einzeleingaben von Bürgerinnen und Bürgern wider, andererseits machen große Fachhäuser Werbung für Quadrocopter & Co mit den passenden Kameras. Soweit Drohnen mit Überwachungstechnik ausgestattet sind, liegen datenschutzrechtliche Fragestellungen mit Blick auf § 6b BDSG auf der Hand. Zu nennen ist hier insbesondere die Frage, ob der mit dem Drohneneinsatz verfolgte Zweck die schutzwürdigen Interessen der Betroffenen überwiegt (vgl. § 6b Abs. 1 Nr. 3 BDSG) und wie eine sinnvolle Kennzeichnung der Videoüberwachung (Pflicht nach § 6b Abs. 2 BDSG) aussehen könnte.

Gesamtbewertung des LfDI

Insgesamt lässt sich die Videoüberwachung daher datenschutzrechtlich wie folgt bewerten:

- Jede Videoüberwachung ist ein Eingriff in das Persönlichkeitsrecht, denn alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.
- Die Videoüberwachung erfasst unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen.
- Daher ist Videoüberwachung immer begründungsbedürftig und darf immer nur offen erfolgen, sie ist stets auf das notwendige Maß zu beschränken und bedarf in zeitlicher Hinsicht der regelmäßigen Überprüfung (jährliche Evaluationspflichten).
- Vor der Einrichtung einer Videoüberwachung müssen alle Alternativen hierzu geprüft und bewertet werden. Videoüberwachung kann nur die ultima ratio sein.
- Jede Einrichtung einer Videoüberwachung muss der datenschutzrechtlichen Vorabkontrolle unterzogen werden (§ 4d Abs. 5 BDSG), gleichzeitig ist die Berufung eines behördlichen bzw. betrieblichen Datenschutzbeauftragten vor Installation der Videoüberwachung verpflichtend.
- Der Zweck der Videoüberwachung muss konkret vor Beginn der Überwachung schriftlich festgelegt werden.
- Während der Videoüberwachung müssen die Zweckbindung, die differenzierte Abstufung zwischen Aufnahmearten, die deutliche Erkennbarkeit der Videoüberwachung sowie die Löschung der Daten binnen kurzer Fristen (48 Stunden) strikt und dauerhaft sichergestellt werden.
- Rechtskonforme Videoüberwachung ist planungsintensiv, kostspielig, aufwändig und nur begrenzt effektiv. Videoüberwachung ist nur bei optimaler technischer und personeller Ausführung erfolgversprechend und nur dann verhältnismäßig.
- Die Beweislast für die Zulässigkeit der Videoüberwachung liegt bei den Betreiberinnen und Betreibern.
- Die flächendeckende Videoüberwachung muss verhindert werden, da die Gefahr besteht, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.
- Mögliche Rechtsverletzungen werden als Ordnungswidrigkeit mit hohen Bußgeldern verfolgt, können aus personellen Gründen jedoch nur unzureichend staatlich geahndet werden (Vollzugsdefizit).

2.4 Auditierung und Zertifizierung

Angesichts von Kontrolldefiziten der Datenschutzaufsichtsbehörden, die sich einer Vielzahl von zu kontrollierenden Unternehmen gegenübersehen, werden seit jeher Versuche unternommen, durch eine Selbstregulierung der Wirtschaft Abhilfe zu schaffen. Dabei spielt die Auditierung und Zertifizierung durch Externe eine große Rolle.

Als Audit (lat. Anhörung) werden Untersuchungsverfahren bezeichnet, die dazu dienen, Prozesse hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten. Dies erfolgt häufig im Rahmen eines Qualitätsmanagements. Die Audits werden von speziell hierfür ausgebildeten Auditorinnen und Auditoren durchgeführt. Das Audit endet mit einer bloßen Bestätigung seiner Durchführung.

Als Zertifizierung (lat. sicher machen) bezeichnet man ein Verfahren, mit dessen Hilfe die Einhaltung bestimmter Anforderungen – etwa die Einhaltung bestimmter Gesetze – nachgewiesen wird. Zertifizierungen werden oft zeitlich befristet von unabhängigen Zertifizierungsstellen, wie z.B. TÜV, DEKRA oder anderen privaten Gutachterstellen vergeben. Anders als ein Audit endet die Zertifizierung also mit der Bekanntgabe eines bestimmten Ergebnisses, das eine Bewertung durch die Zertifizierenden darstellt.

In § 9a BDSG hat der Bundesgesetzgeber ein Datenschutzaudit vorgesehen. Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachterinnen und Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachterinnen und Gutachter werden durch besonderes Gesetz geregelt.

§ 9a BDSG vereint also die Möglichkeiten von Auditierung und Zertifizierung. Allerdings hat die Vorschrift bis heute keine Bedeutung erlangt, weil sich der Bundesgesetzgeber bisher nicht auf ein Ausführungsgesetz verständigen konnte. Will man die Chancen von Auditierung und Zertifizierung dennoch nutzen, müssen drei Probleme gelöst werden:

- sie müssen sich auf Normen einigen, die Maßstab der Prüfungen sein sollen; dazu müssen die gesetzlichen Vorgaben (z.B. § 9 BDSG) in eine prüffähige Form gebracht werden (nach dem Muster von DIN-Normen);
- sie müssen private Gutachterinnen oder Gutachter finden und auswählen, welche die Gewähr dafür bieten, dass die Vor-Ort-Prüfungen sachgerecht und fachkundig durchgeführt werden; hierfür bieten sich private Datenschutzorganisationen/externe Datenschutzberaterinnen oder -berater an;
- sie müssen für die Anerkennung der Audits/Zertifikate sorgen; nur wenn alle Aufsichtsbehörden die Prüfergebnisse akzeptieren, sind die Testate für die Unternehmen nützlich; die bislang auf dem Markt befindlichen Testate vom TÜV etc. werden von den Aufsichtsbehörden nicht anerkannt, führen also nicht zu einer Entlastung der Unternehmen; das Bedürfnis der Unternehmen nach einer solchen Absicherungsmöglichkeit ist unverändert hoch.

Dies hat auch der Düsseldorfer Kreis, der zuständige Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder erkannt und in einem Beschluss vom 26. Februar 2014 mit dem Titel „Modelle zur Vergabe von Prüfzertifikaten“ insbesondere festgestellt:

„Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen. Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.”
Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern. Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.
(…)
Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten. Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.
Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen. Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.“

Der LfDI hat – nach früheren Bemühungen um die Fortentwicklung und Etablierung von Datenschutz-Management-Systemen – besonders durch Kooperation mit RKW Rheinland-Pfalz, Teil der bundesweit operierenden Selbsthilfeeinrichtung der mittelständischen Wirtschaft, einen Prüfkatalog zum Datenschutz mitentwickelt. Dieser soll es gerade kleinen und mittleren Unternehmen erleichtern, datenschutzrechtliche Anforderungen im Betrieb zu erkennen und umzusetzen. Nähere Informationen zum RKW-Prüfzertifikat, das auf Basis eines vom LfDI empfohlenen Prüfkatalogs erteilt werden kann, finden sich unter http://www.rkw-rlp.de/pdf/RKW_Folder_Datenschutz.pdf.

2.5 Ordnungswidrigkeitenverfahren

Der LfDI ist nicht nur Beratungs-, sondern ebenso Kontroll- und wenn nötig auch Sanktionsbehörde. In

den vergangenen Jahren hat sich gerade im Bereich „Datenschutz in der Privatwirtschaft“ gezeigt, dass eine Datenschutzstelle nur dann ihre Aufgabe vollständig erfüllen kann, wenn sie nicht nur unterstützen, aufklären und beraten darf, sondern in besonderen Situationen auch bestrafen kann.

Interessanterweise sind es nicht selten Unternehmen, die sich mit erheblichen Anstrengungen um die Etablierung eines hohen betrieblichen Datenschutzniveaus bemüht haben, die ihrerseits die Sanktionierung von Unternehmen, die Datenschutzrecht verletzten, einfordern. Das gleiche Bild ergibt sich bei internen wie externen betrieblichen Datenschutzbeauftragten, die mit wenig Verständnis solche Unternehmen betrachten, die sich wenig bis gar keine Mühe bei der Einhaltung gesetzlicher Datenschutzstandards geben. Auch von dieser Seite ist die Forderung, Rechtsverletzungen nicht nur abzustellen, sondern mit spürbaren Sanktionen zu ahnden, unüberhörbar.

Der LfDI hat hierauf mit der Einrichtung einer eigenen Bußgeldstelle reagiert, die sich auf die Ahndung von Datenschutzverstößen konzentriert. Zielvorgabe dieser Bußgeldstelle ist es, aus der Vielzahl ahndbarer Datenschutzverstöße jedes Jahr etwa ein Dutzend Vorfälle auszusondern, bei denen eine Sanktionierung besonders naheliegt und exemplarische Wirkung verspricht. Mit diesem Kontrollansatz – erstmals umgesetzt im Jahre 2013 – wurden bisher Bußgelder in fünfstelliger Höhe erzielt. Im Vordergrund der Tätigkeit des LfDI steht aber keineswegs das Ziel, willkommene Einnahmen für das Land Rheinland-Pfalz zu erzielen, sondern durch die exemplarische Bestrafung von Datenschutzverstößen das allgemeine Bewusstsein für die Geltung und Wirksamkeit unserer gesetzlichen Regelungen zu stärken.

2.6 Vorschlag für eine Landesdatenschutzkonferenz

Die dargestellte rasante technische Entwicklung der Datenverarbeitung ist auch Anlass dafür, dass sich im rheinland-pfälzischen Koalitionsvertrag die regierungstragenden Parteien darauf verständigt haben, in dieser Legislaturperiode eine Landesdatenschutzkonferenz in Rheinland-Pfalz durchzuführen. Der LfDI hat dazu einige konzeptionelle Vorstellungen entwickelt, die aus seiner Sicht wesentliche Eckpunkte einer solchen Konferenz darstellen könnten. Orientierungspunkte lieferten dafür zahlreiche Gespräche mit Vertreterinnen und Vertretern der rheinland-pfälzischen Wirtschaft und die mittlerweile fast 2.000 Eingaben, die den LfDI jedes Jahr in seiner Funktion als Aufsichtsbehörde für die Privatwirtschaft erreichen; darüber hinaus wurden die Planungen anderer Länder für die Durchführung von Landesdatenschutzkonferenzen (vgl. Landtag Nordrhein-Westfalen, LT-Drs. 16/1469 vom 20. November 2012) einbezogen.

Eine Landesdatenschutzkonferenz sollte aus Sicht des LfDI mehr sein als ein im Ergebnis unverbindlicher Austausch über aktuelle Themen des Datenschutzes und der Datensicherheit. Die Konferenz sollte vielmehr greifbare Ergebnisse vorweisen können, also in der Verabschiedung von Handlungsempfehlungen, Aktionsprogrammen oder spezifischer Datenschutzentschließungen gipfeln. Da solche Entschließungen einer intensiven Vorbereitung und auch kontroversen Diskussion bedürfen, benötigt die Landesdatenschutzkonferenz eine umsichtige Planung, die in themenbezogenen Workshops auf Arbeitsebene bestehen sollte.

Thematisch wäre die Befassung insbesondere mit den folgenden Themenfeldern zu empfehlen:

IT-Sicherheit und Cloud-Computing

Die bekannt gewordenen Zugriffsmöglichkeiten US-amerikanischer Stellen auf Daten von Cloud-Dienstleistern haben deutlich gemacht, welche Risiken sich beim Cloud Computing für Unternehmensdaten ergeben können. Insbesondere bei mittelständischen Unternehmen hat dies zu einer Verunsicherung darüber geführt, ob diese Form der IT-Nutzung überhaupt anzustreben ist. Vor dem Hintergrund des wirtschaftlichen Potenzials derartiger Lösungen sollten geeignete Handlungsoptionen dargestellt werden. Ziel könnte hier die die Einrichtung eines IT-Kompetenzzentrums für die Wirtschaft sein.

Beschäftigtendatenschutz

Nach dem Scheitern des Gesetzentwurfs der Bundesregierung zum Arbeitnehmerdatenschutz fehlt es in diesem brisanten Bereich an Orientierung. Eine entsprechende Handlungsempfehlung zu zentralen Fragestellungen (Nutzung von E-Mail und Internet am Arbeitsplatz/Videoüberwachung/Mitarbeiterscreening) kann auch auf Länderebene unter Einbeziehung der Tarifpartner, von Wirtschaftsvertretern und Gewerkschaften erarbeitet werden.

Auditierung und Zertifizierung zum Datenschutz

Nachdem die Bemühungen des Bundesgesetzgebers zu § 9a BDSG (Datenschutzaudit) ins Stocken geraten sind, haben die Landesdatenschutzbehörden Anstrengungen unternommen, das Datenschutzniveau von Unternehmen prüfbar und auf der Grundlage anerkannter Zertifikate (Datenschutzsiegel) demonstrierbar zu machen. Solchen Zertifikaten kommt im Wettbewerb der Unternehmen um das Vertrauen ihrer Kundinnen und Kunden und Geschäftspartnerinnen und -partner eine immer größere Bedeutung zu.

3. Datenschutz im öffentlichen Personalwesen

3.1 Datenschutz bei der Bewerbung um Einstellung in den Vorbereitungsdienst für das Lehramt

Wie dem LfDI aufgrund einer anonymen Anzeige bekannt wurde, verwendete die Aufsichts- und Dienstleistungsdirektion als Lehrereinstellungsbehörde bei Online-Bewerbungen ein Formular, in dem nach bereits eingestellten Ermittlungsverfahren gefragt wurde.

Das Bundesarbeitsgericht hatte in seinem Urteil vom 15. November 2012 (Az. 6 AZR 339/11) jedoch festgestellt, dass die Frage nach eingestellten Ermittlungsverfahren, die weder im Führungszeugnis aufzunehmen noch gegenüber Gerichten oder Behörden auskunftsfähig sind, vom Erforderlichkeitsgrundsatz nicht gedeckt und damit unzulässig sind.

Nachdem der LfDI auf diese aktuelle Rechtsprechung hingewiesen hatte, wurde die entsprechende Passage im Formular gestrichen.

3.2 IPEMA

Der Ministerrat hat am 27. November 2007 die Einführung eines Integrierten Personalmanagementsystems (IPEMA) in der Landesverwaltung Rheinland-Pfalz beschlossen. Das Projekt IPEMA hat das Ziel, ein einheitliches und integriertes Softwaresystem für die Bezügeabrechnung und die Personalverwaltung der Landesbediensteten in Rheinland-Pfalz – basierend auf einer Standardsoftware – einzuführen. Mit IPEMA werden insgesamt 26 IT-Systeme ersetzt und die Standardisierung von Geschäftsprozessen bei unterschiedlichen Behörden unterstützt. Dem Problem von Übertragungsfehlern oder veralteten Datenbeständen soll dadurch wirksam begegnet werden, dass mit IPEMA die Daten zu den Bediensteten nur noch an einer Stelle gespeichert und gepflegt werden. IPEMA wird vom Landesbetrieb Daten und Information im Weg der Auftragsdatenverarbeitung für die personalverwaltenden Dienststellen zentral betrieben.

Die Einführung von IPEMA ist im Berichtszeitraum weiter vorangeschritten. Produktivsetzungen erfolgten für die Bezügeabrechnung der Zentralen Besoldungs- Versorgungsstelle, in den Personalverwaltungen innerhalb des Geschäftsbereichs der Oberfinanzdirektion, im Bereich der Lehrerpersonalverwaltung sowie beim Statistischen Landesamt. Bis 2015 soll stufenweise die Ausweitung auf alle Verwaltungen des Landes erfolgen.

Der LfDI hat das Projekt seit dem Start kontinuierlich begleitet. Dabei ging es insbesondere um Fragen der Protokollierung, der Möglichkeit eines (unbemerkten) Datenexports, der Löschung abgeschlossener Personalfälle sowie um die Zulässigkeit eines automatisierten Zugriffs anderer Behörden oder Stellen. Zu dem letztgenannten Punkt wurde dem LfDI eine Musterdienstvereinbarung zur Prüfung vorgelegt, die automatisierte Zugriffe durch oberste Dienstbehörden mittels IPEMA auf Personaldaten des nachgeordneten Bereichs vorsah. Der LfDI vertrat die Auffassung, dass dies mit den beamtenrechtlichen Regelungen zum Personalaktenrecht nicht zu vereinbaren ist. Denn § 89 Abs. 2 Satz 2 LBG sieht vor, dass ein automatisierter Zugriff anderer Behörden – worunter auch vorgesetzte Behörden zu verstehen sind – auf Personalaktendaten nur dann zulässig ist, soweit dies durch eine „besondere Rechtsvorschrift“ zugelassen wird. Der Gesichtspunkt der Dienstaufsicht rechtfertigt es zwar, in Einzelfällen – auch online – auf bestimmte Fälle zuzugreifen, jedoch nicht, ein automatisiertes Abrufverfahren mit der Möglichkeit eines einzelfallunabhängigen Zugriffs auf einen Gesamtdatenbestand einzurichten. Hierfür bedarf es einer ausdrücklichen Regelung. Die Musterdienstvereinbarung wurde daraufhin geändert.

3.3 Datenschutz bei Heim- bzw. Telearbeit

In den vorangegangen Tätigkeitsberichten hatte der LfDI die Auffassung vertreten, dass personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, am Heimarbeitsplatz grundsätzlich nicht verarbeitet werden dürfen (vgl. 17. Tb., Tz. 17.3 und 20. Tb., Tz. 17.1). Gründe hierfür waren eingeschränkte Kontrollmöglichkeiten des LfDI am Heimarbeitsplatz, das erhöhte Missbrauchspotenzial aufgrund fehlender sozialer Kontrolle

sowie allgemein das erhöhte Risiko, dass beim Transport der Daten oder am Heimarbeitsplatz Unbefugte Kenntnis von besonders schützenswerten Daten erlangen können.

Im Berichtszeitraum erreichten den LfDI mehrere Anfragen aus dem Bereich der Polizei und der Finanzverwaltung, in denen es um die Zulässigkeit eines Zugriffs auf Zentralverfahren sowie um die Zulässigkeit der Verarbeitung von besonders schützenswerten Daten im Wege der Telearbeit ging. Dabei wurde vorgetragen, dass es unter dem Gesichtspunkt der Vereinbarkeit von Familie und Beruf auch für den öffentlichen Dienst wichtig sei, attraktive Arbeitsplätze anbieten zu können. Inhaltliche Beschränkungen würden die Gestaltungsmöglichkeiten bei Heimarbeitsplätzen erheblich erschweren.

Die genannten Bedenken haben nach wie vor Bestand. Der LfDI hält es allerdings für hinnehmbar, wenn diese Bedenken durch restriktive technisch-organisatorische Datensicherungsmaßnahmen gewissermaßen „abgefedert“ werden. Dazu zählt insbesondere, dass

- die Datenverarbeitung auf dienstlichen Geräten stattfindet,
- eine vorherige Inspektion des Heimarbeitsplatzes stattfindet,
- der Datentransport gegen Zugriffe durch Unbefugte gesichert ist,
- in einer Individualvereinbarung Zutrittsmöglichkeiten für Kontrollzwecke mit Sanktionsmöglichkeiten bei einer Zutrittsverweigerung vereinbart werden und
- beim Zugriff auf Zentralverfahren eine 100 Prozent-Protokollierung erfolgt.

Die bisherige Position wird insofern modifiziert, als die Beachtung der technisch-organisatorischen Anforderungen nunmehr in den Vordergrund rückt. Dies entspricht der Auffassung vieler Datenschutzbeauftragter anderer Länder, die sich auf eine entsprechende Umfrage des LfDI in diesem Sinne geäußert hatten.

4. Polizei und Verfassungsschutz

4.1 Polizei

4.1.1 Bestandsdatenauskünfte

Sowohl für Zwecke der Straftatenaufklärung als auch für Zwecke der Gefahrenabwehr benötigt die Polizei Auskünfte über Bestandsdaten der Telekommunikation. Bestandsdaten sind Angaben, die für die Begründung, Durchführung und Beendigung eines Nutzungsverhältnisses notwendig sind. Dazu gehören vor allem Angaben über die Identität von Kommunikationsteilnehmerinnen und -teilnehmern, ohne dass dabei der Inhalt der Kommunikation berührt wird. Es geht vielmehr um die Frage: wem z.B. eine bestimmte Rufnummer zugeordnet oder eine bestimmte IP-Adresse zugewiesen war bzw. ist.

Mit seinem Urteil zur Bestandsdatenauskunft (vom 24. Februar 2012, Az. 1 BvR 1299/05) hat das Bundesverfassungsgericht insbesondere in Bezug auf die Herausgabe von dynamischen IP-Adressen durch die Internetprovider an Sicherheitsbehörden neue Schranken formuliert, die im seinerzeit geltenden Recht (Strafprozessordnung, Telekommunikationsgesetz, Polizeigesetze der Länder) gefehlt haben. Der Gesetzgeber musste nachbessern.

Auf der Bundesebene ist dies mit einem neuen § 100j StPO und der Neuformulierung des § 113 TKG geschehen, aus der Sicht von vielen Datenschützern allerdings unzureichend (vgl. http://www.heise.de/newsticker/meldung/Ueber-6000-Buerger-unterstuetzen-Verfassungsbeschwerde-gegen-Bestandsdatenauskunft-1945705.html). Auch der LfDI vertritt die Auffassung, dass § 100j StPO zu weit gefasst ist.

Im rheinland-pfälzischen Polizeigesetz fehlt derzeit noch eine Regelung, die die Polizei ausdrücklich ermächtigt, von den Internetprovidern die IP-Adressen der Nutzerinnen und Nutzer heraus zu verlangen. Aus polizeilicher Sicht ist eine solche Regelung erforderlich. Außer in Rheinland-Pfalz fehlt eine solche Regelung aber auch noch in den Polizeigesetzen von Berlin-Brandenburg, Bremen und dem Saarland.Der LfDI kann nicht beurteilen, ob es wirklich realistisch ist anzunehmen, dass in der Praxis zu Gefahrenabwehrzwecken solche Bestandsdaten von der Polizei benötigt werden. Fälle, in denen das Fehlen einer entsprechenden Befugnis zu Schwierigkeiten geführt hätte, sind ihm nicht vorgetragen worden. Wenn eine solche Notwendigkeit aber bejaht wird, sieht er keine grundsätzlichen Probleme, entsprechend den Vorgaben des Bundesverfassungsgerichts eine polizeigesetzliche Befugnis für solche Abfragen zu schaffen. Diese müsste sich eng am Erforderlichen orientieren.

4.1.2 Zugriff auf POLIS im Rahmen polizeilicher Heimarbeit

Die Zulässigkeit des Zugriffs auf polizeiliche Zentralverfahren durch heimarbeitende Polizeibeamtinnen und -beamte hatte der LfDI zunächst sehr kritisch gesehen. In einem mit dem Innenministerium abgesprochenen Probebetrieb wurde lediglich der Zugriff auf POLADIS zugestanden, womit nur auf Daten des jeweiligen Polizeipräsidiums zugegriffen werden konnte. Landesweite Dateien wie EWOIS, ZEVIS oder POLIS waren vom Zugriff im Bereich der Heimarbeit ausgenommen. Der Probebetrieb zeigte aber, dass durch die Beschränkung ein effektives Arbeiten am Heimarbeitsplatz nicht möglich war. Eine zeitgleich vom LfDI veranlasste Länderumfrage ergab zudem, dass die Zulässigkeit der Verarbeitung von Daten am Heimarbeitsplatz vielerorts von der Beachtung der technisch-organisatorischen Vorgaben abhängig gemacht wird, ohne dabei inhaltliche Beschränkungen vorzunehmen. Dementsprechend wird auch der LfDI künftig verfahren (vgl. Tz. III-3.3).

4.1.3 „Gewalttäter Sport“-Datei

Die Polizeien der Länder und des Bundes unterhalten seit 1994 eine Verbunddatei, in der Personen gespeichert werden, die im Zusammenhang mit Sportveranstaltungen, insbesondere bei Fußballspielen, als Straftäterinnen und -täter aufgefallen sind, gegen die ein Ermittlungsverfahren eingeleitet oder eine polizeiliche Verfügung zur Gefahrenabwehr getroffen wurde.

Die für die Datei erstellte Errichtungsanordnung benennt einen Straftaten- und Anlasskatalog und beschreibt die Einzelheiten der Datenspeicherung. Es können auch Erkenntnisse von ausländischen

Sicherheitsbehörden gespeichert werden. Da Sportveranstaltungen oftmals internationalen Charakter haben, gewinnt dieser Umstand an Bedeutung. Zu nennen sind z.B. die Champions League-Begegnungen oder die regelmäßig wiederkehrenden Europameisterschaften im Fußball.

Die befristete Dateispeicherung, die nach dem Bundeskriminalamtgesetz und der Bundeskriminalamt-Daten-Verordnung erfolgt, soll in erster Linie dazu dienen, gewalttätige Auseinandersetzungen und sonstige Straftaten im Zusammenhang mit Sportveranstaltungen zu verhindern. Die Erfassung potentiell gefährlicher Teilnehmerinnen und Teilnehmer soll ermöglichen, diese vor Ort frühzeitig zu erkennen und Störungen entgegenzuwirken.

Aus datenschutzrechtlicher Sicht können dagegen keine grundsätzlichen Einwände erhoben werden. Die Belange von gewaltbereiten Sportfans müssen hinter das Allgemeininteresse an einem störungsfreien Ablauf von sportlichen Wettkämpfen zurücktreten. Allerdings müssen die Rechtschutzinteressen der von der Datenspeicherung Betroffenen gewahrt bleiben. Diese müssen die Möglichkeit haben, staatliches Handeln überprüfen zu lassen. Insofern ist es aus der Sicht des Datenschutzes wichtig, dass die Rechte der Betroffenen angemessen berücksichtigt werden und neben transparenten Aufnahmekriterien eine generelle Benachrichtigung über die Aufnahme in die „Gewalttäter Sport“-Datei erfolgt.

Der Speicherung liegt regelmäßig eine polizeiliche einzelfallbezogene Prognoseentscheidung zugrunde. Da jedoch keine Benachrichtigungsverpflichtung besteht, ist es tatsächlich möglich, dass Betroffene in Unkenntnis über die bestehende Speicherung eine Überprüfung der Einzelentscheidung nicht herbeiführen können. Im rheinland-pfälzischen Koalitionsvertrag 2011 – 2016 der Parteien SPD und BÜNDNIS 90/DIE GRÜNEN wurde diese Problematik thematisiert und eine Neugestaltung der „Gewalttäter Sport“-Datei vereinbart. Der LfDI hat im Berichtszeitraum mehrfach die Einführung einer einheitlichen Benachrichtigungsverpflichtung gefordert, um Transparenz hinsichtlich der erfolgten Speicherungen für die Betroffenen zu erreichen. So wurde das Thema auch durch das rheinland-pfälzische Ministerium des Innern, für Sport und Infrastruktur auf der 193. Sitzung der Innenministerkonferenz aufgegriffen und eine Änderung der bundeseinheitlichen Errichtungsanordnung vorgeschlagen. Leider folgte nur Bremen der Ansicht von Rheinland-Pfalz, so dass eine einheitliche Regelung auf Bundesebene bis heute nicht umgesetzt werden konnte.

Auf die Initiative des LfDI hin wurde durch das rheinland-pfälzische Innenministerium geprüft, ob in einem ersten Schritt zumindest diejenigen benachrichtigt werden können, die ausschließlich auf der Grundlage einer vorangegangenen Gefahrenabwehrmaßnahme (z.B. Platzverweis, Identitätsfeststellung) durch das Land Rheinland-Pfalz in der „Gewalttäter Sport“-Datei gespeichert wurden. Das Innenministerium hat dies für möglich angesehen. Dementsprechend werden ab dem 1. Januar 2013 die vorgenannten Personen über entsprechende Speicherungen unterrichtet. Der darin liegende Zugewinn an Transparenz ist zu begrüßen.

Unabhängig von diesem Teilerfolg wird der LfDI auch künftig Anstrengungen unternehmen, eine Neugestaltung der Benachrichtigungsregelung auf Bundesebene für alle von rheinland-pfälzischen Polizeidienststellen veranlasste Speicherungen zu erreichen.

4.1.4 Die polizeiliche Videoüberwachung zum Zwecke der Gefahrenabwehr

Die Videoüberwachung spielt nicht nur in Einkaufszonen und an Tankstellen eine Rolle. Auch die rheinland-pfälzische Polizei hat sich in den letzten Jahren dieser Technik zum Zweck der Gefahrenabwehr bedient.

Anfang 2011 wurde für polizeiliche Videoüberwachungsmaßnahmen, die in öffentlich zugänglichen Räumen durch den offenen Einsatz technischer Mittel erfolgen, eine Anzeigepflicht beim LfDI eingeführt (§ 27 Abs. 7 POG). Dies führte dazu, dass der LfDI im Berichtszeitraum frühzeitig über präventiv-polizeiliche Videoüberwachungsmaßnahmen informiert wurde und sie aus Datenschutzsicht beeinflussen konnte.

- Videoüberwachung anlässlich der Heilig-Rock-Wallfahrt 2012 in Trier

Das Polizeipräsidium Trier legte dem LfDI Anfang 2012 ein umfangreiches Videokonzept anlässlich der damals bevorstehenden Heilig-Rock-Wallfahrt vor und beschrieb darin den beabsichtigten Einsatz von Videokameras im Stadtgebiet von Trier. Die Verwendung von Überwachungstechnik wurde mit der internationalen Bedeutung, der mehrwöchigen Dauer der Veranstaltungen (13. April bis 13. Mai 2012), den eng begrenzten baulichen Gegebenheiten vor Ort, der zu erwartenden Besucherzahl und den vielen Rahmenveranstaltungen, die in unmittelbaren Bezug zur Wallfahrt vorgesehen waren, begründet. Störungen durch Veranstaltungsgegnerinnen und -gegner, erhebliche Besucherströme und die regelmäßig im Umfeld von Großveranstaltungen auftretenden Straftaten sollten durch die Videoüberwachung frühzeitig lokalisiert und abgewendet werden.

Weiter beinhaltete das Konzept die Darlegung der technischen Einzelheiten, Angaben zur beabsichtigten Speicherdauer und der Bedienungsmodalitäten. Entsprechend der Bedeutung einer über einen Monat andauernden Veranstaltungsüberwachung nahm der LfDI das Angebot der Polizei an und informierte sich vor Ort über Art und Umfang der beabsichtigten Maßnahme. Darauf hin wurde in beidseitigem Einverständnis die Anzahl der Kameras reduziert, die Live-Überwachung für den Betrieb im Übersichtsmodus voreingestellt und eine verkürzte Speicherdauer vereinbart. Zudem wurden Privatbereiche, die im Zoombereich der Kameras lagen, verpixelt. Ergänzende Zugriffsprotokollierungen und automatisierte Löschroutinen rundeten das Konzept ab.

Das gemeinsam erarbeitete Ergebnis führte aus Sicht des LfDI zu einem gelungenen Interessenausgleich und erwies sich zugleich als Beispiel dafür, dass die technischen Verbesserungen auch einen differenzierten Umgang mit dem polizeilichen Instrument der Videoüberwachung im Sinne des Datenschutzes ermöglichen.

- Videoüberwachung anlässlich des Rheinland-Pfalz-Tages 2012 in Ingelheim

Durch das Polizeipräsidium Mainz wurde der LfDI im Mai 2012 informiert, dass während des Rheinland-Pfalz-Tages (1. bis 3. Juni 2012) eine Videokamera zur Fertigung von Übersichtsaufnahmen zum Einsatz kommen sollte. Das Konzept legte dar, dass die Zuwege zur Veranstaltungsörtlichkeit zu Spitzenzeiten so stark frequentiert sein könnten, dass polizeiliche Lenkungsmaßnahmen erforderlich erschienen. Um entsprechende Lageentwicklungen frühzeitig erkennen und Einsatzmaßnahmen besser koordinieren zu können, beabsichtigte das Polizeipräsidium die Einrichtung einer erhöht angebrachten Videokamera. In das Konzept eingeflossen waren bereits die Anregungen, die der LfDI im Zusammenhang mit dem Trierer Verfahren gegeben hatte, so dass hier lediglich in Bezug auf die anzubringenden Hinweisschilder ein ergänzender Vorschlag seitens des LfDI eingebracht wurde. Die Veranstaltung verlief nach polizeilicher Verlautbarung mit einem stark verteilten Besucheraufkommen, so dass der Einsatz der Videotechnik nicht erforderlich wurde.

- Videoüberwachung anlässlich einer Gerichtsverhandlung am Landgericht Kaiserslautern im Sommer 2012

Ebenfalls im Mai 2012 legte das Polizeipräsidium Kaiserslautern dem LfDI ein Videokonzept anlässlich einer bevorstehenden Gerichtsverhandlung am Landgericht Kaiserslautern vor. Die polizeiliche Lagebeurteilung hinsichtlich des Mordprozesses, der mit zwei Verhandlungstagen pro Woche vom 5. Juni bis 16. August 2012 vorgesehen war, thematisierte die möglichen Auseinandersetzungen der Mitglieder zweier rivalisierender Motorradclubs und berücksichtigte auch die Erfahrungen bei einer in dieser Angelegenheit erfolgten Verhandlung von Dezember 2009 bis Mai 2010.

Das umfangreiche Videokonzept sah die Einbindung bestehender Kamerainstallationen, die Errichtung neuer stationärer Kameraeinheiten sowie den Einsatz mobiler Videotechnik vor. Zur Verdeutlichung der räumlichen Gegebenheiten besichtigte der LfDI den Einsatzraum und ließ sich das Konzept durch die Polizei Kaiserslautern näher erörtern. Auch hier zeigte sich, dass die zurückliegenden Anregungen

des LfDI, insbesondere im Bereich der technischen Möglichkeiten, bereits berücksichtigt worden waren. Einzelheiten hinsichtlich der Aufzeichnungsdauer und Löschregelung konnten im gemeinsamen Gespräch mit der Polizei vor Ort geklärt werden. Einige Anregungen des LfDI zugunsten von Datensparsamkeit und Datenvermeidung wurden aufgenommen und im Konzept umgesetzt. Die nachfolgende Gerichtsverhandlung verlief weitgehend störungsfrei, da der Angeklagte aussagebereit war und die Polizei an den Veranstaltungstagen entsprechende Präsenz zeigte. Aus Sicht des Datenschutzes wäre hier eine schrittweise Rücknahme des Einsatzes von Videotechnik möglich gewesen, was seitens der Polizei jedoch nicht als zielführend angesehen wurde.

- Der polizeiliche Einsatz von zivilen Drohnen zur Fertigung von Videoaufnahmen

Zunehmend werden frei erwerbbare unbemannte Fluggeräte, auch Drohnen genannt, angeboten, die nicht nur fliegen, sondern auch Luftaufnahmen fertigen können. Die Einsatzmöglichkeiten sind nahezu unbegrenzt. Auch staatliche Stellen erkennen in der neuen Technik einen Nutzen und begründen den Einsatz mit der Möglichkeit der Kostenreduzierung oder der verbesserten Aufgabenwahrnehmung. Bereits Ende 2012 hatte der LfDI das rheinland-pfälzische Ministerium des Innern, für Sport und Infrastruktur um Auskunft gebeten, ob die rheinland-pfälzische Polizei Drohnen eingesetzt hat. Darauf hin wurde dem LfDI mitgeteilt, dass die Polizei in Rheinland-Pfalz keine eigenen unbemannten Fluggeräte unterhalte, sich aber in zurückliegender Zeit (März 2011 bis Juni 2012) in drei Fällen solcher Gerätschaften bedient habe. So sei in einem Vermisstenfall eine private Drohne zum Absuchen eines unwegsamen Geländes und in zwei weiteren Fällen polizeiliche Drohnen des Landes Hessen eingesetzt worden, um unmittelbar bevorstehende Maßnahmen an den Einsatzörtlichkeiten besser planen zu können. In der Folgezeit fanden zwischen Vertreterinnen und Vertretern des rheinland-pfälzischen Innenministeriums und des LfDI Besprechungen statt, die die Frage zum Gegenstand hatten, ob für einen solchen Einsatz die vorhandenen Rechtsgrundlagen ausreichen.

Ebenso versuchte der LfDI, die Datenschutzbeauftragten des Bundes und der Länder für das Thema zu sensibilisieren und eine gemeinsame Stellungnahme zu erarbeiten. Diese Bemühungen sind noch nicht abgeschlossen.Um die Problematik der polizeilichen Drohneneinsätze deutlicher herauszuarbeiten, fand im August 2013 auf Anregung des LfDI eine Veranstaltung zu diesem Thema statt, die in Kooperation mit dem rheinland-pfälzischen Innenministerium erfolgte. An der ganztägigen Veranstaltung nahmen Vertreterinnen und Vertreter des Justiz- und Innenministeriums, Abgeordnete des rheinland-pfälzischen Landtages, Führungskräfte der rheinland-pfälzischen Polizei sowie weitere Gäste aus dem Bereich des Datenschutzes teil. Die Referenten vermittelten einen Überblick über den derzeitigen Stand der Technik und mögliche Einsatzbereiche. Sie konnten den Gästen zudem die luftverkehrsrechtliche Situation bei unbemannten Fluggeräten sowie die derzeitigen rechtlichen Grundlagen für den Drohneneinsatz vermitteln. Deutlich wurde, dass der Einsatz von Drohnen eine neue Qualität im Bereich der Überwachungstechnik darstellt und insofern nur nach strenger Verhältnismäßigkeitsprüfung und unter Beachtung der rechtlichen Voraussetzungen erfolgen kann. Die Veranstaltung schloss mit dem Fazit, dass Drohnen auch in Zukunft als polizeiliches Standardeinsatzmittel nicht eingesetzt werden können und dürfen.

- Weitere Befassungen mit polizeilicher Videoüberwachung

Im Berichtszeitraum hat sich der LfDI darüber hinaus mit Regelungen zur Videoüberwachung polizeilicher Liegenschaften, zur optischen Überwachung von polizeilichen Gewahrsamsräumen, der polizeilichen Videoüberwachung bei Fußballspielen in der Coface-Arena in Mainz und mit einem Konzept zum Einsatz von polizeilicher Videotechnik anlässlich des Rosenmontagsumzuges befasst. Die jeweiligen Konzeptionen konnten in Abstimmung mit den jeweiligen Polizeibehörden so ausgestaltet werden, dass ein Ausgleich zwischen dem Schutz auf informationelle Selbstbestimmung und staatlichem Überwachungsinteresse hergestellt werden konnte.

Die eingeführte Anzeigeverpflichtung von polizeilichen Videoüberwachungsmaßnahmen in das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz (§ 27 Abs. 7 POG RP) hat sich bewährt. Hierdurch hat der LfDI frühzeitig von beabsichtigten Maßnahmen erfahren

und konnte so die Belange des Datenschutzes zur Geltung bringen. Im Rahmen des gemeinsamen Austausches wurde ein gegenseitiges Verständnis geschaffen, das sich in den polizeilichen Maßnahmen widerspiegelt und dazu geführt hat, dass von Videotechnik nur maßvoll Gebrauch gemacht wird. Das rheinland-pfälzische Ministerium des Innern, für Sport und Infrastruktur erarbeitet derzeit eine Handlungsempfehlung „Polizeilicher Einsatz von Videotechnik“, die in Abstimmung mit dem LfDI die Planung und Vorbereitung derartiger Konzepte erleichtern soll.

Im politischen Raum wurden immer wieder Stimmen laut, die Video-Überwachung deutlich auszubauen. Für Diskussionen sorgte etwa die anlässlich des fehlgeschlagenen Bombenattentats auf dem Bonner Hauptbahnhof erhobene Forderung des seinerzeitigen Bundesínnenministers, ausnahmslos alle Bahnhöfe mit Videotechnik intensiv zu überwachen. Solchen Ansinnen hat sich der LfDI stets entschieden entgegen gestellt und betont, dass immer eine Einzelfallprüfung unter Abwägung der betroffenen Rechtsgüter erfolgen müsse. Eine generelle Ausweitung der Überwachung ohne Kosten-Nutzenanalyse in Bezug auf die betroffenen Grundrechte ist nicht zielführend und gefährdet den verfassungsrechtlich gebotenen Grundrechtsschutz.

4.1.5 Polizeiliche Nutzung von Twitter

Um im Zusammenhang mit den Heimspielen des 1. FC Kaiserslautern die direkte Kommunikation mit betroffenen Gruppen (z.B. Anwohnerschaft in Bezug auf Absperrungen, Beeinträchtigungen; Anreisende in Bezug auf die Parksituation; Fangruppen) zu ermöglichen und um Ausschreitungen und Probleme im Zusammenhang mit Fußballspielen zu vermeiden, hat das Polizeipräsidium Westpfalz das Projekt „Taktische Kommunikation anlässlich von Fußballspielen über Facebook“ initiiert.

Nach Gesprächen mit dem LfDI nahm die Polizei Abstand von dem Vorhaben, Facebook für diese Zwecke zu nutzen, da dies viele Datenschutzfragen aufgeworfen hatte. Polizei und LfDI verständigten sich auf die Online-Plattform Twitter, welche die Polizei Kaiserslautern im Rahmen eines Pilotprojekts zur kommunikativen Begleitung von Fußballspielen seit dem Herbst 2012 einsetzt. Der Einsatz von Twitter sei neben dem Einsatz in der Ultra-Szene und durch Konfliktmanager eine weitere Maßnahme zur Information, Transparenz und Deeskalation. Die Twitternachrichten enthielten bewusst viele Informationen zur Verkehrslage, da gerade auch in diesem Aspekt ein hohes Aggressionspotenzial liege. Die Polizei habe diese neue Maßnahme im Vorfeld durch Pressearbeit bekannt gemacht. Straftaten, wie z.B. Beleidigungen, via Twitter würde man nachgehen. Während der Testphase werde das Medium nur in Kaiserslautern eingesetzt. Das Pilotprojekt sollte bis zum Ende der Saison laufen und dann evaluiert werden.

Der LfDI hat gegenüber der Polizei betont, dass man sich bewusst sein müsse, dass die im Rahmen der Kommunikation über Twitter gespeicherten Daten, die Polizeizwecken dienten, von Twitter verkauft würden. Die erforderliche Rechtfertigung sei zweifelhaft. Das Projekt biete zwar viele Vorteile, diese würden aber dadurch erkauft, dass der Staat Privatpersonen veranlasse, Daten von sich herauszugeben. In einem ersten Erfahrungsbericht hat das Innenministerium die Nützlichkeit des Instruments betont. Der LfDI ist aber noch nicht davon überzeugt, dass bei einer Abwägung der datenschutzrechtlichen Nachteile des Verfahrens mit den dargelegten Vorteilen diese tatsächlich überwiegen. Er hat deshalb weitere Fragen formuliert. Die Erörterungen dauern derzeit an.

4.1.6 Polizeiliche Fahndung mit Hilfe von Facebook

Umstritten war und ist, ob öffentliche Fahndungsmaßnahmen der Strafverfolgungsbehörden auf Facebook-Seiten erfolgen dürfen. Mit dieser Frage haben sich nicht nur die Datenschutzbeauftragten, sondern auch die Innenminister- sowie die Justizministerkonferenz befasst, außerdem die Konferenz der Chefs der Staatskanzleien.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat darauf hingewiesen, dass eine Nutzung von Facebook zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch

Zeuginnen und Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist (Entschließung „Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“ vom 28. März 2014; vgl. http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=087_fahndung).

Eine Nutzung sozialer Netzwerke zum Zweck der Verbreitung von Fahndungsaufrufen darf nach der Auffassung der Konferenz – der sich der LfDI angeschlossen hat – nur erfolgen, wenn

- die Kommentierungsfunktion deaktiviert ist,
- die besonderen Voraussetzungen der Fahndung in sozialen Netzwerken in Umsetzungsvorschriften konkretisiert werden und insbesondere die Anlage B der Richtlinien für das Straf- und Bußgeldverfahren geändert wird,
- sichergestellt wird, dass eine solche Fahndung nur bei schwerwiegenden Straftaten erfolgt,
- die Staatsanwaltschaft verpflichtet wird, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben und zu begründen, warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll,
- sichergestellt wird, dass die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,
- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzerinnen und Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Für die Verwendung von Fahndungshinweisen auf der Facebook-Seite der Polizei Rheinland-Pfalz gelten derzeit die nachfolgenden verfahrenssichernden Regelungen:

1. Pressemeldungen, die Fahndungsmitteilungen enthalten, können auf der Startseite der Fanpage „Polizei Rheinland-Pfalz“ veröffentlicht werden, wenn keine personenbezogenen Daten und Abbildungen enthalten sind und die Überleitung durch einen Link zu weiteren Informationen auf die Homepage der Polizei Rheinland-Pfalz erfolgt. Die weiterführenden Fahndungsinformationen sind dort der jeweiligen Pressemeldung zu entnehmen.
2. Fahndungsmeldungen können darüber hinaus auf der Startseite der Fanpage „Polizei Rheinland-Pfalz“ durch unmittelbare Verlinkung zur Fahndungsseite der Homepage der Polizei Rheinland-Pfalz dargestellt werden; auch hier darf der überleitende Text in Facebook keine personenbezogenen Daten und Abbildungen enthalten. Die weiteren Fahndungsinformationen sind auf der Homepage der Polizei Rheinland-Pfalz gebündelt auf einer gesonderten Fahndungsseite abrufbar.

Der LfDI prüft derzeit, ob damit die datenschutzrechtlichen Anforderungen als erfüllt angesehen werden können. Es ist aus der Sicht des LfDI in jedem Fall zu vermeiden, dass im Zusammenhang mit Fahndungshinweisen durch Nutzerkommentare auf Facebook personenbezogene Daten verbreitet und möglicherweise völlig Unschuldige öffentlich an den Pranger gestellt werden.

4.1.7 Das „TKÜ–Competence Center“ der rheinland-pfälzischen Polizei

Die Kommunikationstechnik hat sich in den letzten zwei Jahrzehnten strukturell wesentlich verändert. Smartphones und Laptops sind allgegenwärtig. Mit der Digitalisierung aller Telekommunikationsvorgänge verschwimmen die Grenzen zwischen Telefonie und mobiler Datenverarbeitung.

Die Sicherheitsbehörden sehen das Bedürfnis, ihre Überwachungsmaßnahmen dieser neuen Situation anzupassen. Eine Telefonüberwachung, die mittels eines einfachen „Aufschaltens“ auf die Leitung einer Telefonkundin oder eines Telefonkunden durchgeführt werden konnte, hat sich zu einem komplexen Vorgang entwickelt.

Das rheinland-pfälzische Ministerium des Innern, für Sport und Infrastruktur hat deshalb im Sommer 2009

eine Projektgruppe TKÜ-CC (Telekommunikationsüberwachungs-Competence Center) eingesetzt, welche die Beschaffung und den Betrieb einer zentralen TKÜ-Anlage sowie den Aufbau und die Implementierung eines Kompetenzzentrums sowohl für die klassische als auch für die operative elektronische Kommunikationsüberwachung vorbereiten soll. Die Kompetenzbündelung war ein weiteres Ziel. Zukünftig soll eine zentrale Stelle der gesamten Polizei zugänglich sein.

Der LfDI wurde frühzeitig über das Projekt informiert. So erstellte das Landeskriminalamt Rheinland-Pfalz ein Datenschutz- und IT-Sicherheitskonzept für die zentrale TKÜ-Anlage der rheinland-pfälzischen Polizei und stimmte diese mit dem LfDI ab. In diesem Zusammenhang nahm der LfDI die beschaffte Hardware und deren Sicherung in den Räumlichkeiten beim Landesbetrieb Daten und Information in Augenschein. Es gab keine Beanstandungen.

Das vorgelegte Datenschutzkonzept für die TKÜ-Anlage erfüllt die Anforderungen, die § 41a POG (Technische und organisatorische Maßnahmen des Datenschutzes) beschreibt. Außerdem wird die Kernbereichsproblematik aufgegriffen, Dokumentations- und Zugriffsregelungen werden beschrieben und die Voraussetzungen für Datenübermittlungen in polizeiliche Bearbeitungsprogramme werden festgelegt. Insgesamt wurde eine Grundlage erarbeitet, die die datenschutzrechtlichen Anforderungen berücksichtigt.

Weiter wurden dem LfDI eine Generalerrichtungsanordnung und eine Verfahrensbeschreibung zur Telekommunikationsüberwachung vorgelegt, die weitere datenschutzrechtlich relevante Festlegungen enthalten.

Die neue TKÜ-Anlage wurde im Mai 2012 in Betrieb genommen. Sie löst sukzessive die dezentralen Überwachungseinheiten in den einzelnen Polizeipräsidien ab. Zwischenzeitlich laufen alle Überwachungsmaßnahmen über die zentrale Überwachungstechnik sowie unter Aufsicht und mit dem Know-how des TKÜ-CC, das in die Organisationsstruktur des Landeskriminalamtes Rheinland-Pfalz überführt wurde.

Diese neue zentrale Struktur der Telekommunikationsüberwachung ermöglicht auch dem LfDI unter erleichterten Bedingungen Kontrollen und Nachprüfungen. Wenn dem Staat im Interesse der Strafverfolgung und der Gefahrenabwehr unter engen gesetzlich geregelten Voraussetzungen Eingriffe in das Telekommunikationsgeheimnis gestattet sind, so ist es nicht zu beanstanden, wenn diese Eingriffe technisch effizient erfolgen. Zu begrüßen ist es, wenn die damit geschaffenen Strukturen die rechtsstaatlich gebotenen und vorgesehenen Kontrollen erleichtern, ob die verfassungsrechtlichen und gesetzlichen Schranken eingehalten werden. Dies scheint nach derzeitigem Erkenntnisstand mit dem TKÜ-Kompetenzzentrum gelungen zu sein.

4.1.8 Quellen-TKÜ – Staatstrojaner

Unter der Überschrift „Der Staatstrojaner“ wurde im Datenschutzbericht 2010/2011 bereits ausführlich beschrieben, welche Datenschutzfragen sich stellen, wenn die Strafverfolgungsbehörden verschlüsselte Kommunikation abhören wollen, die über das Internet erfolgt (vgl. 23. Tb., Tz. I-3.5). Entsprechende Maßnahmen werden „Quellen-TKÜ“ genannt, weil sie heimlich an der Quelle, dem Ausgangscomputer der Kommunikation, oder dem Zielgerät der Kommunikation ansetzen und dort mittels einer „Trojaner-Software“ unverschlüsselte Kommunikationsdaten ausleiten, d.h. an die Strafverfolgungsbehörden senden. An die Technik, die eingesetzt werden muss, wenn solche Abhörmaßnahmen durchgeführt werden, sind zur Wahrung des Datenschutzes besondere Anforderungen zu stellen. Seit dem letzten Tätigkeitsbericht wurden in Abstimmung mit dem LfDI detaillierte Anforderungsprofile an die Software und an das Verfahren beim Einsatz dieser Software formuliert. Derzeit wird eine solche Software entwickelt. Einsatzbereit ist sie nach wie vor noch nicht.

Ebenso fehlt nach wie vor eine ausreichende Rechtsgrundlage in der Strafprozessordnung, um eine solche Technik im Bereich der Strafverfolgung rechtskonform einsetzen zu können.

Im Land gilt nach wie vor die Regelung, dass eine Quellen-TKÜ erst durchgeführt wird, wenn eine solche Technik einsatzbereit ist. Mit anderen

Worten: Entsprechende Ermittlungsmaßnahmen wurden im Berichtszeitraum nicht vorgenommen.

4.1.9 Antiterrordatei und Rechtsextremismusdatei

Die Antiterrordatei hat der LfDI bereits in vorangegangenen Tätigkeitsberichten dargestellt (vgl. 21. Tb., Tz. 5.4; 23. Tb., Tz. II-4.3). Über die im letzten Bericht erwähnte Verfassungsbeschwerde, die von den Datenschutzbeauftragten unterstützt worden war, ist nunmehr entschieden worden (Verfassungsbeschwerde gegen das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern – Antiterrordateigesetz). Sie hatte zu einem erheblichen Teil Erfolg (Urteil des Bundesverfassungsgerichts vom 24. April 2013, Az. 1 BvR 1215/07).

Die Antiterrordatei ist danach zwar in ihren Grundstrukturen mit dem Recht auf informationelle Selbstbestimmung vereinbar. Allerdings müssen die Regelungen hinsichtlich der zu erfassenden Daten und deren Nutzungsmöglichkeiten normenklar und in der Sache hinreichend begrenzt ausgestaltet sein sowie qualifizierte Anforderungen an die Kontrolle vorsehen. Das Antiterrordateigesetz genügt diesen Maßstäben nicht vollständig. Im Einzelnen hat das Bundesverfassungsgericht Folgendes festgestellt:

§ 1 Abs. 2 ATDG, der die Beteiligung weiterer Polizeivollzugsbehörden an der Antiterrordatei nur nach weiten und wertungsoffenen Kriterien regelt, ist mit dem Bestimmtheitsgebot unvereinbar.

Nicht in jeder Hinsicht mit den verfassungsrechtlichen Anforderungen vereinbar sind die Vorschriften, die den von der Datei erfassten Personenkreis festlegen. Die Vorschrift des § 2 Satz 1 Nr. 1 ATDG erfasst zunächst Angehörige, Unterstützer und unterstützende Gruppierungen von terroristischen Vereinigungen. Sie lässt zu, dass auch Personen erfasst werden, die im Vorfeld und ohne Wissen von einem Terrorismusbezug eine in ihren Augen unverdächtige Vereinigung unterstützen. Insoweit verstößt die Regelung nach dem Urteil des Bundesverfassungsgerichts gegen den Grundsatz der Normenklarheit und ist mit dem Übermaßverbot nicht vereinbar. Eine verfassungskonforme Auslegung scheidet hier aus.

Nicht vollständig mit der Verfassung vereinbar ist auch § 2 Satz 1 Nr. 2 ATDG. Die Vorschrift, die Einzelpersonen erfassen soll, die möglicherweise in einer Nähe zum Terrorismus stehen, verbindet eine Reihe von mehrdeutigen und potenziell weiten Rechtsbegriffen. Das bloße „Befürworten von Gewalt“ reicht für die Erfassung von Personen in der Antiterrordatei nicht. Die Vorschrift verstößt insoweit gegen das Übermaßverbot. Das Gesetz macht hier die subjektive Überzeugung als solche zum Maßstab und legt damit Kriterien zugrunde, die vom Einzelnen nur begrenzt beherrscht und durch rechtstreues Verhalten nicht beeinflusst werden können.

Verfassungswidrig ist § 2 Satz 1 Nr. 3 ATDG. Nach dieser Regelung sind die einfachen Grunddaten in die Datei einzustellen, soweit Kontaktpersonen von einem Terrorismusbezug der Hauptperson nichts wissen, bei Kenntnis vom Terrorismusbezug auch die erweiterten Grunddaten. Infolgedessen erstreckt sich der Austausch von Klarinformationen zwischen den beteiligten Behörden auch auf Daten zu den Kontaktpersonen. Die Regelung ist weder mit dem Bestimmtheitsgrundsatz noch mit dem Übermaßverbot vereinbar. Möglich wäre es, Kontaktpersonen mit wenigen Elementardaten zu erfassen und diese – als Information zu der terrorismusnahen Hauptperson – nur verdeckt recherchierbar zu speichern.

Die nach § 3 Abs. 1 Nrn. 1a und 1b ATDG erfassten Datenkategorien müssen veröffentlicht werden.

Nicht in jeder Hinsicht mit dem Übermaßverbot vereinbar sind die Regelungen zur Verwendung der Daten. Mit dem Übermaßverbot nicht vereinbar ist die Regelung zur sog. Inverssuche (§ 5 Abs. 1 Satz 2 Nr. 1a ATDG). Hierbei handelt es sich um merkmalbezogene Recherchen in den erweiterten Grunddaten, die der abfragenden Behörde im Trefferfall nicht nur eine Fundstelle zu weiterführenden Informationen vermitteln, sondern unmittelbar Zugang zu den entsprechenden einfachen Grunddaten verschaffen. So kann eine Behörde z.B. nach Personen mit einer bestimmten Religionszugehörigkeit und Ausbildung, die einen bestimmten Treffpunkt frequentieren, suchen und erhält im Trefferfall nicht nur die Angabe, welche Behörde darüber Informationen

besitzt, sondern auch die Namen, Adressen sowie weitere Grundinformationen von allen Personen, auf die die abgefragten Merkmale zutreffen. Eine solch weitgehende Nutzung trägt der inhaltlichen Reichweite der erweiterten Grunddaten nicht hinreichend Rechnung. Wenn sich eine Recherche auch auf erweiterte Grunddaten erstreckt, dürfen nur das Aktenzeichen und die informationsführende Behörde angezeigt werden, nicht aber auch die korrespondierenden einfachen Grunddaten.

Schließlich müssen die Aufsichtsinstanzen auf Bundes- wie auf Landesebene – also auch die Datenschutzbeauftragten – wie nach geltendem Recht die Datenschutzbeauftragten – mit wirksamen Befugnissen ausgestattet sein. Zugriffe und Änderungen im Datenbestand müssen vollständig protokolliert und den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung gestellt werden. Kontrollen sind in angemessenen Abständen durchzuführen, deren Dauer ein gewisses Höchstmaß – etwa zwei Jahre – nicht überschreiten darf. Hinsichtlich des Erfordernisses turnusmäßig festgelegter Pflichtkontrollen fehlt es an einer hinreichenden gesetzlichen Vorgabe; den Gesetzgeber trifft insoweit eine Nachbesserungspflicht. Im Übrigen sind die Vorschriften verfassungskonform auszulegen. Der Gesetzgeber hat im Übrigen zu beobachten, ob Konflikte auftreten, die gesetzlicher Klarstellungen oder der Einführung etwa von Streitlösungsmechanismen wie dem Ausbau von Klagebefugnissen bedürfen.

Zur Gewährleistung von Transparenz und Kontrolle bedarf es außerdem einer gesetzlichen Regelung von Berichtspflichten. Regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit über Datenbestand und Nutzung der Antiterrordatei sind sicherzustellen.

Die teilweise Verfassungswidrigkeit der angegriffenen Vorschriften führt nicht zu deren Nichtigkeit, sondern nur zur Feststellung ihrer Unvereinbarkeit mit dem Grundgesetz. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014, dürfen die Vorschriften unter gewissen Voraussetzungen weiter angewendet werden.

Der LfDI hat das Innenministerium angeschrieben und angeregt, die Feststellungen des Bundesverfassungsgerichts bereits vorab im Vollzug umzusetzen. So sollten z.B. Kontaktpersonen schon jetzt aus den Datenbanken gelöscht werden.

Weiterhin hat der LfDI darauf hingewiesen, dass die Entscheidung des Bundesverfassungsgerichts zur Antiterrordatei auf die Rechtsextremismusdatei zu übertragen sei und daher die verfassungsgerichtlichen Anforderungen auch auf diese Datei zu erstrecken seien (vgl. 23. Tb., Tz. II-4.3).

Das Innenministerium hat diesen Anliegen zwischenzeitlich entsprochen.

Außerdem hat der LfDI eine Prüfung rheinland-pfälzischer Speicherungen und Nutzungen der Antiterrordatei in Angriff genommen. Es war zunächst festzustellen, dass die vom Bundesverfassungsgericht geforderten Kontrollen nicht möglich waren, da die Datei in einer nicht kontrollfähigen Weise geführt wurde. Das Bundeskriminalamt war zunächst trotz einer Anmahnung nicht in der Lage, die Inhalte der Protokollierungen in einer für Kontrollmaßnahmen geeigneten Weise zur Verfügung zu stellen. Zwischenzeitlich hat das Bundeskriminalamt Protokolldaten übersandt. Die Prüfung dieser Dateien dauert derzeit noch an.

4.1.10 Funkzellenabfragen

Bereits im letzten Tätigkeitsbericht 2010/2011 hat der LfDI die Problematik der Funkzellenabfragen geschildert (vgl. 23. Tb., Tz. I-8.2.7). Eine Funkzelle ist eine Vermittlungsstelle für Mobilfunkverbindungen und sonstige Dienste. Erfolgt ein Verbindungsaufbau von einem Mobiltelefon aus oder zu einem solchen Gerät, werden Daten gespeichert, um die Kommunikation zu ermöglichen und die Verbindungskosten zu dokumentieren. Zu diesen Daten zählen die Rufnummern der Gesprächsteilnehmerinnen und -teilnehmer, Zeit, Verbindungsdauer, Art des genutzten Dienstes (z.B. SMS), die Identifizierungskennzeichnung der Funkzelle und deren Geo-Koordinaten.

Eine Datenspeicherung erfolgt bei aktiven (Anruferin/Anrufer) und bei passiven Kommunikationsvorgängen (Angerufene/Angerufener) und wird erst nach Ablauf einer vom Netzbetreiber bestimmten Frist gelöscht. Da sich ein Mobilfunkgerät immer in

die örtlich am nächsten liegende Funkzelle „einbucht“, bedeutet dies, dass sich das Mobilfunkgerät und seine Nutzerin oder sein Nutzer im räumlichen Umfeld der Funkzelle aufhält. Je nach Größe der Funkzelle kann die Distanz wenige Meter oder einige Kilometer betragen. Hierdurch ergibt sich ein Rückschluss auf den Aufenthaltsort der Nutzerin oder des Nutzers.

Die Zellen werden in Deutschland von vier Netzbetreibern unterhalten und decken die gesamte Fläche der Bundesrepublik Deutschland ab. Hinsichtlich der technischen Grundausstattung einer Netzzelle und ihrer Reichweite bestehen Unterschiede, die sich am Bedarf sowie an regionalen und geografischen Gegebenheiten orientieren.

Der LfDI hatte in seinem 23. Tätigkeitsbericht auch auf die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011, „Funkzellenabfrage muss eingeschränkt werden“, hingewiesen. Die an den Gesetzgeber gerichteten Forderungen in diesem Zusammenhang sind leider nicht umgesetzt worden. Vor diesem Hintergrund schien es geboten, in Zusammenarbeit mit dem rheinland-pfälzischen Ministerium des Innern, für Sport und Infrastruktur eine Handlungsanleitung für die Polizeibehörden zu erstellen, die die rechtsstaatliche Eingrenzung dieser Maßnahme befördern sollte.

Dabei war es dem LfDI besonders wichtig, Vorkehrungen vorzusehen, die das Ziel unterstützen, möglichst keine Daten von Unbeteiligten zu erheben. Dieser Gesichtspunkt soll bereits bei der Selektierung der Funkzelle, der zeitlichen Eingrenzung und im Rahmen der sich anschließenden Auswertung Berücksichtigung finden. Die mit dem LfDI abgestimmte Richtlinie zur „Funkzellenabfrage und -auswertung“ steht der polizeilichen Praxis seit Ende 2012 zur Verfügung und soll zukünftig regelmäßig an die technische und rechtliche Entwicklung gepasst werden.

Durch Funkzellenabfragen erhalten die Sicherheitsbehörden einen Überblick, welche Mobilfunkgeräte sich zu einem bestimmten Zeitpunkt an einer bestimmten Örtlichkeit befunden haben. Dies allerdings nur, wenn durch aktive oder passive Kommunikation auch ein Verkehrsdatum erzeugt wurde.

4.1.11 Stille SMS

Die „stille SMS“, auch „Stealth SMS“ oder „Ping“, ist ein Ermittlungsinstrument der Sicherheitsbehörden, das zur Lokalisierung von Mobilfunkgeräten eingesetzt wird. Bei einer stillen SMS wird eine textfreie Nachricht an das Zielgerät gesandt, welches lokalisiert werden soll. Dadurch wird ein Verkehrsdatum bei der Funknetzzelle generiert (siehe Funkzellenabfrage), in der das Zielgerät aktuell eingebucht ist. Diese SMS wird am Empfangsgerät nicht angezeigt und erzeugt auch kein akustisches Signal. Das „künstlich erzeugte“ Verkehrsdatum erlaubt bei einem eingeschalteten Mobilfunktelefon dessen Lokalisierung über den Standort der Funkzelle. Werden stille SMS in einem sehr kurzen Abstand an das Zielgerät gesandt, kann dadurch ein detailliertes Bewegungsprofil erstellt werden. Diese technischen Gegebenheiten werden von den Sicherheitsbehörden genutzt, um Standortbestimmungen zur Erforschung eines Sachverhaltes vorzunehmen oder den Aufenthaltsort von Gesuchten zu ermitteln.

Die datenschutzrechtliche Problematik des Einsatzes der stillen SMS durch die Polizei wird bereits seit Längerem erörtert (19. Tb., Tz. 7.3.3; 23. Tb., Tz. I-8.2.6). Inzwischen besteht weitgehend Einigkeit, dass als spezifische Rechtsgrundlage für die Erhebung von Standortdaten in Echtzeit für Strafverfolgungszwecke § 100g Abs. 1 StPO anzusehen ist. Zum Zwecke der Gefahrenabwehr kann die rheinland-pfälzische Polizei stille SMS auf der Grundlage von § 31a POG einsetzen. Ein klassischer Anwendungsfall stellt hier die Suche nach einer vermissten Person dar.

Auf Nachfrage wurde dem LfDI durch das rheinland-pfälzische Innenministerium mitgeteilt, dass die Polizei des Landes im Jahr 2011 über 150.000 sog. „stille SMS“ zu 541 Vorgängen versandt hat. Im Hinblick auf die große Zahl von durchgeführten Maßnahmen war die Verhältnismäßigkeit der Nutzung dieses Instruments sowie der Umgang mit den erhobenen Daten in Bezug auf verfahrenssichernde Maßnahmen zu prüfen. In Zusammenarbeit mit dem rheinland-pfälzischen Ministerium des Innern, für Sport und Infrastruktur wurden die bestehenden Abläufe erhoben und unter Datenschutzaspekten überprüft.

In einer „Richtlinie stille SMS“ wurden dann die erforderlichen Festlegungen getroffen. Dem abschließenden Regelungsentwurf konnte der LfDI Anfang 2013 zustimmen, so dass den Beamtinnen und Beamten des Polizeidienstes in Rheinland-Pfalz ein zur Aufgabenwahrnehmung geeigneter und aus datenschutzrechtlicher Sicht nicht zu beanstandender Umgang mit dem Ermittlungsinstrument „stille SMS“ erleichtert wird.

4.1.12 Datenschutzaudit des Polizeilichen Informationssystems (POLIS)

Mit § 41a POG existiert eine ausdrückliche Regelung zum technisch-organisatorischen Datenschutz in den polizeilichen Verfahren.

Sie sieht u.a. vor, dass die von der Polizei eingesetzten IT-Verfahren und technischen Einrichtungen durch unabhängige Stellen geprüft und bewertet werden können (IT-Sicherheits- und Datenschutzaudit). Der LfDI empfahl dem Innenministerium, ein solches Audit bezogen auf POLIS durchführen zu lassen. Das Innenministerium hat dies aufgegriffen und ein entsprechendes Audit durch eine akkreditierte Prüfstelle beauftragt.

POLIS ist die landesseitige Komponente des beim Bundeskriminalamt zentral für die Landespolizeien betriebenen Verfahrens INPOL und enthält neben den dort nachgewiesenen Einträgen auch die Daten, die nicht INPOL-relevant sind, also nicht von länderübergreifender, internationaler oder erheblicher Bedeutung sind (§ 2 BKA-Gesetz). Das Audit betraf ausschließlich die landesseitigen Verarbeitungsschritte; einbezogen wurde dabei auch die Schnittstelle zum Vorgangsbearbeitungssystem POLADIS der Polizei.

Grundlage der Auditierung waren die Anforderungen aus dem Datenschutz-Baustein der Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik sowie ergänzende Vorgaben des Innenministeriums. Dies umfasste wesentliche Bereiche wie

- das Datenschutzmanagement im Bereich der Polizei,
- die technisch-organisatorischen Datenschutzmaßnahmen,
- die Sicherstellung der Rechte der Betroffenen (Auskunft, Unterrichtung),
- die Löschung nicht mehr erforderlicher Daten,
- die Nachvollziehbarkeit der Nutzung des Verfahrens (Protokollierung/Auswertung),
- die verfahrensbezogene Aus- und Fortbildung.

Nach dem Ergebnis des Audits werden die datenschutzrechtlichen Anforderungen insgesamt angemessen und in weiten Teilen in vorbildlicher Weise umgesetzt.

Unabhängig davon zeigt das Audit weitere Optimierungsmöglichkeiten auf. Diese betreffen z.B. eine verbesserte Dokumentation der getroffenen Datenschutz- und Sicherheitsmaßnahmen, verstärkte Schulungen der behördlichen Datenschutzbeauftragten oder Stichprobenüberprüfungen bei automatisierten Datenübermittlungen.

Aus Sicht des LfDI dokumentiert das Audit das vergleichsweise hohe Datenschutzniveau im Verfahren POLIS und ist geeignet, etwaigen Befürchtungen hinsichtlich einer unkontrollierten Datenverarbeitung durch die Polizei entgegenzutreten. Neben POLIS spielen in diesem Zusammenhang auch andere zentrale Verfahren der Polizei ein Rolle. Vor dem Hintergrund der Diskussion um die Instrumente Online-Durchsuchung und Telekommunikationsüberwachung sollten entsprechende Untersuchungen insbesondere auch für diesen Bereich in Betracht gezogen werden.

4.2 Verfassungsschutz

Im Berichtszeitraum hat der LfDI eine umfangreiche, anlassunabhängige datenschutzrechtliche Überprüfung von Datenverarbeitungen des rheinland-pfälzischen Landesamtes für Verfassungsschutz begonnen (§ 19 LVerfSchG). Bis Redaktionsschluss wurden mehr als zehn örtliche Feststellungen durchgeführt und dabei unterschiedliche Themen aufgearbeitet.

Für einzelne Aufgabenbereiche des rheinland-pfälzischen Verfassungsschutzes hat der LfDI aufgrund gesetzlicher Vorgaben keine Kontrollbefugnis. Dies betrifft zunächst alle TKÜ-Überwachungsmaßnahmen des Verfassungsschutzes (gemäß § 6

G10AG). Insoweit ist allein das entsprechende Gremium des Landtags (die G-10-Kommission) überprüfungsbefugt. Außerdem unterliegt das Abhören von Wohnungen gemäß § 10b LVerfSchG der gerichtlichen Anordnungsbefugnis. Auch dieser Bereich ist von der Kontrolle durch den LfDI ausgenommen (§ 10c Abs. 1 Satz 2 LVerfSchG).

Die Schwerpunkte der datenschutzrechtlichen Überprüfung lagen deshalb im Bereich der Einhaltung der datenschutzrechtlichen Vorgaben nach §§ 11 ff. LVerfSchG. Dazu gehörte die Prüfung, ob personenbezogene Daten, die in Dateien gespeichert sind, durch Akten oder andere Datenträger belegbar waren. Weiter wurde geprüft, ob Daten über Unbeteiligte (Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst verfassungsfeindlichen Bestrebungen nachgehen), nur innerhalb der dafür geltenden engen Schranken gespeichert wurden. Außerdem ging es auch um die Frage, ob die gesetzlichen Löschungsvorgaben eingehalten werden (§ 12 LVerfSchG). Dabei wurde den Daten von Minderjährigen, die nur unter besonders engen Voraussetzungen durch den Verfassungsschutz erfasst und gespeichert werden dürfen (§ 17 LVerfSchG), besondere Aufmerksamkeit gewidmet. Auch die vorhandenen technischen und organisatorischen Datenschutzmaßnahmen wurden überprüft. Schließlich wurde die Auskunftserteilung und die Datenweitergabe an Dritte in die Prüfung einbezogen.

Die Antiterrordatei, eine gemeinsam von Polizei und Verfassungsschutz betriebene Datei, war Gegenstand besonderer Aufmerksamkeit. Grundlage der Prüfung waren Protokolldaten, die vom Bundeskriminalamt beschafft werden mussten. Die entsprechenden Auswertungen konnten noch nicht abgeschlossen werden (vgl. Tz. III-4.1.9).

Die Prüfung vor Ort wurde im Berichtszeitraum abgeschlossen. Derzeit wird an der Erstellung des Abschlussberichts gearbeitet. Er wird demnächst vorgelegt werden.

5. Soziales und Gesundheit

5.1 Soziales

5.1.1 Internetrecherche durch Jugendämter

Mit dem Einzug des Internets in den Alltag der Menschen bieten sich der öffentlichen Verwaltung völlig neue Möglichkeiten der Datenerhebung (vgl. 23. Tb., Tz. I-3.2.5). Fraglich ist dabei regelmäßig, ob und ggf. welche Schranken das informationelle Selbstbestimmungsrecht den Behörden setzt. Im Berichtszeitraum wandten sich mehrere Jugendämter an den LfDI, um die datenschutzrechtliche Zulässigkeit einer von ihnen erwogenen Internetrecherche klären zu lassen.

Eine bereichsspezifische Vorgabe, die die Nutzung des Internets zur Sachverhaltsaufklärung durch die Jugendämter regelt, existiert nicht. Aufgrund dessen muss auf die allgemeinen Maßstäbe, die das Bundesverfassungsgericht im Zusammenhang mit seiner Entscheidung vom 27. Februar 2008 zur sog. Online-Durchsuchung (BVerfGE 120, 274 ff.) aufgestellt hat, zurückgegriffen werden. Hiernach bewirke die reine Internetaufklärung als solche keinen Eingriff in das informationelle Selbstbestimmungsrecht. Darüber hinaus sei selbst bei einer Kommunikationsbeziehung im Internet, die – wie bei sozialen Netzwerken – eine elektronische Gemeinschaft gebildet habe, das Vertrauen der Kommunikationsteilnehmerinnen und -teilnehmer in die Identität und die Wahrhaftigkeit der Kommunikationspartnerinnen und -partner nicht schutzwürdig, so dass auch das Auftreten staatlicher Stellen unter einer Legende nicht automatisch einen Grundrechtseingriff bedeute. Das gezielte Zusammentragen und Speichern der in sozialen Netzwerken allgemein zugänglichen Inhalte könne zwar einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellen und eine besondere Gefahrenlage für die Persönlichkeit der Betroffenen erzeugen. Bei Vorliegen einer Ermächtigungsgrundlage sei dies allerdings zulässig.

Auf der Grundlage dieser Vorgaben des Bundesverfassungsgerichts vertritt der LfDI zur Nutzung des Internets durch Jugendämter folgende Rechtsauffassung:

- Das **gezielte** Zusammentragen, Speichern und Auswerten der frei im Internet verfügbaren personenbezogenen Informationen greift in das informationelle Selbstbestimmungsrecht der Betroffenen ein. Ein derartiges Handeln wäre nur bei Vorliegen einer Ermächtigungsgrundlage zulässig. Im Hinblick auf die unterschiedlichen Aufgaben eines Jugendamtes sind in diesem Falle die Voraussetzungen der §§ 62 SGB VIII oder 67a SGB X zu prüfen.

- Bei der Recherche personenbezogener Informationen in sozialen Netzwerken, wie z.B. Facebook, gelten die dargelegten Grundsätze gleichfalls, sofern die konkret erhobenen Daten als frei zugänglich im Sinne der Rechtsprechung des Bundesverfassungsgerichts qualifiziert werden können. Richten die sich in dem Netzwerk enthaltenen Informationen an alle Mitglieder oder einen nicht weiter abgegrenzten Personenkreis dieser elektronischen Gemeinschaft, wäre das gezielte Zusammentragen, Speichern und Auswerten dieser Daten bei Vorliegen einer Verarbeitungsbefugnis zulässig. Dies wäre z.B. bei Informationen auf Pinnwänden oder in Gästebüchern der Fall, nicht aber bei Daten, die nur einem bestimmten Personenkreis wie z.B. sog. „Freunden“ zugänglich sind.

- Auf der Grundlage der Entscheidung des Bundesverfassungsgerichts wäre bei Vorliegen der Erhebungsvoraussetzungen sowohl eine Recherche unter eigener Identität als auch unter einem Pseudonym („Legende“) zulässig. Gleichwohl sollten nach Auffassung des LfDI die Jugendämter Pseudonyme im Rahmen einer Internetrecherche in elektronischen Gemeinschaften nur sparsam und nur dann einsetzen, wenn dies zur Aufgabenerfüllung zwingend erforderlich ist, da sie als staatliche Stellen grundsätzlich zu einem transparenten Handeln verpflichtet sind.

5.2 Gesundheit

5.2.1 Einsatz intelligenter Assistenzsysteme im Gesundheits- und Pflegebereich

Der LfDI begleitete im Berichtszeitraum ein seitens der Landesregierung unterstütztes wissenschaftliches Verbundprojekt zur telemedizinischen Betreuung von Menschen mit Herzinsuffizienz und Herzrhythmusstörungen. Bei dem federführend durch ein rheinland-pfälzisches Klinikum geführten Vorhaben war vorgesehen, auf der Grundlage eines detaillierten Versorgungskonzeptes intelligente Assistenzsysteme (sog. Ambient-Assisted-Living Technologien, kurz AAL) einzusetzen. Dabei sollten zwischen den Behandlungsterminen bei Fachärztinnen und -ärzten bzw. im Krankenhaus Vitalparameter der zu Hause lebenden Patientinnen und Patienten über ein Fernüberwachungssystem an die Behandelnden übermittelt werden. Die Nutzung der AAL-Technologie diente dem Zweck, die Patientensicherheit im häuslichen Alltag permanent zu erhöhen und ggf. entstehende Gefahrensituationen frühzeitig zu erkennen und behandeln zu können. Technische Grundlage der Datenübermittlung war ein zwischen der behandelnden Ärzteschaft und Kliniken aufgebautes Telemedizin-Netzwerk einschließlich geeigneter Telemonitoring-Systeme.

Intelligente Assistenzsysteme dienen primär dem Erhalt eines selbstbestimmten und unabhängigen Lebens der Betroffenen im eigenen häuslichen Umfeld. Den in unterschiedlichen Bereichen einsetzbaren Systemen ist eigen, dass sie je nach Ausgestaltung selbstlernend agieren, autonom Informationen austauschen, Verhaltens- und Kontextanalysen vornehmen und situationsbedingt reagieren. Mögliche Einsatzgebiete der AAL-Technologie sind neben der Telemedizin u.a. die Hausgeräte- oder die Kommunikationstechnik. Im Gesundheits- und Pflegebereich kommt den intelligenten Assistenzsystemen vor dem Hintergrund des demografischen Wandels zunehmende Bedeutung zu, da mit ihrem Einsatz ein möglichst langer Aufenthalt älterer oder pflegebedürftiger Menschen in ihrer eigenen Wohnung erreicht werden könnte.

Soweit intelligente Assistenzsysteme menschliches Verhalten betreffen, werden durch sie regelmäßig auch personenbezogene Daten verarbeitet. Der Einsatz von AAL-Technologie muss in diesem Fall im Einklang mit dem Datenschutzrecht stehen.

Der LfDI hat die Durchführung des wissenschaftlichen Vorhabens auf der Grundlage einer informierten Einwilligung für zulässig bewertet. Allerdings zeigte sich deutlich, dass das Instrument der Einwilligung als Rechtsgrundlage für eine umfassende Verarbeitung schutzbedürftiger Vital- und Bewegungsdaten der Patientinnen und Patienten durch eine Vielzahl von Stellen an seine Grenzen stößt. Letztlich war es aus der Sicht des LfDI kaum möglich, die Betroffenen gemäß § 5 Abs. 2 Satz 2 LDSG angemessen über die teilweise äußerst komplexe technische Struktur des Verfahrens und die damit zusammenhängenden Datenflüsse aufzuklären. Auch ist es diskussionswürdig, ob in solchen Zusammenhängen überhaupt noch von einer „freien Entscheidung“ der Betroffenen gesprochen werden kann. Denn ausschlaggebend für die Erteilung einer Einwilligung wird in der Praxis für die Patientinnen und Patienten vorrangig der mit der Zustimmung zu erlangende persönliche Vorteil sein, ohne die mit der eingesetzten Technik ggf. verbundenen Grundrechtsgefährdungen überhaupt noch in die eigene Interessenabwägung mit einfließen zu lassen.

Angesichts des demografischen Wandels und des damit einhergehenden Kostendrucks in den Sozialversicherungen wird der Einsatz intelligenter Assistenzsysteme im Gesundheits- und Pflegebereich in Zukunft zunehmen. Die Landesregierung hat wiederholt bekräftigt, dass für sie die Erhaltung eines selbstbestimmten Lebens möglichst im gewohnten Umfeld auch im Alter und bei Pflege- und Unterstützungsbedarf höchste Priorität habe. Hierzu gehöre auch der Grundsatz „ambulant vor stationär“. Der LfDI hält dies durchaus für nachvollziehbar. Allerdings muss hierbei eben auch das Datenschutzgrundrecht der Betroffenen gewahrt bleiben.

Aus Sicht des LfDI sollten die Betroffenen grundsätzlich darauf vertrauen können, dass bei dem Einsatz derartiger Systeme im Gesundheits- und Pflegebereich die sie betreffenden Daten von allen Beteiligten datenschutzgerecht verarbeitet werden. Denn die mit der AAL-Technologie verbundenen Chancen zur Beibehaltung eines weitgehend selbstbestimmten und unabhängigen Lebens auch im Krankheits- oder Pflegefall dürfen nicht mit einem

unverhältnismäßigen Verlust an Vertraulichkeit oder Privatheit für die Patientinnen und Patienten erkauft werden. Es bedarf deshalb ausdrücklicher rechtlicher und technischer Standards, um das informationelle Selbstbestimmungsrecht der Betroffenen effektiv zu schützen. Vor diesem Hintergrund plädiert der LfDI dafür, die aus dem informationellen Selbstbestimmungsrecht resultierenden Anforderungen an den Einsatz einer derartigen Technologie rechtzeitig und umfassend festzulegen:

- Der Gesetzgeber ist aufgefordert, die datenschutzrechtlichen Mindestanforderungen an die Gestaltung der informationstechnischen Abläufe beim Einsatz intelligenter Assistenzsysteme im Gesundheits- und Pflegebereich zu definieren und damit frühzeitig die Entwicklung datenschutzgerechter Systeme sicherzustellen (privacy by design). Denkbar ist, wie im Bereich der elektronischen Gesundheitskarte, zumindest gesetzliche Rahmenbedingungen für die jeweils einzusetzende technische Infrastruktur zu schaffen.

- Die Anforderungen an eine datenschutzrechtliche Einwilligung und das Einwilligungsverfahren müssen gesetzlich präzisiert werden, sofern es bei der Nutzung von AAL-Technologien zu einer Verarbeitung personenbezogener Daten kommt. Es muss sichergestellt werden, dass die Betroffenen ihre Rechte, insbesondere auf Auskunft und Löschung, unabhängig von der Zahl der an einem telemedizinischen oder vergleichbaren Vorhaben beteiligten Stellen, einfach und umfassend wahrnehmen können. Auf die Gewährleistung von Transparenz bei der Datenverarbeitung ist dabei besonders Wert zu legen.

Es bleibt zu hoffen, dass die datenschutzrechtlichen Rahmenbedingungen für den Einsatz intelligenter Assistenzsysteme im Gesundheits- und Pflegebereich bei der Etablierung derartiger Technologien frühzeitig beachtet werden. Aus der Sicht des Datenschutzes ist es nur zu begrüßen, wenn ältere Menschen oder Pflegebedürftige im Interesse eines selbstbestimmten und unabhängigen Lebens so lange wie möglich ihr häusliches Umfeld bewahren können. Dass dies nicht dazu führen darf, das informationelle Selbstbestimmungsrecht der Betroffenen über Bord zu werfen, ist jedoch selbstverständlich. Vor diesem Hintergrund hat der Staat seiner Verpflichtung zu einem wirksamen Grundrechtsschutz nachzukommen.

5.2.2 Schutz von Patientendaten in der Universitätsmedizin Mainz

Die besondere Situation der Universitätsmedizin Mainz ist dadurch gekennzeichnet, dass diese einerseits Klinikum mit einer großen Zahl von Fachkliniken ist und andererseits Fachbereich der Johannes Gutenberg-Universität. Dies führt dazu, dass Krankenversorgung, Forschung und Lehre eng miteinander verbunden sind, eine strikte Trennung häufig nur bedingt möglich ist und sich vielfältige und teils gegenläufige Anforderungen ergeben. Unbestreitbar und unbestritten steht dabei eine optimale Patientenversorgung und das Patientenwohl im Vordergrund. Mit Blick auf die grundgesetzlich garantierte Forschungsfreiheit ist aus Sicht des LfDI auch anzuerkennen, dass deren Belange grundsätzlich gleichwertig mit den Anforderungen des Datenschutzes berücksichtigt werden müssen.

Um dem angemessen entsprechen zu können, bedarf es einer IT-Struktur, welche die für die jeweilige Aufgabenerfüllung benötigten Daten bereitstellt, gleichzeitig jedoch gewährleistet, dass Patientendaten vor unbefugter oder unnötiger Kenntnisnahme geschützt sind. Die angemessene Berücksichtigung beider Seiten erfordert verbindliche Regelungen und technisch unterlegte Verfahrensweisen für den Zugriff auf Patientendaten und den Datenaustausch zwischen den Bereichen Klinische Versorgung und Forschung und Lehre.

Hierzu hatte der LfDI Empfehlungen ausgesprochen. Diese zielen auf die Einrichtung separater Netzsegmente für die Bereiche Klinische Versorgung, Lehre und Forschung sowie die Einführung geeigneter Schutzmaßnahmen. Neben einer solchen Aufteilung des Netzes sollte eine Rollen- und Berechtigungskonzeption vorgesehen werden, die netzweit die Voraussetzungen und Verfahrensweisen für interne und externe Zugriffe auf die in den verschiedenen Netzsegmenten angesiedelten Daten, Systeme und Verfahren festlegt. Notwendige Voraussetzung hierfür ist ein Sicherheits- und Datenschutzkonzept, welches grundlegende Vorgaben zur IT-Infrastruktur der Universitätsmedizin macht, Sicherheitsleitlinien für den Zugang zu IT-Systemen und Anwendungen

und für den Datenaustausch formuliert und Verantwortlichkeiten beschreibt.

Derzeit sind an der Universitätsmedizin zwar vereinzelt entsprechende Ansätze vorhanden, diese sind jedoch auf Teilbereiche beschränkt und nicht in ein Gesamtkonzept eingebunden; sie sollten jedoch flächendeckend und verbindlich umgesetzt werden. Trotz langjähriger Vorarbeiten wurde ein hierfür notwendiges Gesamtkonzept bislang nicht verabschiedet. Es ist bislang nicht erkennbar, dass sich hinsichtlich eines übergreifenden Konzepts Fortschritte ergeben hätten.

Angesichts vorliegender Konzeptentwürfe geht es aus Sicht des LfDI dabei weniger um die Frage, welche Maßnahmen im Rahmen einer Neukonzeption zu ergreifen wären, sondern vielmehr darum, dass vom Klinikvorstand verbindliche Vorgaben formuliert werden, aus denen sich notwendige technische Maßnahmen und Verfahrensregelungen ableiten lassen. Der LfDI verkennt dabei nicht die Schwierigkeiten, für eine Einrichtung in der Größe und mit den Aufgaben der Universitätsmedizin IT-Strukturen zu betreiben, die den unterschiedlichen Anforderungen gerecht werden. Auch ist er sich der personellen und finanziellen Rahmenbedingungen bewusst, die dazu führen können, dass notwendige Maßnahmen nicht kurzfristig zum Abschluss gebracht werden können.

Die Einhaltung gesetzlicher Anforderungen darf jedoch nicht von finanziellen Erwägungen abhängig gemacht werden, zumal dann, wenn, wie vorliegend, besonders sensible personenbezogene Daten betroffen sind. Zuzugestehen ist, dass unter Umständen nicht alle im Rahmen einer Neustrukturierung erforderlichen Maßnahmen kurzfristig umzusetzen sind und notwendige Vorhaben ggf. zeitlich und finanziell aufgeteilt werden müssen. Voraussetzung dafür ist jedoch eine Planung, die vordringliche Maßnahmen priorisiert und erkennen lässt, in welchen Schritten die Neustrukturierung vorgenommen werden soll.

Das Fehlen eines verbindlichen, vom Vorstand verabschiedeten Konzepts für die Neustrukturierung der IT der Universitätsmedizin stellt einen grundlegenden und mittlerweile dauerhaften Mangel dar. Es ist nicht hinnehmbar, dass für einen derart bedeutenden IT-Verbund wie die Universitätsmedizin keine verbindlichen Leitlinien und kein allgemeines Sicherheits- und Datenschutzkonzept existieren.

Trotz mehrfacher konzeptioneller Ansätze steht eine entsprechende Leitlinie nach wie vor aus. Hier sieht der LfDI dringenden Handlungsbedarf.

6. Schuldatenschutz und Wissenschaft

6.1 Schuldatenschutz

6.1.1 Facebook als Lernplattform

Im schulischen Alltag besteht für Lehrkräfte nicht selten das Erfordernis, mit Schülerinnen und Schülern auch nach dem Präsenzunterricht noch in schulischen Angelegenheiten zu kommunizieren. Wenn diese Kommunikation unmittelbaren Unterrichtsbezug hat, steht vielen Schulen mit der Software „Moodle“ hierfür eine eigene kostenlose Lernplattform zur Verfügung (vgl. Tz. II-2.5). Die Vorteile dieser Plattform liegen u.a. darin, dass eine Trennung zwischen dienstlichen und privaten Inhalten möglich ist und die Datensicherheit durch die Verwendung von landeseigenen Servern sichergestellt ist.

Würde eine Schule gleichwohl Facebook als Lernplattform nutzen, wäre dies datenschutzrechtlich aus folgenden Gründen unzulässig:

- Verstoß gegen den Grundsatz der Erforderlichkeit, da der Einsatz von Facebook für Unterrichtszwecke nicht zur Erfüllung des Bildungs- und Erziehungsauftrages der Schule erforderlich ist;
- Verstoß gegen die Bestimmungen zum technisch-organisatorischen Datenschutz, da die Datensicherheit bei einer Datenverarbeitung in den USA nicht sichergestellt werden kann;
- Verstoß gegen die Bestimmungen zur Auftragsdatenverarbeitung;
- Verstoß gegen die Bestimmungen des Telemediengesetzes.

6.1.2 Facebook-Freundschaften zwischen Lehrkräften und Schülerinnen und Schülern

Wenn eine Lehrkraft über einen eigenen privaten Facebook-Account verfügt, stellt sich die Frage, ob sie sich mit Schülerinnen und Schülern im Sinne der Facebook-Terminologie „befreunden“ darf.

Das Meinungsbild reicht hierbei von einer „Facebook-Pflicht“ für Lehrkräfte bis hin zu einem Verbot von Facebook-Freundschaften zwischen Lehrkräften und Schülerinnen und Schülern. Vermittelnde Positionen lassen unter bestimmten Voraussetzungen, wie z.B. dem Anlegen eines Zweitprofils oder der Bildung von geschlossenen Benutzergruppen, Facebook-Kontakte zu.

Aus datenschutzrechtlicher Sicht hätte eine Facebook-Freundschaft zur Folge, dass Lehrkräfte und Schülerinnen und Schüler wechselseitig Einblick in die jeweils anderen Profile und die dort hinterlegten Daten und Fotos erhalten. Sie könnten erfahren, wer, wann und auf welcher Webseite den Like Button betätigt hat, welche Nachricht auf einer „befreundeten“ Pinnwand gepostet wurde und was sonst noch aus dem realen Leben bei Facebook preisgegeben wird. Über die „benutzerdefinierten Freundeslisten“ kann man zwar die Zugriffsmöglichkeiten der Facebook-Freundinnen und -Freunde in Bezug auf das eigene Profil einschränken; dies ist aber mit einem gewissen Aufwand verbunden und dürfte schon aus Bequemlichkeit in der Praxis kaum genutzt werden.

Facebook-Freundschaften zwischen Lehrkräften und Schülerinnen und Schülern sind aber auch deshalb problematisch, weil man nicht immer davon ausgehen kann, dass Schülerinnen und Schüler wirklich frei entscheiden können, ob sie die „Freundschaftsanfrage“ einer Lehrkraft akzeptieren. Ein Akzeptieren der Anfrage könnte mit der Befürchtung einhergehen, ansonsten schulische Nachteile zu erleiden. Bei Freundschaftsanfragen durch Schülerinnen und Schüler besteht umgekehrt für die Lehrkraft das Problem der Ungleichbehandlung und die Gefahr, dass die gebotene Trennung zwischen schulischen und privaten Angelegenheiten (Distanzgebot) unterlaufen wird. Darüber hinaus kann nicht ausgeschlossen werden, dass die Facebook-Nutzung durch Lehrkräfte Schülerinnen und Schüler überhaupt erst zu einer Facebook-Mitgliedschaft veranlasst, an Facebook bindet oder den Entschluss, das Angebot von Facebook nicht mehr zu nutzen, erschwert. Ganz abgesehen davon ist es mit dem Bildungs- und Erziehungsauftrag der Schule nicht zu vereinbaren, wenn das Geschäftsmodell von Facebook – „Verkauf“ persönlicher Daten für kommerzielle Zwecke – durch die Institution Schule und ihre Repräsentantinnen und Repräsentanten zumindest indirekt unterstützt wird.

Diese Bedenken können auch durch das Anlegen eines Zweit-Accounts, benutzerdefinierte Freundeslisten oder die Bildung einer geschlossenen Benutzergruppe nicht ausgeräumt werden.

Etwas anderes gilt freilich für die rein private Kommunikation von Lehrkräften. Dies betrifft aber die wenigen Fälle, in denen eine Lehrkraft einzelne Schülerinnen und Schüler aus dem privaten Umfeld kennt (Verwandtschaft, Nachbarschaft, Vereinsmitgliedschaft) und nicht unterrichtet.

Ende 2011 hatte sich der LfDI an das Bildungsministerium gewandt und angeregt, den Lehrkräften eine Orientierungshilfe zur Facebook-Nutzung im Schulbereich zur Verfügung zu stellen. Dies wurde in der Weise aufgegriffen, dass unter Beteiligung des LfDI ein Ergänzungskapitel „Datenschutzrechtliche Anforderungen bei der Verwendung von facebook im Schulbereich“ zum Handbuch „Schule.Medien.Recht. – Ein juristischer Wegweiser zum Einsatz digitaler Medien in der Schule“ erstellt wurde. Darin wird erläutert, warum Facebook für die schulische Kommunikation zwischen Lehrkraft und Schülerinnen und Schülern nicht in Betracht kommt.

Ergänzend hierzu hat das Bildungsministerium im Oktober 2013 allen Lehrkräften und pädagogischen Fachkräften über die Schulleitungen ein Merkblatt aushändigen lassen, in dem auf das Facebook-Nutzungsverbot für unterrichtliche Zwecke nochmals hingewiesen wird.

Auf Initiative des LfDI wurde in die JIM-Studie 2013 eine Frage zur Häufigkeit von Facebook-Freundschaften mit Lehrkräften aufgenommen. Die Ergebnisse liegen nunmehr vor und geben Anlass zur Sorge: Im Schnitt sind 37 Prozent der 12- bis 19-Jährigen mit einer Lehrkraft auf Facebook „befreundet“. Da es sich um eine bundesweite Studie handelt, liegen keine konkreten Zahlen für Rheinland-Pfalz vor; auch kann nicht evaluiert werden, ob sich durch das Verbot des Bildungsministeriums an den Zahlen etwas ändert. Der LfDI wird die Thematik aber weiterhin kritisch verfolgen und auch darauf hinwirken, dass die Absprachen mit dem Bildungsministerium tatsächlich eingehalten werden.

6.1.3 Datenaustausch bei Schulwechsel

Immer wieder spielt bei Anfragen an den LfDI der Umfang des Datenaustauschs zwischen abgebender und aufnehmender Schule eine Rolle. Die Schulordnungen lassen bei einem Wechsel der Schule nur auf den Einzelfall bezogene Datenübermittlungen zu; ein routinemäßiger Informationsaustausch ohne Beteiligung der betroffenen Schülerinnen und Schüler bzw. deren Erziehungsberechtigten ist daher nicht zulässig (vgl. § 89 Übergreifende Schulordnung).

Im Zuge der Reform der Berufsfachschule I beabsichtigte das Bildungsministerium, den Berufsbildenden Schulen eine Handreichung zur Verfügung zu stellen, die in dem Abschnitt „Pädagogische Prädiagnostik“ sog. Übergabegespräche mit der abgebenden Schule vorsah. Die in den Gesprächen mit den ehemaligen Klassenleitungen gewonnenen Informationen sollten dazu genutzt werden, eine sinnvolle Klasseneinteilung in der Berufsschule vorzunehmen und Hilfen frühzeitig anbieten zu können. Dadurch, dass die Schülerinnen und Schüler nur ein Jahr in der Berufsfachschule I bleiben, sei es – so die Verantwortlichen im Bildungsministerium – wichtig, möglichst früh an schulrelevante Informationen zu gelangen.

Datenschutzrechtlich problematisch war die angedachte Vorgehensweise deshalb, weil dieser Informationsaustausch ohne die betroffenen Schülerinnen und Schüler bzw. deren Erziehungsberechtigten stattfinden sollte. Mit dem Bildungsministerium wurde daher vereinbart, dass die Schülerinnen und Schüler nach ihrer Anmeldung bei der Berufsfachschule einen Fragebogen erhalten, der auf die Möglichkeit eines anlassbezogenen Datenaustauschs mit der abgebenden Schule hinweist und hierfür eine Einwilligungserklärung vorsieht.

6.1.4 Schulbuchausleihe

Nach der Einführung der Schulbuchausleihe im Schuljahr 2010/2011 können Lernmittel, also vor allem Schulbücher, gegen ein Entgelt ausgeliehen werden. Die ausgeliehenen Lernmittel sind am Ende des Schuljahres an den Schulträger zurückzugeben. Ist dies wegen Verlust oder Beschädigung nicht möglich, wird durch den Schulträger Schadens-

ersatz geltend gemacht, der an das Land abgeführt wird (§ 5 Abs. 4 LernMFrhAuslV).

Der Schulträger ist verpflichtet, dem Bildungsministerium bzw. der Aufsichts- und Dienstleistungsdirektion (ADD) als Schulaufsichtsbehörde über alle Angelegenheiten im Zusammenhang mit der Lernmittelfreiheit und der entgeltlichen Ausleihe Auskunft zu erteilen (§ 6 Abs. 5 LernMFrhAuslV).

Dabei kommen sog. Verwendungsnachweise zum Einsatz, in denen der Schulträger Differenzen zwischen Ist- und Soll-Beträgen zu erklären hat. Insbesondere ist über offene Leihentgeltforderungen und offene Schadensersatzforderungen Auskunft zu geben, damit die ADD anlassbezogen eine Einzelfallkontrolle vornehmen kann. Im Verwendungsnachweis 2012/13 wurde seitens des Bildungsministeriums insofern eine Änderung vorgenommen, als eine namentliche Liste mit den säumigen Zahlern von den Schulträgern erstellt und der ADD zur Prüfung übermittelt werden sollte.

Aus Sicht des Datenschutzes war zu klären, ob nicht eine anonymisierte oder pseudonyme Liste für die Prüfung durch die ADD ausreichend ist. Ansonsten würde bei der ADD eine landesweite Liste sämtlicher Schuldner entstehen, was datenschutzrechtlich eine Reihe von Fragen aufwerfen würde (z.B. Anmeldung zum Datenschutzregister, Benachrichtigung der Betroffenen, Hinweis auf Auskunfts- und Berichtigungsansprüche; Festlegung von Löschfristen).

Im Rahmen einer Besprechung mit Vertreterinnen und Vertretern des Bildungsministeriums wurde vereinbart, dass das vorgegebene Online-Formular – vorbehaltlich einer abschließenden Prüfung durch die ADD – geändert wird. Damit auch weiterhin eine Einzelfallprüfung durch die ADD im Bedarfsfall möglich ist, kann anhand des mitgeteilten Freischaltcodes eine Nachfrage beim Schulträger erfolgen. Soweit erforderlich, kann der ADD im Zusammenhang mit der Überprüfung dann auch der Namen der Schuldnerin bzw. des Schuldners mitgeteilt werden.

6.1.5 Handyfotos durch Lehrkräfte

Aufgrund mehrerer Eingaben zu Schuljahresbeginn wurde der LfDI davon in Kenntnis gesetzt, dass Lehrkräfte mit ihrem privaten Mobiltelefon Portraitfotos von Schülerinnen und Schülern ihrer neuen Klassen als Gedächtnisstütze oder zur Vervollständigung eines Sitzplans gefertigt hatten. In einem konkreten Fall drohte die Lehrkraft einem Schüler bei einer Weigerung sogar mit einem Klassenbucheintrag.

Die schulrechtlichen Bestimmungen sehen vor, dass die Erhebung personenbezogener Schülerdaten, wozu auch das Fertigen von Fotos gehört, für die Erfüllung schulbezogener Aufgaben erforderlich sein muss (§ 67 Abs. 1 SchulG). Dies bedeutet, dass eine schulische Aufgabe ohne die Datenerhebung nicht oder nur mit einem unverhältnismäßigen Aufwand erfüllt werden kann. Beim Anfertigen von Fotos zur Gedächtnisstütze oder zur Vervollständigung eines Sitzplans wird diese Voraussetzung nicht erfüllt. Von daher muss eine wirksame Einwilligungserklärung der Schülerinnen und Schüler bzw. deren Eltern vorliegen.

Gegenüber den Schulleitungen war darüber hinaus auf § 89 Abs. 4 Übergreifende Schulordnung hinzuweisen, wonach personenbezogene Daten auf privateigenen Datenverarbeitungsgeräten von Lehrkräften nur gespeichert werden dürfen, wenn die Schulleitung dies im Einzelfall genehmigt hat, das Einverständnis dafür vorliegt, dass das Gerät unter den gleichen Bedingungen wie dienstliche Geräte kontrolliert werden kann und den Belangen des Datenschutzes Rechnung getragen ist. Die letztgenannte Anforderung bedeutet konkret, dass die Verarbeitung personenbezogener Schülerdaten auf privaten Smartphones und Tablets der Lehrkräfte nur erfolgen darf, wenn eine Verschlüsselung der Daten sichergestellt ist.

Die Schulleitungen unterrichteten die Lehrkräfte über die Rechtslage; bereits gefertigte Fotos wurden gelöscht.

6.2 Wissenschaft

6.2.1 Datenschutzrechtliche Prüfung wissenschaftlicher Forschungsvorhaben

Die datenschutzrechtliche Bewertung wissenschaftlicher Forschungsvorhaben war schon immer ein Arbeitsschwerpunkt des LfDI, doch stieg die Zahl der der nach Maßgabe des § 67 Abs. 6 SchulG zur Prüfung eingereichten Vorhaben im Berichtszeitraum noch einmal deutlich an.

Wurden dem LfDI 2008/2009 gut 100 Vorhaben vorgelegt, waren es 2010/2011 bereits 125 und in den letzten beiden Jahren sogar fast 250. Die datenschutzrechtliche Prüfung dieser Vorhaben lässt sich mit den vorhandenen personellen Kapazitäten nicht mehr zeitnah bewältigen, zumal sie ohnehin bereits zu Einschnitten in anderen Aufgabenbereichen führt. Bedauerlicherweise konnte z.B. ein für das Jahr 2012 geplantes Treffen mit den behördlichen Datenschutzbeauftragten der Hochschulen wegen der überbordenden Zahl der zu prüfenden wissenschaftlichen Forschungsvorhaben nicht durchgeführt werden. Um für Entlastung zu sorgen, wurde bereits vor einiger Zeit gemeinsam mit der Aufsichts- und Dienstleistungsdirektion als Schulbehörde und dem Wissenschaftsministerium eine Verfahrensänderung bei der datenschutzrechtlichen Prüfung wissenschaftlicher Untersuchungen an Schulen abgestimmt.

Den rheinland-pfälzischen Hochschulen soll eine generelle Genehmigung für die Durchführung wissenschaftlicher Untersuchungen in Schulen erteilt werden. Anhand einer vom LfDI zu Verfügung gestellten „Checkliste“ sollen diese 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.

Bedauerlicherweise konnte diese Verfahrensänderung vom Wissenschaftsministerium noch nicht in die Praxis umgesetzt werden.

6.2.2 Forschungsdatenzugang im Bildungswesen

Auf die Einladung des Deutschen Instituts für Internationale Pädagogische Forschung (DIPF) hatte der LfDI im Rahmen eines wissenschaftlichen Kolloquiums zum Thema „Bedarfe und Desiderate des Forschungsdatenzugangs im Bildungswesen in Deutschland“ referiert (http://www.datenschutz.rlp.de/de/service/reden/20130304_lfdi_-_Rede_Frankfurt.pdf). Dabei stellte er u.a. fest, dass Defizite im Vollzug der datenschutzrechtlichen Forschungsklauseln von den Verantwortlichen der Forschungsprojekte gemeinsam mit den Vertretern der Datenschutzbeauftragten behoben werden sollten.

Daran anknüpfend haben die Leitungen verschiedener namhafter Forschungsinstitute einen Vorschlag für eine Verfahrensabrede zur datenschutzrechtlichen Prüfung bundeslandübergreifender Schulleistungsuntersuchungen entwickelt, mit dem eine Erleichterung und Entbürokratisierung von Abläufen sowohl in den Aufsichtsbehörden als auch in den Forschungsinstituten einhergehen soll.

Mit Schulleistungsuntersuchungen wie z.B. PISA werden Kenntnisse und Fertigkeiten von Schülerinnen und Schülern gemessen, um u.a. die Leistungen der Schulen zu evaluieren. Bei einer bundesweiten Untersuchung hat dies die Beteiligung aller Bundesdatenschutzbeauftragten zur Folge und führt mitunter zu unterschiedlichen Einwänden und Rückmeldungen aus den Behörden an die verantwortlichen Forschungsinstitute.

Der o.g. Vorschlag wird derzeit in einem Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beraten.

7. Kommunales, Meldewesen und Statistik

7.1 Kommunales

7.1.1 Solarkataster der Kommunen

Im Datenschutzbericht 2010/2011 (23. Tb., Tz. II-7.1.1) waren zum einen die rechtlichen Voraussetzungen für die Veröffentlichung von Orthofotos, Ort, Straße, Hausnummer und Geeignetheit einer Dachfläche für eine Photovoltaikanlage im Internet erläutert worden. Zum anderen hatte der LfDI darauf hingewiesen, dass er bei einer Kommune, die sich trotz intensiver Bemühungen und förmlicher Beanstandung nicht seiner Rechtsauffassung anschloss, deren Durchsetzung mit den Mitteln der Kommunalaufsicht einleiten werde.

In der Tat reagierte die Kommune erst auf eine kommunalaufsichtliche Anordnung der Aufsichts- und Dienstleistungsdirektion Trier. Der Internetauftritt wurde geändert. Es wurden nur noch die datenschutzrechtlich zulässigen Daten veröffentlicht, so dass der Beanstandung und der kommunalaufsichtlichen Anordnung entsprochen wurde.

Trotzdem haben in der Folgezeit verschiedene Kommunen in Kenntnis dieser Sachlage das von ihnen eingerichtete Solarkataster datenschutzwidrig gestaltet und online geschaltet. Jetzt genügte allerdings der Hinweis des LfDI, dass eine Beanstandung ausgesprochen werde, um die Verantwortlichen zu einem entsprechenden Tätigwerden zu bewegen.

7.1.2 Neues zur Videoüberwachung in Kommunen

Im Berichtszeitraum gingen mehrfach Anfragen zur beabsichtigten Installation von Überwachungsanlagen in kommunalen Schwimmbädern ein. Da es sich überwiegend um vergleichbare Sachverhalte – Vermeidung und/oder Aufklärung von Vandalismus, Einbrüchen, Diebstählen – handelte, hat der LfDI Leitlinien für die datenschutzrechtliche Bewertung ausgearbeitet.

Der Einsatz von Videoüberwachungstechnik in den als öffentlich-rechtliche Wettbewerbsunternehmen zu qualifizierenden kommunalen Schwimmbädern zur Wahrung des Hausrechts (§ 2 Abs. 3 LDSG i.V.m. § 6b BDSG) wird grundsätzlich nicht in Frage gestellt. Im Rahmen der Angemessenheitsprüfung einer entsprechenden Videoanlage geht es dann insbesondere um folgende Fragen:

- Kann die Überwachung (teilweise) als Monitoring organisiert werden?
- Kann die Betriebsdauer der Anlage eingeschränkt werden?
- Muss auf einzelne Kameras verzichtet werden oder sind andere Standorte zu wählen?
- Können Bildausschnitte bzw. Überwachungsbereiche anders definiert werden?

Dies gilt grundsätzlich auch für die Überwachung sog. gefährlicher Stellen wie der Einstieg in eine Wasserrutsche und deren Auffangbecken oder ein Sprungbecken.

Regelmäßig fordert der LfDI dabei, dass

- alle mit einer Überwachungsanlage zusammenhängenden Fragen in einer Dienstanweisung zu regeln sind; sofern es sich bei den überwachten Bereichen zugleich um Arbeitsplätze von Beschäftigten handelt, ist darauf zu achten, dass der Einsatz von Videoüberwachung so restriktiv wie möglich gestaltet wird. Dabei muss insbesondere verhindert werden, dass eine dauerhafte Mitarbeiterüberwachung erfolgt, welche Leistungs- bzw. Verhaltenskontrollen ermöglicht;
- Videoaufnahmen regelmäßig zwei Arbeitstage nach dem Beginn der Aufzeichnung zu löschen sind, es sei denn, durch Feiertage werden längere Speicherzeiten notwendig; eine an einen Schichtbetrieb angepasste Speicherdauer von z.B. sieben Tagen ist demnach zu lang.

Auch im Hinblick auf die **Sicherung von IT-Technikräumen** gab es verschiedentlich entsprechende Anfragen. Bei diesen Räumen handelt es sich um nicht-öffentliche Bereiche, d.h. sie sind nur einem bestimmten Personenkreis zugänglich, die Verwaltung als Inhaberin des Hausrechts kann die Nutzerinnen und Nutzer, z.B. IT-Beschäftigte

und Beschäftigte des Gebäudemanagements, generell konkret bestimmen.

Zweck der beabsichtigten Videoüberwachung ist es dann, in den IT-Technikräumen zweck- oder pflichtwidriges Verhalten zu verhindern bzw. wenigstens aufzuklären. Ein solches Verhalten könne nicht ausgeschlossen werden, wenn die Räume für sonstige Arbeiten (Brandschutz, Klimaanlagenwartung, Elektroinstallation, Reinigungsdienst) durch Beschäftigte des Gebäudemanagements oder durch Dritte betreten werden müssen.

Ein bloßes Monitoring während der üblichen Dienstzeiten könnte im Hinblick auf das Interesse der Verwaltung an einem störungsfreien IT-Betrieb der Behörde zulässig sein, da diese Form der Videoüberwachung weniger intensiv in die Rechte der Betroffenen eingreift als die Videoaufzeichnung. Bei dieser Konstellation stellt der Monitor sozusagen ein „verlängertes Auge“ der Betrachtenden dar.

Hinsichtlich der Aufzeichnung ist allerdings schon fraglich, ob die Überwachungsmaßnahme überhaupt dazu geeignet ist, den o.g. Zweck zu erreichen. Daran bestehen Zweifel, weil eine unbefugte Beeinträchtigung der zentralen IT-Komponenten nur durch unmittelbares Eingreifen gänzlich ausgeschlossen werden kann, so dass eine Videoaufzeichnung in diesem Zusammenhang regelmäßig unzulässig sein wird.

Außerdem ist zur Absicherung von Räumen mit zentralen IT-Komponenten auf die entsprechenden Kapitel der IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu verweisen.

In diesem Zusammenhang kann es also durchaus angemessen und auch die geeignetere Maßnahme sein, dass Beschäftigte der IT-Abteilung die Ausführung o.g. Arbeiten in den Technikräumen überwachen. Insofern sollte durch organisatorische Regelungen sichergestellt werden, dass Räume mit zentralen IT-Komponenten nur in Begleitung von IT-Personal betreten werden.

U.a. die Katastrophe in Duisburg 2010 hat dazu geführt, dass große Kommunen bei **Volks- und Straßenfesten** neuerdings Videoüberwachungstechnik einsetzen, um die Besucherströme mit Kameras zu überwachen. Wird das Besucheraufkommen an neuralgischen Stellen zu groß, sollen Sicherheitskräfte die Gäste umleiten, um eine Überfüllung von einzelnen Plätzen oder die Unzugänglichkeit von Rettungswegen zu vermeiden.

Als geeignetes Mittel kommt hier grundsätzlich nur die Videobeobachtung (Monitoring) in Frage, um das Verhalten der Festgäste einschätzen und ohne zeitliche Verzögerung z.B. Maßnahmen zur Lenkung von Besucherströmen ergreifen zu können. Die Bildübertragung erfolgt auf einen Monitor in der Einsatzleitstelle.

Zudem können die Kameras ggf. so installiert werden, dass verbunden mit der eingestellten Auflösung sogar gewährleistet wird, dass Einzelpersonen nicht erkennbar sind. Besucherinnen und Besucher, die die Kameras wahrnehmen, werden ihr Verhalten zwar möglicherweise an der vermeintlich personenscharfen Überwachung und Aufzeichnung ausrichten und anpassen. Diese Auswirkung ist aus datenschutzrechtlicher Sicht aber akzeptabel, da die Persönlichkeitsrechte der Festgäste nur gering beeinträchtigt werden. Aus der „Vogelperspektive“ der Kameras ist zudem besser zu erkennen, wie sich Besucherströme entwickeln, als durch Ordnungskräfte vor Ort.

Eine Bildaufzeichnung und spätere Einsichtnahme ist dagegen unzulässig. Als denkbarer Kompromiss käme allenfalls in Frage, im Rahmen des Monitorings im Falle einer sich ergebenden konkreten Gefahr eine kurzzeitige zusätzliche (Alarm-)Aufzeichnung vorzunehmen.

Nur am Rande sei bemerkt, dass der LfDI auch von Angeboten an Kommunen Kenntnis erhalten hat, mit **Drohnen** (unbemannte Luftfahrtsysteme, vgl. § 1 Abs. 2 S. 3 LuftVG) sog. Kugelbildpanoramas vom Gemeindegebiet zum Zwecke der Tourismus- oder Wirtschaftsförderung herzustellen. Von der Annahme solcher Angebote wurde aus Datenschutzgründen abgeraten.

7.2 Meldewesen

7.2.1 Kein reiner Grund zur Freude – Jubiläen nach dem Melderecht

Nach wie vor führen zahlreiche Bürgerinnen und Bürgern beim LfDI Beschwerde darüber, dass ihre Meldedaten ohne ihr Wissen anderen Personen oder Stellen übermittelt werden. Dies betrifft vor allem die Weitergabe von Meldedaten an politische Parteien und für Jubiläumszwecke. Hier steht den Betroffenen zwar ein Widerspruchsrecht zu; dieses Recht ist aber meistens nicht bekannt. Das neue Bundesmeldegesetz, das am 1. Mai 2015 in Kraft treten wird, wird hier leider keine Verbesserung bringen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in ihrer Entschließung „Melderecht datenschutzkonform gestalten!“ vom 22. August 2012 u.a. noch gefordert:

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

Die Frage, ob es unter demokratietheoretischen Gesichtspunkten nicht gerechtfertigt sein könnte, die Parteien in diesem Zusammenhang zu privilegieren, wofür aus der Sicht des LfDI einiges spricht, sei hier dahingestellt. Denn die Forderungen der Konferenz der Datenschutzbeauftragten wurden vom Gesetzgeber nicht aufgegriffen, obwohl es für viele Bürgerinnen und Bürger nicht einzusehen ist, dass sie selbst aktiv werden müssen, wenn sie die Weitergabe ihrer „zwangsweise“ erhobenen Meldedaten unterbinden möchten.

Hinzu kommt, dass einige Meldeämter bei der Weitergabe von Meldedaten für Jubiläumszwecke bisweilen über das Ziel hinausschießen: So veröffentlichen einige Kommunen Altersjubiläen im Amtsblatt unter Nennung der Anschrift, was vielen Jubilarinnen und Jubilaren schon aus einem gewissen Sicherheitsbedürfnis heraus nicht recht ist und daher auch aus Sicht des LfDI unterbleiben sollte. In einem anderen Fall teilte der Ortsbürgermeister im Amtsblatt unter der Rubrik „Sonstige amtliche Mitteilungen“ über einen Altbürgermeister u.a. mit, der Jubilar erfreue sich bester Gesundheit, verfolge das Ortsgeschehen unverändert mit großem Interesse und persönlichem Engagement und habe seinen Geburtstag im Kreise seiner Familie sowie mit Freunden und Bekannten gefeiert. Was sicherlich nett gemeint war, erfolgte jedoch ohne Rücksprache mit dem Betroffenen, der sich daher zu Recht beim LfDI über die Veröffentlichung beschwerte.

Teilweise wird den Bürgerinnen und Bürgern die Wahrnehmung ihres Widerspruchsrechts unnötig erschwert, indem etwa mitgeteilt wird, man trage nur Widersprüche ein, die sich auf ein unmittelbar bevorstehendes Jubiläum beziehen. Aus § 35 Abs. 3 MG folgt jedoch nur, dass Daten über Alters- und Ehejubiläen frühestens zwei Monate vor dem Jubiläum seitens der Meldeämter übermittelt werden dürfen, da Betroffene bis zu diesem Zeitpunkt der Weitergabe widersprechen können. Eine vorherige Eintragung des Widerspruchs ist damit nicht ausgeschlossen.

Einige Ortsbürgermeisterinnen und -bürgermeister möchten aus durchaus nachvollziehbaren Gründen nicht nur ab dem 70. Lebensjahr, sondern auch andere Geburtstage, wie z.B. die Volljährigkeit, zum Anlass nehmen, um Glückwünsche auszusprechen. Die Meldeämter sind aber aufgrund der einschlägigen Bestimmungen gehindert, diese Auskünfte zu erteilen: Der Gesetzgeber hat in § 35 Abs. 3 MG klargestellt, dass ein Altersjubiläum der 70. Geburtstag und jeder folgende Geburtstag ist. Im Übrigen macht § 31 Abs. 6 i.V.m. Abs. 1 MG die Zulässigkeit der Übermittlung von der Erforderlichkeit zur Aufgabenerfüllung abhängig. Eine solche Erforderlichkeit im Sinne einer zwingenden Notwendigkeit besteht jedoch nicht. Dies wird durch die Regelung in § 8 MeldDÜVO bestätigt, wonach nur die mit dem 70. Lebensjahr beginnenden Altersjubiläen als Übermittlungsanlass gesehen wird. Ansonsten erhält die Ortsgemeinde nur aus Anlass der Anmeldung bestimmt Daten. Andere Anlässe sind nicht genannt.

7.3 Statistik

Im Datenschutzbericht 2010/2011 (vgl. 23. Tb., Tz. II-7.3) wurde über die „heiße Phase“ der ersten Volkszählung für die Bundesrepublik Deutschland seit 1981 (Ostdeutschland) bzw. 1987 (Westdeutschland) berichtet und als Fazit festgehalten, dass Maßnahmen des Datenschutzes und der Datensicherheit von den beteiligten Stellen mit der nötigen Konsequenz getroffen wurden und der Zensus 2011 in Rheinland-Pfalz weitgehend reibungslos verlaufen ist.

Ein solches Fazit kann auch für die „Befragung zur Klärung von Unstimmigkeiten“ sowie die „Ersatzvornahmen zur Gebäude- und Wohnungszählung“ gezogen werden. Beides wurde im Laufe des Mai 2012 abgeschlossen und damit die Erhebungsphase des Zensus 2011 beendet, so dass die bei Kreis- und Stadtverwaltungen eingerichteten Erhebungsstellen wieder aufgelöst werden konnten. Auch diese Phase des Zensus 2011 wurde vom LfDI begleitet.

Mittlerweile wurden die amtlichen Einwohnerzahlen für alle Gemeinden als erste Ergebnisse des Zensus 2011 bekannt gegeben. Die Aufbereitung der Zensusdaten ist allerdings noch nicht abgeschlossen. Eine zweite Veröffentlichung von Ergebnissen ist für Anfang 2014 vorgesehen.

Nach den Vorgaben der Europäischen Union soll die nächste Volkszählung in Deutschland aber bereits im Jahr 2021 durchgeführt werden. Dies wurde vom BfDI zum Anlass genommen, mit „Eckpunkten für eine datenschutzgerechte Volkszählung“ frühzeitig auf wichtige datenschutzrechtliche Anliegen für den Zensus 2021 aufmerksam zu machen. Dazu gehört insbesondere, dass

- keine personenbezogene Erhebung an Anschriften mit sensiblen Sonderbereichen (z.B. Justizvollzugsanstalten) stattfindet,
- auf Datenerhebungen bei Dritten verzichtet wird,
- für die Löschung von Hilfsmerkmalen eine kürzere Frist geregelt wird.

Der LfDI teilt diese Auffassung und hat entsprechende Überlegungen auch in die 47. Tagung des Statistischen Landesausschusses Rheinland-Pfalz eingebracht. In dem Landesausschuss, der das Statistische Landesamt und die Landesregierung in Grundsatzfragen berät, sind u.a. die obersten Landesbehörden, die kommunalen Spitzenverbände, die Kammern und auch ein Vertreter der wirtschaftswissenschaftlichen Fakultäten der Universitäten Mitglied.

8. Justiz und Verbraucherschutz

8.1 Justiz

8.1.1 Übermittlung von Strafbefehlsanträgen und Anklageschriften an Ausländerbehörden

Aus Anlass einer Eingabe hat sich der LfDI mit der Frage befasst, unter welchen Voraussetzungen Strafbefehlsanträge und Anklageschriften an Ausländerbehörden übermittelt werden dürfen. In der Vergangenheit war es so, dass bei einer Anklageerhebung und einem Strafbefehlsantrag regelmäßig eine Mehrausfertigung des entsprechenden Schriftstücks an die zuständige Ausländerbehörde weitergeleitet wurde. Aus datenschutzrechtlicher Sicht war diese Praxis bedenklich. Bei der Übersendung der Mehranfertigungen handelt es sich um die Übermittlung personenbezogener Daten. Diese bedarf – soweit sie nicht mit der Zustimmung des Betroffenen erfolgt – einer gesetzlichen Grundlage.

Als bereichsspezifische Sonderregelungen enthalten die §§ 12 ff. EGGVG Rechtsvorschriften für die Übermittlung personenbezogener Daten durch Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften. Nach § 13 Abs. 1 Nr. 1 EGGVG ist eine Übermittlung nur zulässig, wenn eine Vorschrift die Übermittlung ausdrücklich vorsieht oder zwingend voraussetzt. Vorliegend ist § 87 Abs. 4 Satz 1 AufenthG maßgeblich. Danach haben die für die Einleitung und Durchführung von Straf- und Bußgeldvorschriften zuständigen Stellen die zuständige Ausländerbehörde unverzüglich über die Einleitung des Strafverfahrens sowie die Erledigung des Straf- oder Bußgeldverfahrens bei der Staatsanwaltschaft, bei Gericht oder bei der für die Ahndung der Ordnungswidrigkeit zuständigen Verwaltungsbehörde unter Angabe der gesetzlichen Vorschriften zu unterrichten.

Nach § 18 Abs. 2 EGGVG hat die übermittelnde Stelle die Form der Übermittlung nach pflichtgemäßem Ermessen zu bestimmen. Bei der Ausübung der Ermessensentscheidung ist das informationelle Selbstbestimmungsrecht des Betroffenen wesentlich zu berücksichtigen. Der LfDI hat – auch unter Berücksichtigung von Nr. 42 Abs. 1 Nr. 1, Abs. 3 MiStra – die Ansicht vertreten, dass auf dieser Grundlage die Übermittlung von Abschriften der getroffenen Entscheidungen in der Regel nicht erforderlich ist. Dabei ist auch zu beachten, dass die Dokumente zum Teil Daten Dritter (z.B. Opfer, Zeuginnen und Zeugen, Sachverständige) enthalten.

Mit dem Ministerium der Justiz und für Verbraucherschutz und den Generalstaatsanwaltschaften wurde Einvernehmen dahingehend erzielt, dass eine Übermittlung von Abschriften nicht mehr generell erfolgt. In der praktischen Anwendung durch die Staatsanwaltschaften wurde das Regel-Ausnahme-Verhältnis damit umgekehrt. Die Staatsanwaltschaften haben aber ausdrücklich darauf hingewiesen, dass eine Übermittlung von Abschriften im Einzelfall möglich sein muss, wenn Ausländerbehörden auf eine umfassende Tatsachenkenntnis angewiesen sind. Soweit im Einzelfall die engen Voraussetzungen für die Übermittlung von im Strafverfahren gespeicherten personenbezogenen Daten an die örtlich zuständigen Ausländerbehörden gegeben sind, kann auch nach Auffassung des LfDI eine Übermittlung von Amts wegen möglich sein. Allerdings werden die Betroffenen gemäß § 18 LDSG hiervon grundsätzlich zu unterrichten sein.

8.1.2 Novellierung der Grundbuchordnung – Auskunftsanspruch von Gründstückseigentümerinnen und -eigentümern

Am 1. Oktober 2013 hat der Deutsche Bundestag das Gesetz zur Einführung eines Datenbankgrundbuchs verabschiedet. Das Gesetz verfolgt den Zweck, das Grundbuchrecht zu modernisieren und an aktuelle Entwicklungen anzupassen. Mit der veränderten Datenstruktur werden neue Darstellungsformen des Grundbuchinhalts sowie neue Recherche- und Auskunftsmöglichkeiten zugelassen. Bereits im Gesetzgebungsverfahren wurden die Datenschutzbeauftragten des Bundes und der Länder beteiligt. Auch der LfDI hat im Verlauf des Gesetzgebungsverfahrens mehrere Stellungnahmen zu datenschutzrechtlich bedeutsamen Punkten abgegeben.

U.a. hat der LfDI darauf hingewiesen, dass klare Verantwortlichkeiten sichergestellt werden müssen und damit die Auftragsdatenverarbeitung von der

Funktionsübertragung abgegrenzt werden muss, wenn Grundbuchämtern die Möglichkeit eröffnet wird, Änderungen in Grundbüchern anderer Grundbuchämter vorzunehmen. Weiterhin hat sich der LfDI unter Hinweis auf das informationelle Selbstbestimmungsrecht der Betroffenen gegen grundbuchblattübergreifende Auswertungen gewendet bzw. die restriktive Handhabung solcher Auswertungsinstrumentarien angemahnt. Hinsichtlich der im Gesetz an mehreren Stellen vorgesehenen elektronischen Übermittlung von Daten erfolgte ferner der Hinweis darauf, dass der jeweilige Stand der Technik beachtet werden muss, um die notwendige Datensicherheit zu gewährleisten.

Den Vorschlägen ist der Bundesgesetzgeber nicht in allen Punkten gefolgt. So enthält das am 1. Oktober 2013 verabschiedete Gesetz nach wie vor eine Verordnungsermächtigung für die Landesregierungen grundbuchblattübergreifende Auswertungen zu ermöglichen. Auch ein Hinweis auf ggf. entgegenstehende berechtigte Interessen des Betroffenen wurde in der Gesetzesformulierung nicht aufgegriffen. Nichtsdestotrotz lässt sich insgesamt festhalten, dass aus Sicht des Datenschutzes begrüßenswerte Änderungen des ursprünglichen Gesetzentwurfs vorgenommen wurden.

Von besonderer Bedeutung ist aus rheinland-pfälzischer Sicht die ab Oktober 2014 wirksam werdende Einfügung eines Abs. 4 in § 12 GBO. Nach dieser Norm sollen Einsichten in die Grundbücher und Grundakten sowie die Erteilung von Abschriften hieraus protokolliert werden. Den Eigentümerinnen und Eigentümern eines Grundstücks oder eines grundstücksgleichen Rechts ist auf Verlangen Einsicht in die Protokollierung zu geben. Diese Neuregelung greift eine Problematik auf, die Gegenstand einer Eingabe beim LfDI war. Ein Petent hatte sich darüber beschwert, dass ihm seitens des Grundbuchamts – mangels Protokollierung – keine Auskünfte darüber gegeben werden konnten, ob und durch wen eine Einsichtnahme des Grundbuchs in Bezug auf sein Grundstück erfolgt war.

Der LfDI hat zu dieser Frage den Standpunkt vertreten, dass ein Auskunftsanspruch der Eigentümerinnen und Eigentümer zwar nicht nach der Grundbuchordnung oder der Grundbuchverfügung bestehe, dass ein solcher aber aus § 18 Abs. 3 Nr. 2 LDSG folge. Zweck dieser Norm sei es, Betroffene in die Lage zu versetzen, den Verlauf ihrer Daten und den Umgang mit diesen zu kontrollieren. Eine solche Kontrolle sei auch für Grundbuchdaten notwendig. Gründe, die dem Anspruch entgegenstünden, seien nicht ersichtlich. Demgegenüber wurde zum Teil vertreten, dass die Regelungen des Grundbuchrechts abschließend seien und daher ein Auskunftsanspruch nicht bestehe. Mit der Schaffung von § 12 Abs. 4 GBO werden diese Unsicherheiten überwunden. Die Norm stellt eine bereichsspezifische und damit vorrangige Regelung dar, die den aus datenschutzrechtlicher Sicht zu begrüßenden Auskunftsanspruch sicherstellt. Damit wird ferner ein Gleichlauf zwischen dem elektronischen Abrufverfahren (§ 133 GBO) erzielt, bei dem ein solcher Auskunftsanspruch bereits existierte. Im Übrigen stellt der Auskunftsanspruch eine Kompensation dafür dar, dass die Eigentümerinnen und Eigentümer nach der Rechtsprechung bei Grundbuchabfragen Dritter im Vorfeld nicht zu beteiligen sind.

8.2 Verbraucherschutz

8.2.1 Verbraucherdialog „Mobile Payment“

Vom Mobile Payment, also dem mobilen Bezahlen, wird allgemein gesprochen, wenn Nutzerinnen und Nutzer sich eines mobilen Endgeräts bedienen, um einen Zahlungsvorgang durchzuführen. Anders als bei der eher erfolglosen Geldkarte wird die Zukunft des Mobile Payment vor allem im Einsatz des Smartphones als mobile Geldbörse (mobile wallet) gesehen. Während eine Applikation auf dem Smartphone oder an der Bezahlstelle (POS – Point Of Sale) das Bezahlen ermöglicht, werden die dazu notwendigen Daten mittels drahtloser Übertragungstechnologie, z.B. per NFC übertragen. Aber auch der QR-Code wird teilweise für Bezahlvorgänge benutzt. Bargeld, Kreditkarten, Rabattkarten, Gutscheine oder Tickets – alle könnten beim Mobile Payment durch ein Gerät ersetzt werden, um Produkte und Dienstleistungen aller Art zu bezahlen.

Auch wenn Mobile Payment noch am Anfang der Entwicklung steht, muss rechtzeitig sichergestellt werden, dass beim Erschließen neuer Geschäftsfelder die Suche nach datenschutzgerechten

Lösungen nicht aus dem Blick gerät. Daher hat der LfDI zusammen mit dem Ministerium für Justiz und Verbraucherschutz und der rheinland-pfälzischen Verbraucherzentrale im Jahr 2013 den 3. Verbraucherdialog zum Thema „Mobile Payment“ durchgeführt. Im Dialog mit Anbietern mobiler Bezahlsysteme, Wissenschaft und Datenschützern wurden sowohl unter dem Gesichtspunkt der Zahlungssicherheit als auch des Datenschutzes Empfehlungen erarbeitet, bei deren Einhaltung ein verbraucherfreundlicher Einsatz von mobilen Bezahlverfahren gewährleistet sein soll. Für den Bereich Datenschutz hat sich dabei gezeigt, dass derzeit die bestehenden datenschutzrechtlichen Regelungen ausreichen, um entsprechende Anforderungen an mobile Bezahlverfahren zu formulieren.

Schwerpunkt der datenschutzrechtlichen Empfehlungen war die Transparenz für Verbraucherinnen und Verbraucher. Dazu gehört in erster Linie, in verständlicher Form über die Datenverarbeitungsvorgänge aufzuklären, so dass sich Nutzerinnen und Nutzer von mobilen Zahlverfahren gut informiert und frei für eine Bezahlmethode entscheiden können. Dies und eine angemessenen Absicherung der Datenverarbeitung sollen die ausgearbeiteten Empfehlungen gewährleisten (http://www.datenschutz.rlp.de/de/service.php?submenu=mat#mobile_payment).

Die Datenschutzaufsichtsbehörden befassen sich derzeit intensiv mit den technisch-organisatorischen Anforderungen an Girogo, eine Form des Mobile Payment (vgl. Tz. III-8.2.2).

8.2.2 Kontaktlose Bezahlverfahren

Kontaktlose Bezahlverfahren erlangen deutschlandweit zunehmende Bedeutung. Aus diesem Grund haben der LfDI, das Ministerium der Justiz und für Verbraucherschutz und die Verbraucherzentrale Rheinland-Pfalz den 3. Verbraucherdialogs dem Thema „Mobile Payment“ gewidmet (vgl. Tz. III-8.2.1). Auch die zuständigen Gremien der Datenschutzaufsichtsbehörden haben sich intensiv mit den datenschutzrechtlich relevanten Problemkreisen kontaktloser Bezahlvorgänge auseinandergesetzt.

Bereits mit einem Beschluss vom 19. September 2012 hat der Düsseldorfer Kreis auf spezifische Gefahren des „Mobile Payments“ hingewiesen (Beschluss des Düsseldorfer Kreises „Near Field Communication (NFC) bei Geldkarten“ vom 18./19. September 2012. Weiterhin haben die Datenschutzaufsichtsbehörden von den Anbietern kontaktloser Bezahlverfahren Datenschutzfolgeabschätzungen, auch Privacy Impact Assessments (PIA) genannt, eingefordert.

Bei einem PIA handelt es sich um die systematische Analyse eines Verfahrens oder einer Anwendung unter Gesichtspunkten der Privatsphäreneinstellung und des Datenschutzes. Durch sie werden Defizite aufgezeigt und der Anbieter in die Lage versetzt, Anpassungen der Prozesse vorzunehmen. Ziel ist es, das Datenschutzniveau im Sinne eines „privacy by design“ zu erhöhen. Die in der Zwischenzeit vorliegenden Ergebnisse der Datenschutzfolgeabschätzungen werden nunmehr durch die Datenschutzaufsichtsbehörden ausgewertet. Im Vordergrund stehen dabei Fragen der Transparenz sowie Maßnahmen des technisch-organisatorischen Datenschutzes.

8.2.3 Smartphones und Apps

Smartphones gehören mittlerweile zur täglichen Lebenswirklichkeit vieler Menschen. Ihnen wächst nach und nach der Status eines persönlichen Begleitgegenstandes wie Geldbörsen, Brillen oder Armbanduhren zu. So wie diese begleiten die Geräte ihre Besitzerinnen und Besitzer auf Schritt und Tritt. Bereits 2012 verfügte jede bzw. jeder dritte Deutsche über ein Smartphone. Bei den unter 30-Jährigen war es sogar jede bzw. jeder zweite. Smartphones fungieren dabei nicht nur als Mobiltelefon, sondern verfügen wie kleine Computer über verschiedene Datenschnittstellen, GPS-Ortung, mobilen Internetzugang und eigene Betriebssysteme.

Das erlaubt den Nutzerinnen und Nutzern, Anwendungssoftware, sog. Apps, herunterzuladen, mit denen sie die Funktionen ihrer Mobiltelefone beliebig erweitern können. Die Anwendungsgebiete für Apps scheinen unbegrenzt. Sie reichen von Spielen, über Text- und Bildbearbeitungsprogramme, bis hin zu Anwendungen, die Kommunikation mit Freunden oder Banküberweisungen ermöglichen. Fast eine Milliarde Apps wurden in Deutschland im Jahr 2011 auf mobile Systeme

geladen. Mit Hilfe dieser Apps, die ein Smartphone erst smart werden lassen, verfügen die digitalen Alleskönner über ein umfangreiches Wissen über ihre Besitzerinnen und Besitzer und deren soziales Umfeld: Kontaktdaten, Termine, Kommunikations- und Nutzungsverhalten, Aufenthaltsorte, Konsumgewohnheiten, Interessen und Vorlieben.

Smartphonenutzerinnen und -nutzer machen sich dabei selten klar, dass über die Verbindung zum Internet oder über Datenschnittstellen wie z.B. Bluetooth ein Zugriff auf diese Daten für Dritte möglich wird. Verschiedene Vorkommnisse in der Vergangenheit haben gezeigt, dass durch Apps Daten über Nutzerinnen und Nutzer eines Smartphones erhoben und ohne deren Wissen an Dritte übermittelt wurden. Gerade bei der Nutzung von kostenlosen Apps, die häufig durch Werbung finanziert werden, besteht die Gefahr, dass Nutzerprofile erstellt werden, die dann gezielt zu Werbezwecken eingesetzt werden. Untersuchungen zeigen, dass eine Reihe von Apps in einer Weise auf Daten des Smartphones zugreifen, die die Nutzerinnen und Nutzer so nicht erwarten. Etwa, wenn eine Anwendung, die eine bloße Taschenlampenfunktion bietet auf das Adressbuch, die Telefonliste, den Nutzerstandort oder die besuchten Webseites zugreift – ohne die Nutzerinnen und Nutzer darüber zu informieren oder um Erlaubnis zu fragen. Daneben kann nicht ausgeschlossen werden, dass unseriöse Anbieter über eine App Schadsoftware auf einem Smartphone installieren, die Daten heimlich sammeln und weitergeben. Es ist für Dritte dabei auch möglich, die vollständige Kontrolle über ein Smartphone zu übernehmen.

Man sollte also darauf achten, welche Daten eine App verwenden will. Für Smartphones mit dem weit verbreiteten Betriebssystem „Android“ lässt sich dies vor dem Download oder spätestens bei der Installation klären, da hier entsprechende Informationsmöglichkeiten bestehen bzw. die Nutzerinnen und Nutzer darum gebeten werden, den Datenzugriffen zuzustimmen. Bei Geräten mit dem Betriebssystem iOS (iPhone/iPad) erfolgt jeweils eine Nachfrage, wenn auf das Adressbuch oder den Standort zugegriffen werden soll; darüber hinaus kann festgelegt werden, welche Apps überhaupt auf Standortdaten zugreifen können sollen. Steuern kann man auch grundsätzlich, ob, wann und wer erfährt, wo man sich gerade befindet. Schließlich muss die GPS- oder WLAN-Funktion des Smartphones ja nicht dauerhaft aktiv sein, und wenn sie abgeschaltet sind, kann auch keine Applikation ungefragt auf Standortdaten zugreifen.

Zusammen mit dem Ministerium der Justiz und für Verbraucherschutz und der Verbraucherzentrale Rheinland-Pfalz hat sich der LfDI das Ziel gesetzt, die Nutzerinnen und Nutzer von Smartphones über diese Gefahren aufzuklären und ihnen Möglichkeiten für einen wirksamen Selbstdatenschutz aufzuzeigen. An einem Informationsstand und bei einer Diskussionsrunde, an der der Minister der Justiz und für Verbraucherschutz, Jochen Hartloff, der Vorstand der Verbraucherzentrale, Ulrike von der Lühe, und der LfDI, Edgar Wagner, teilnahmen, konnten sich Interessierte am 31. August 2012 in der Mainzer Innenstadt über die Thematik informieren. Außerdem wurde eine Informationsbroschüre mit dem Titel „Smartphones und Apps – Spione in der Hosentasche“ aufgelegt. Umfangreichere Informationen finden sich auf dem gemeinsamen Internetportal. Ziel ist es dabei, dass Nutzerinnen und Nutzer von Smartphones in die Lage versetzt werden, selbstbestimmt über ihre Daten zu entscheiden.

Weitere Informationen zum Thema:

- http://www.datenschutz.rlp.de/de/selbstds.php?submenu=mobile
- http://www.mjv.rlp.de/smartphones

9. Finanzen

9.1 Die „Bettensteuer“

Die sog. Bettensteuer oder auch Kultur- und Tourismusförderabgabe wird von Kommunen pro Übernachtung erhoben. In der Regel schulden die Beherbergungsbetriebe die Steuer. Grundlage ist eine entsprechende kommunale Abgabensatzung. Da bei der Erhebung einer sog. Bettensteuer nach einem Urteil des Bundesverfassungsgerichts vom Juli 2012 zwischen privat und beruflich veranlassten Übernachtungen zu unterscheiden ist, stellte sich die Frage, wie der Nachweis des Übernachtungszwecks bei Hotelgästen datenschutzgerecht gestaltet werden kann.

Da auch eine rheinland-pfälzische Kommune auf Einnahmen aus der sog. Bettensteuer baute, wurde die entsprechende Satzung in datenschutzrechtlicher Hinsicht überprüft. Nach dieser Satzung sollte zwar auch nur für Gäste, die aus privaten Anlässen übernachten, pro Nacht ein Euro, beschränkt auf maximal vier Nächte, erhoben werden, es blieb aber völlig unklar, in welcher Form und von wem entsprechende Nachweise über den Übernachtungszweck zu führen sind.

Da die Beherbergungsbetriebe steuerpflichtig sind, müssten sie gegenüber der Kommune den Übernachtungszweck nachweisen können. Diesen Zweck können sie aber nur von den Übernachtungsgästen erfahren. Diese wiederum sind nicht verpflichtet, solche Angaben zu machen. Dies kann allenfalls auf freiwilliger Basis erfolgen und würde dann aber einer einheitlichen Besteuerung zuwiderlaufen. Fraglich ist auch, ob der Erhebungsaufwand und der damit verbundene Eingriff in das Recht auf informationelle Selbstbestimmung gerechtfertigt ist, wenn pro Gast lediglich maximal vier Euro Steuern anfallen.

Die Rechtsprechung ist – auch über die Grenzen von Rheinland-Pfalz hinaus – vielfältig und bietet den einzelnen Kommunen keine Rechtsklarheit, um eine rechtskonforme Satzung durchzusetzen. Daher wird nach derzeitigem Kenntnisstand auch die vom LfDI überprüfte Satzung nicht angewendet, so dass der LfDI trotz datenschutzrechtlicher Bedenken derzeit keinen Handlungsbedarf sieht.

9.2 Kontenabrufe durch die Finanzämter

Seit Einführung des sog. Kontenabrufverfahrens im April 2005 sind die Zahlen dieser Abrufe kontinuierlich gestiegen und dies, obwohl seit Einführung der Abgeltungssteuer 2009 die Konten durch die Finanzverwaltung fast ausschließlich im Bereich der Vollstreckung und nicht mehr im Bereich der Veranlagung überprüft werden. Diese Entwicklung hat der LfDI zum Anlass genommen, die in Rheinland-Pfalz seitens der Finanzämter durchgeführten Kontenabrufe stichprobenhaft auf die Einhaltung der datenschutzrechtlichen Vorgaben zu überprüfen.

Dabei ist vor allem aufgefallen, dass die Betroffenen in rund drei viertel der Fälle gar nicht bzw. nicht zeitnah über den Kontenabruf benachrichtigt wurden, so wie es § 93 Abs. 9 Satz 2 AO fordert.

In der Regel erfolgte nach dem Eingang des Ergebnisses des Abrufs sofort eine Kontenpfändung, wenn unbekannte Konten aufgedeckt wurden. Schuldnerinnen und Schuldner werden über diese Kontenpfändung unterrichtet. In dieser Unterrichtung wurde systemseitig eine Information über den Kontenabruf angeboten, die die Sachbearbeiterinnen und Sachbearbeiter nur „aktivieren“ mussten. Dennoch erfolgte diese Information in den wenigsten Fällen. Wenn es nicht zu einer Kontenpfändung gekommen war, wurde regelmäßig nicht benachrichtigt.

Gerade die Information der Betroffenen ist aber eine nachdrückliche Forderung der Datenschutzbeauftragten. Wenn schon Daten bei Dritten erhoben werden, soll dies wenigstens transparent geschehen, damit die Betroffenen die Möglichkeit haben, die Rechtmäßigkeit zu überprüfen. Nur ganz ausnahmsweise darf von einer Information der Betroffenen abgesehen werden: nämlich dann, wenn die Aufgabenerfüllung oder die öffentliche Sicherheit und Ordnung gefährdet wäre oder der Kontenabruf zum Schutze Dritter geheim gehalten werden muss. Die Information vor dem Abruf im Vollstreckungsbereich würde die Vollstreckung gefährden, denn dann würden die Schuldnerinnen und Schuldner voraussichtlich ihre Konten leer räumen. Dass vorab auf eine solche Information verzichtet wird, ist vom Gesetz gedeckt. Allerdings

treffen diese Voraussetzungen für den Verzicht auf eine nachträgliche Benachrichtigung nicht zu.

Weiterhin wurde festgestellt, dass sich die interne Kontrolle darauf beschränkte, dass die Anträge zum Kontenabruf mitgezeichnet wurden, also ein Vier-Augen-Prinzip eingehalten wurde. In keinem Fall kam es vor, dass irgendwelche Bedenken oder Rückfragen dokumentiert wurden, auch dann nicht, wenn z.B. nur wegen geringer Summen ein Verfahren eingeleitet wurde.

Auch erfolgte keine Erfolgskontrolle, obwohl dies so im Verfahren vorgesehen war. Das ist jedoch wichtig, um zu überprüfen, in welchen Fällen ein Kontenabruf vielleicht zukünftig gar nicht mehr erforderlich ist.

Auch die behördlichen Datenschutzbeauftragten sind in das Verfahren nicht eingebunden gewesen. Eine Stichprobenkontrolle würde sicherlich dazu beitragen, nicht nur die vollstreckungsrechtliche Seite, sondern auch die datenschutzrechtlichen Aspekte des Abrufs besser zu berücksichtigen.

Das Finanzministerium hat die datenschutzrechtliche Kritik anerkannt und mittlerweile entsprechende Empfehlungen in einer Handlungsanleitung für die Mitarbeiterinnen und Mitarbeiter der Finanzämter zusammengefasst.

9.3 Überprüfung der Zugriffe von Beschäftigten der Finanzverwaltung auf Steuerdaten

Im April 2013 hatte die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg in einer Pressemitteilung auf die Praxis des dortigen Finanzministeriums hingewiesen, die Zugriffe der Finanzbeamtinnen und -beamten auf Steuerdaten auf ihre Berechtigung hin zu überprüfen, und zwar anlasslos und unbegrenzt.

Eine solche Überprüfung ist zwar im Sinne der Steuerpflichtigen, denn die Einhaltung des Steuergeheimnisses durch die Finanzamtsmitarbeiterinnen und -mitarbeiter kann auf diese Weise lückenlos überprüft werden. Zum Schutz der Steuerpflichtigen sind auch durch die Steuerdatenabrufverordnung entsprechende Stichprobenkontrollen vorgesehen. So ist gemäß § 7 StDAV zeitnah und in angemessenem Umfang zu prüfen, ob Abrufe von Steuerdaten berechtigt waren. Ansonsten können Abrufe nur anlassbezogen geprüft werden. Eine anlasslose und unbegrenzte Überprüfung hat der Verordnungsgeber hingegen ausdrücklich nicht vorgesehen.

Auch in Rheinland-Pfalz wurden Beschäftigte der Finanzverwaltung überprüft, datenschutzrechtlich war dies aber nicht zu beanstanden. Die Überprüfung der Zugriffe war auf eine geringe Zahl von Mitarbeiterinnen und Mitarbeitern beschränkt. Außerdem gab es für ihre Überprüfung einen konkreten Anlass. Dies entspricht der Steuerdatenabrufverordnung (§ 7 Satz 2 StDAV), wonach Abrufe neben den Stichprobenkontrollen auch anlassbezogen überprüft werden dürfen. Daher unterschied sich das Vorgehen der rheinland-pfälzischen Finanzverwaltung grundlegend von dem in Brandenburg, wo eine generelle Überprüfung aller Beschäftigten angeordnet worden war, ohne dass es konkrete Hinweise auf ein Fehlverhalten gegeben hätte.

9.4 Post der Oberfinanzdirektion auf Abwegen

Die Oberfinanzdirektion hat ein ganz erhebliches Briefaufkommen. Sendungen der Finanzämter und der Zentralen Besoldungs- und Versorgungsstelle müssen täglich zur Post und auch zu den im Lande verteilten Dienststellen der Landesverwaltung transportiert werden. Diese Aufgabe übernehmen seit Jahren Dienstleister im Auftrag der Oberfinanzdirektion.

Zum Ende des Berichtszeitraums kam es zu einigen Vorfällen, in denen Sendungen nicht ihre Adressaten erreichten. So wurden einmal Kartons mit Gehaltsabrechnungen in verschlossenen Briefumschlägen auf einer Mülltonne gefunden, ein anderes Mal waren es kistenweise Finanzamtsbriefe, die vor der Rhein-Zeitung in Koblenz abgestellt worden waren. Die polizeilichen Ermittlungen ergaben, dass die Sendungen den Transportdienstleistern gestohlen wurden, ein Täter konnte jedoch nicht ermittelt werden.

Der LfDI hat diese Vorfälle zum Anlass genommen, die Vertragsgestaltung zwischen der Oberfinanzdirektion und den Transportdienstleistern zu überprüfen. Denn grundsätzlich ist es zulässig, Dritte mit solchen Aufgaben zu betrauen, wenn die Voraussetzungen für eine Datenverarbeitung im Auftrag gemäß § 4 LDSG eingehalten werden. Im Ergebnis konnte festgestellt werden, dass die Auftragsvergabe entsprechend den gesetzlichen Vorgaben erfolgte. Die beauftragten Unternehmen waren nach dem Postgesetz lizenziert und waren als zuverlässig bekannt, die mit dem Transport betrauten Mitarbeiterinnen und Mitarbeiter wurden nach dem Verpflichtungsgesetz verpflichtet, und die Rahmenvorgaben für den Transport waren hinreichend klar im Sinne des Datenschutzes festgeschrieben.

Eine Überprüfung der beteiligten Transportdienstleister war dem LfDI nicht möglich, da diese als nach dem Postgesetz lizenzierte Unternehmen insoweit der Kontrolle des BfDI unterliegen. Dieser wurde entsprechend informiert und wird in eigener Zuständigkeit die beteiligten Unternehmen überprüfen.

IV. Anhang

A.1 Geschichte, Regelung und Modernisierung des Datenschutzes

Im 40. Jahr seit Inkrafttreten des Landesdatenschutzgesetzes macht es Sinn, die Geschichte des modernen Datenschutzes in den letzten vier Jahrzehnten in der geboten Kürze zusammenzufassen. Danach lassen sich vier verschiedene Phasen unterscheiden:

Erste Phase

1. Die Entstehung und Entwicklung des Datenschutzes ist eng verknüpft mit der technologischen Umstellung von der manuellen zur automatisierten Datenverarbeitung. Ausgangspunkt waren die USA, wo die Computertechnik entwickelt, aber auch früh – nämlich nach dem 2. Weltkrieg – vor den Gefahren der neuen Informationstechnik gewarnt wurde. Diese Warnungen verhallten zunächst, weil die Datenverarbeitungstechnologie zwar rasch weiterentwickelt wurde, aber mangels breitenwirksamer Anwendung in der Gesellschaft allenfalls als Gegenstand von Science-Fiction-Storys wahrgenommen wurde.

Ihre Bedeutung rückte wohl zum ersten Mal ins öffentliche Bewusstsein, als die demokratische Partei ihrer Wahlstrategie eine computerbasierte Auswertung des langjährigen Wählerverhaltens zugrunde legte und u.a. damit den Wahlsieg John F. Kennedys sicherstellte. Das schärfte den Blick für die mit der elektronischen Datenverarbeitung einhergehenden neuartigen Möglichkeiten.

Wenig später kam es in den USA zu einer intensiven Diskussion in den USA um Datensammlungen über Vietnam-Kriegsgegner und die Absicht der Administration, ein Nationales Datenzentrum in Washington einzurichten, in dem alle vorhandenen Datenbestände zusammengeführt werden sollten. Zugleich wurde bekannt, dass es zu diesem Zeitpunkt bereits zahlreiche Dossiers mit Informationen über politische und private Verhaltensweisen von Bürgern im staatlichen wie im wirtschaftlichen Bereich gab, was die amerikanische Öffentlichkeit befürchten ließ, dass Computer mit Hilfe von Telefonüberwachungen und Kameras die persönlichen Lebensbereiche ausforschen würden. Mitte der 60iger Jahre wurde daraufhin dieses Vorhaben zunächst gestoppt.

2. In der Bundesrepublik Deutschland hatte die Entwicklung der EDV auch mit der Verankerung des Sozialstaatsprinzips in Art. 20 des Grundgesetzes zu tun. Arbeitslosenversicherung, Rentensystem und dergleichen mussten neu organisiert und durchgeführt werden. Dafür waren viele Informationen erforderlich, z.B. Daten der Leistungsempfänger, um über Anspruch und Höhe der Leistungen entscheiden zu können. So entstanden umfangreiche Karteisysteme und Berechnungsverfahren, die jeweils per Hand auf Rechenmaschinen durchgeführt wurden. Um die vielfältigen neuen Aufgaben erledigen zu können, ohne dabei eine übermäßige Personalvermehrung herbeizuführen, musste rationalisiert und wirtschaftlich gearbeitet werden. Dazu gehörte auch eine Verbesserung der Kooperation zwischen den verschiedenen Verwaltungseinrichtungen. In diesem Kontext hat die elektronische Datenverarbeitung in der Bundesrepublik ihre Wurzeln. Dies kommt auch in den Statistiken zum Ausdruck. 1957 gab es in der Bundesrepublik 21 EDV-Anlagen, 1958 allein in der öffentlichen Verwaltung bereits 139 Anlagen. 1968 schließlich zählte man in der gesamten Republik bereits 3.863 Anlagen. Zugleich waren 1.607 neue Bestellungen in Auftrag gegeben worden. 1970 gab es in der Bundesrepublik dann bereits 7.250 Anlagen, ein Jahr später 7.500 Anlagen. Damit befand sich das Land hinter den USA (70.000 Anlagen) und Japan (7.900) weltweit an dritter Stelle, vor England (6.000 Anlagen) und der damaligen UdSSR (5.000 Anlagen). Die Deutsche Bundespost (36 Anlagen) und die Deutsche Bundesbahn (30 Anlagen) zählten zu den größten kommerziellen Anwendern Europas.

3. Die zentrale Datenverarbeitung hatte in dieser Zeit einen Namen: IBM System/360 bzw. System/370. Ein Großteil der EDV-Anlagen z.B. im Auswärtigen Amt, im Bundesministerium des Innern, im Bundesministerium der Finanzen und im Bundesministerium der Verteidigung sowie im Bundesverkehrsministerium bestand aus diesen Modellen, die noch auf der Basis von Lochkarten arbeiteten. Auch auf Landesebene wurde die „360er-Architektur“ zum Standard. Mit Hilfe dieser Großrechner wurden Ende der 1960er, Anfang der 1970er Jahre in den Bun-

desländern auch sog. Rechenzentren eingerichtet. In Hessen geschah dies bereits im Dezember 1969, in Rheinland-Pfalz im Mai 1971.

Die Großrechner in Staat und Wirtschaft verfügten damals über Hauptspeicher von maximal vier Megabyte. Heute hat jeder leistungsfähige Laptop das 250-Fache davon. Jedes dieser vier Megabyte bestand damals aus einem großen Schrank, daneben stand in der Regel ein fünfter Schrank, der für die Wasserkühlung sorgte. Aber das war noch nicht alles. Weitere „Schränke“ kamen hinzu: Einer war die zentrale Recheneinheit, ein weiterer diente dazu, die Magnetbänder abzuspielen und ein dritter war dazu da, die Lochkartenstapel zu verarbeiten. Es gab keine Bildschirme und keine sonstigen externen Geräte, natürlich auch keine Computernetze. Es gab nur große Stapel von Lochkarten und Festplatten, die in 30er-Stapeln in Geräte eingesteckt wurden, die aussahen wie Waschmaschinen.

4. Eine öffentliche Diskussion über die Vorteile und Risiken solcher Anlagen hat es lange Zeit nicht gegeben. Sie wurde allenfalls unter Verwaltungsfachleuten und Juristen geführt. In den Medien waren die EDV-Anlagen kein Thema. Eine Wendung nahm das Geschehen als im Herbst 1968 Pläne der damaligen Bundesregierung publik wurden, ein Verbundsystem von vier zentralen Datenbanken für alle staatlich gesammelten Anlagen einzuführen. Alle Bürger sollten dazu ein sog. Personenkennzeichen erhalten, mit dem alle gespeicherten Daten dann zum jeweiligen Bürger zuordenbar und zentral abrufbar werden sollten. Grundidee war, die bisher in getrennten Systemen gespeicherten Daten zentral zusammenzuführen, so dass „die Daten laufen, nicht die Bürger“. Bezeichnend war, dass die Pläne der Bundesregierung weder mit dem Bundestag noch mit dem Bundesrat abgestimmt waren. Es war offenbar auch nicht daran gedacht worden, den Bundestag an den Vorteilen eines solchen Systems teilhaben zu lassen. Nutzer dieses „Bundesdatenbanknetzes“ sollte die Exekutive sein. Erst 1968/1969 wurde der Einsatz der EDV in der öffentlichen Verwaltung in aller Öffentlichkeit und dann auch heftig diskutiert. Dies führte letztlich dazu, dass die entsprechenden Pläne von der Bundesregierung ad acta gelegt wurden.

So blieb es zunächst dabei, dass die EDV-Anlagen dezentral als Rechner genutzt wurden, um zunächst bestimmte Rechenoperationen durchzuführen. In den 60er Jahren wurden sie auch für Abrechnungs-, Buchungs- und Kontrollvorgänge eingesetzt. Neben der Bearbeitung solcher Massenvorgänge wurde die EDV mit Beginn der 70er Jahre aber auch zur Bewältigung von sonstigen Verwaltungsaufgaben herangezogen. Im ersten Bericht der Bundesregierung über die Anwendung der elektronischen Datenverarbeitung in der Bundesverwaltung vom 7. Oktober 1968 heißt es: „Die EDV ist das zurzeit und wohl auf lange Sicht geeignetste Mittel, die immer schneller anwachsenden Bestände menschlichen Wissens besser zu ordnen und zu einem rascheren Zugriff zu erschließen. Moderne Dokumentation ist ohne die EDV nicht mehr denkbar. Damit ist die EDV auch eine ausgezeichnete Hilfe zur Optimierung der Regierungstätigkeit und zur Verbesserung der Informationsmöglichkeit.“

5. Erst Ende der 1960iger Jahre begann in der Bundesrepublik Deutschland im Zusammenhang mit den neuen Formen der Datenverarbeitung die Diskussion um den **Schutz der Privatsphäre**. Besonders mit den großen Datenbanken sah man die Gefahr heraufziehen, dass deren Betreiber eine umfassende „Informationsmacht“ gegenüber dem Bürger würden erlangen können. Die neuen Anlagen wurden zunehmend auch als Instrument staatlicher Machtausübung mit allen damit verbundenen Missbrauchsmöglichkeiten gesehen. Dabei sah man insbesondere Gefahren für die Privatsphäre des Einzelnen, befürchtete gleichzeitig aber auch eine Gefährdung des Informationsgleichgewichts zwischen den Bürgern einerseits und dem Staat andererseits sowie zwischen den staatlichen Institutionen selbst. Das waren die Hauptüberlegungen, welche die Datenschutzgesetzgebung in der Bundesrepublik Deutschland auslösten. Es ging nicht nur um technisch-organisatorische Aspekte der automatisierten Datenverarbeitung, sondern auch um wichtige verfassungspolitische Fragen.

Von wem das Wort „Datenschutz“ ursprünglich geprägt wurde, lässt sich heute nicht mehr mit Sicherheit feststellen. Der Begriff tauchte wohl erstmals im Rahmen der Vorarbeiten zum hessischen Datenschutzgesetz auf, das ihn mit seinem Inkrafttreten im Jahre 1970 übernahm. Zuweilen wurde alternativ

noch der Begriff „Informationsschutz“ verwendet. Doch bald hatte sich der Begriff „Datenschutz“ durchgesetzt, auch international: von „Data Protection“ war und ist im angloamerikanischen Sprachraum die Rede von „Protezione dei Dati“ im Italienischen und von „Protección de Datos“ im Spanischen. Glücklich war diese Wortwahl nicht. Dessen war man sich auch bewusst. Sie suggerierte den Eindruck, der Gesetzgeber wolle nur Daten schützen. Dabei ging und geht es doch um den Schutz des Betroffenen vor den Folgen der Datenverarbeitung.

6. In der Bundesrepublik wurde das erste Datenschutzgesetz in Hessen verabschiedet, und zwar – wie gesagt – 1970. Es war damit weltweit das erste Datenschutzgesetz überhaupt. Es versuchte Datenschutz durch eine Reihe von Maßnahmen sicherzustellen, u.a. durch die Einrichtung eines unabhängigen, von Weisungen freien Datenschutzbeauftragten. Als ersten Datenschutzbeauftragten wählte der hessische Landtag den vormaligen Abgeordneten und Chef der hessischen Staatskanzlei Willy Birkelbach.

Am selben Tag, als in Hessen das dortige Landesdatenschutzgesetz in Kraft trat – am 7. Oktober 1970 – brachte die CDU-Fraktion im rheinland-pfälzischen Landtag einen entsprechenden Entwurf für ein rheinland-pfälzisches Landesdatenschutzgesetz ein. Wegen des Ablaufs der Legislaturperiode wurde der Entwurf am 15. September 1971 mit einigen Änderungen erneut eingebracht und nach eingehenden Beratungen im Rechtsausschuss und im Innenausschuss am 17. Januar 1974 vom Landtag verabschiedet. Damit war Rheinland-Pfalz nach Hessen das zweite Bundesland und nach Schweden weltweit das dritte Land, das ein Datenschutzgesetz erlassen hatte. Es trug die Bezeichnung „Landesgesetz gegen missbräuchliche Datenverarbeitung“.

Wie das hessische Datenschutzgesetz beschränkte sich auch das rheinland-pfälzische auf die **maschinelle** Verarbeitung **personenbezogener** Daten und wie dieses auch auf die Datenverarbeitung durch **staatliche** Stellen. Es verpflichtete die öffentlichen Stellen Vorsorge dafür zu treffen, dass schutzwürdige Interessen der Betroffenen bei der elektronischen Verarbeitung ihrer personenbezogenen Daten nicht beeinträchtigt werden. Weder in diesem Gesetz noch im hessischen Datenschutzgesetz fand sich ein Ansatz, auch die Datenverarbeitung durch die Privatwirtschaft in die Gesetze mit einzubeziehen. Das mag auch darin begründet gewesen sein, dass man die Privatsphäre der Bürgerinnen und Bürger in erster Linie vom Staat und weniger von privater Seite bedroht glaubte. Vor allem ging man aber davon aus, dass die Länder für eine Regelung des Datenschutzes in der Privatwirtschaft keine Gesetzgebungskompetenz besaßen. Diese lag beim Bund. Bis auf Weiteres gab es deshalb keine besonderen Datenschutzregelungen für den privaten Bereich.

7. Zwischenzeitlich hatte sich aber auch der Bund um die Regelung eines Bundesdatenschutzgesetzes bemüht. Diese Bemühungen waren aber nicht über erste Entwürfe hinausgegangen, obwohl z.B. der Deutsche Juristentag mit seiner 1972 eingesetzten Datenschutzkommission Anfang 1974 Grundsätze für eine gesetzliche Regelung vorgelegt hatte. Erst im November 1973 kam es zur ersten Lesung eines Entwurfs für ein Bundesdatenschutzgesetz im Deutschen Bundestag. Es folgte eine dreijährige parlamentarische Beratung. In der Geschichte der Bundesrepublik dürfte es bis dahin kaum ein Gesetz gegeben haben, das auf soviel Vorbehalte gestoßen ist und zwar bei Vertretern der Privatwirtschaft ebenso wie bei den Repräsentanten der Verwaltung. Außerdem waren viele Bürgerinnen und Bürger sehr sensibilisiert, z.B. durch Affären wie die um die Abhöraktion um den Atomwissenschaftler Klaus Traube im Zusammenhang mit den Ermittlungen gegen die Rote Armee Fraktion oder durch die Kontrollvorstellungen des damaligen Präsidenten des Bundeskriminalamtes Horst Herold.

Erst am 10. Juni 1976 wurde das Bundesdatenschutzgesetz gegen die Stimmen der Fraktion von CDU/CSU, die keine unabhängige Kontrollinstanz für den Datenschutz wollte, vom Deutschen Bundestag verabschiedet. Danach wurde es aber erst richtig spannend. Denn die Legislaturperiode ging im Herbst 1976 zu Ende und der Bundesrat hatte noch im Juni 1976 den Vermittlungsausschuss angerufen. Der neue Bundestag war schon gewählt, aber noch nicht zusammengetreten, als der alte Bundestag im November 1976 dem Gesetz in der Fassung des Vermittlungsausschusses zustimmte. Ein wohl einmaliger Vorgang in der Geschichte der Bundesre-

publik Deutschland. Der Bundespräsident zögerte deswegen auch mit der Ausfertigung des Gesetzes und ließ zunächst ein Rechtsgutachten erstellen. Im Januar 1977 war es dann soweit. Walter Scheel unterzeichnete das Gesetz, das daraufhin am 1. Februar 1977 im Bundesgesetzblatt verkündet wurde. Wesentliche Teile sollten aber erst 1978 in Kraft treten.

Wiederum beschränkte sich das Gesetz – wie in Hessen und in Rheinland-Pfalz – auf personenbezogene Daten. Aber der Bundesgesetzgeber erfasste – im Unterschied zu Hessen und Rheinland-Pfalz – auch die manuelle Datenverarbeitung, wenn und soweit sie sich auf Dateien bezog. Außerdem unterstellte es die **Datenverarbeitung durch Private** den gesetzlichen Regelungen. Des Weiteren ist die gesetzliche Verpflichtung zur Einrichtung betrieblicher Datenschutzbeauftragter hervorzuheben und ein relativ weitgehender Auskunftsanspruch der Betroffenen, selbst im nicht-öffentlichen Bereich. Im Übrigen galt und gilt das Bundesdatenschutzgesetz nur für die Behörden des **Bundes**. Für die Behörden der Länder wurde dem Bund vom Bundesrat auch dann keine Zuständigkeit zugestanden, wenn diese Bundesgesetze vollzogen. Wie in Hessen wurde auch für den Bund ein Datenschutzbeauftragter bestellt. Erster Bundesdatenschutzbeauftragter wurde im Februar 1978 Prof. Dr. Hans Peter Bull, der sein Amt bis April 1983 wahrnahm. Seine Zuständigkeit beschränkte sich aber im Wesentlichen auf die Bundesverwaltung. Im nicht-öffentlichen Bereich wurde die institutionelle Kontrolle den nach Landesrecht zuständigen Aufsichtsbehörden übertragen. In Hessen wie in Rheinland-Pfalz waren dies die Bezirksregierungen.

8. Kaum war das Bundesdatenschutzgesetz in Kraft getreten, zogen die übrigen Bundesländer nach: Bremen 1977, Bayern, Saarland, Niedersachsen, Schleswig-Holstein, Berlin und Nordrhein-Westfalen 1978, Baden-Württemberg 1979 sowie Hamburg im Jahre 1981. Die landesrechtlichen Datenschutzbestimmungen waren in ihrer rechtlichen Substanz einander ähnlich und oft dem Bundesdatenschutzgesetz nachgebildet. Wo bereits vor dem Inkrafttreten des Bundesdatenschutzgesetzes Landesdatenschutzgesetze bestanden, wurden diese überarbeitet und weitgehend an das Bundesrecht angeglichen. Dies war auch in Rheinland-Pfalz der Fall. Die rheinland-pfälzische Novelle stammt vom Dezember 1978 und erhielt die Bezeichnung „Landesgesetz zum Schutz des Bürgers bei der Verarbeitung personenbezogener Daten“. Unterschiede zum Bundesdatenschutzgesetz gab es vor allem bei der Struktur der Aufsichtsbehörden für den privaten Datenschutz. Sie wurde – wie gesagt – der damaligen Bezirksregierung übertragen, andere Bundesländer betrauten damit ihre Datenschutzbeauftragten.

Im Unterschied zu den meisten Bundesländern und zum Bund gab es in Rheinland-Pfalz zunächst keinen Datenschutzbeauftragten. Die Kontrollaufgabe hatte man hier einem Datenschutzausschuss übertragen, an dessen Stelle im Jahre 1978 die Datenschutzkommission trat. Neben drei Abgeordneten waren ein Vertreter der Landesregierung und ein vom Landtag gewählter Beamter Mitglieder dieser Kommission. Zu den ersten Mitgliedern gehörte Rudolf Scharping, der spätere Ministerpräsident des Landes Rheinland-Pfalz.

9. 1977/1978 begann die Privatwirtschaft mit der Einrichtung von betrieblichen Datenschutzbeauftragten, die nach dem Bundesdatenschutzgesetz vorgeschrieben waren. So gut wie nichts war vorbereitet. Die Unternehmen waren vollauf damit beschäftigt, die mit der EDV verbundenen technisch-organisatorischen Probleme in den Griff zu bekommen. Schon das war schwierig genug. Die neuen Datenschutzbeauftragten wurden deshalb nicht selten als ein weiterer Störfaktor empfunden. Ohnehin gab es kaum jemanden, der mit dem neuen Bundesdatenschutzgesetz zufrieden war. Kaum war es verabschiedet, wurde von überall her der Ruf nach einer Novellierung laut. Damit endete die erste die Phase der Geschichte des Datenschutzes in der Bundesrepublik Deutschland.

Zweite Phase

1. Mit dem Jahr 1983 begann die zweite Phase. Zum Ausdruck kam dies zunächst darin, dass der PC vom Magazin „Time“ zum „Mann des Jahres“ gekürt wurde. Noch wichtiger war die Entscheidung, die das Bundesverfassungsgericht am 15. Dezember 1983 zum Volkszählungsgesetz fällte. Dieses Gesetz, das vom Bundestag und Bundesrat ein Jahr zuvor einstimmig verabschiedet worden war, wurde

vom höchsten deutschen Gericht in wichtigen Teilen für nichtig erklärt. Vorangegangen war eine u.a. vom „SPIEGEL“ und der „taz“ publizistisch begleitete Massenbewegung gegen die Volkszählung, die als „Volksaushorchung“ und „Volksdurchleuchtung“ bekämpft worden war, auch von prominenten Schriftstellern wie Günther Grass und Walter Jens. Sie und die Kläger fürchteten, dass die Vielzahl der Fragen Rückschlüsse auf die Identität der Befragten ermöglichen würde. Ihre Klage hatte Erfolg.

Mit Urteil vom 15. Dezember 1983 wurde das Gesetz für verfassungswidrig erklärt, weil es die Beschwerdeführer in ihrem Recht auf informationelle Selbstbestimmung verletze. Mit diesem Recht hatte das Bundesverfassungsgericht den Datenschutz mit verfassungsmäßigem Rang ausgestattet. Seither ist Datenschutz Grundrechtsschutz. Staatliche Eingriffe in dieses Recht sind danach nur rechtmäßig, wenn

- ein überwiegendes Allgemeininteresse für die Datenverarbeitung spricht,
- die Datenverarbeitung gesetzlich zugelassen ist,
- der Zweck der Datenverarbeitung im Gesetz präzise festgelegt ist und
- das Gesetz bestimmt und verhältnismäßig ist.

Im Übrigen hat das Bundesverfassungsgericht in seiner Volkszählungsentscheidung ausdrücklich bestimmt, dass der Verarbeitungsprozess in jeder seiner Phasen der Kontrolle durch eine eigens dafür eingerichtete, unabhängige Instanz, den Datenschutzbeauftragten, unterliegen muss. In einer späteren Entscheidung aus dem Jahre 1988 hat es ausdrücklich darauf hingewiesen, dass diese Voraussetzungen generell für den Umgang mit personenbezogenen Daten erfüllt werden müssen und nicht nur dann, wenn die Verarbeitung der Daten in automatisierter Form erfolge. Überraschen konnte diese Entscheidung nicht, denn bereits vor der Volkszählungsentscheidung hatte Karlsruhe wiederholt u.a. im Jahre 1970 deutlich gemacht, dass staatliche Eingriffe in das allgemeine Persönlichkeitsrecht ohne Einwilligung des Betroffenen nur rechtmäßig sein können, wenn diese Eingriffe im überwiegenden allgemeinen Interesse erfolgten und verhältnismäßig seien.

2. Der hessische Gesetzgeber war der erste Landesgesetzgeber, der die Konsequenzen aus der Volkszählungsentscheidung zog. 1986 novellierte er das Hessische Datenschutzgesetz. Er verwarf die Verknüpfung der gesetzlichen Regelungen mit der Verarbeitung in „Dateien“, bezog die Akten ausdrücklich ein, stellte klar, dass es für die Erhebung von Daten genauso gesetzlicher Bestimmungen bedarf wie für jede andere Verarbeitungsphase, schrieb die Zweckbindung fest, räumte dem Datenschutzbeauftragten ein uneingeschränktes Kontrollrecht ein und formulierte zugleich eine Reihe bereichsspezifischer Vorschriften, vor allem für die Verarbeitung von Arbeitnehmerdaten sowie die Verwendung personenbezogener Angaben im Rahmen wissenschaftlichen Forschungen.

In den folgenden drei Jahren wurden das Bremische, das Nordrhein-Westfälische, das Hamburgische und das Berliner Datenschutzgesetz novelliert. Wie die hessische Novelle konkretisierten auch diese vier Gesetzesänderungen die Vorgaben des Bundesverfassungsgerichtes und legten damit einen neuen, gemeinsamen legislativen Rahmen für die Verarbeitung personenbezogener Daten fest. Die übrigen Bundesländer warteten mit ihrer Novelle auf den Bundesgesetzgeber.

3. Zur Novellierung des Bundesdatenschutzgesetzes kam es nach quälend langen Beratungen aber erst im Dezember 1990. Sieben Jahre hatte der Bund sich Zeit gelassen, um die Volkszählungsentscheidung des Bundesverfassungsgerichts normativ umzusetzen. Dies gelang nur zum Teil. Simitis spricht in seiner Kommentierung zum Bundesdatenschutzgesetz davon, dass es sich bei der Novellierung letztlich um ein „Flickwerk“ gehandelt habe. Anders als die bis dahin novellierten Landesdatenschutzgesetze blieb das Bundesdatenschutzgesetz beim „Dateibegriff“, Akten und Aktensammlungen wurden von ihm – auch im nicht-öffentlichen Bereich – nicht erfasst, neue technologische Entwicklungen – wie die Videotechnologie – noch nicht einmal angesprochen. Überarbeitet wurden dagegen die Regelungen über den Bundesdatenschutzbeauftragten. Er wurde der Rechtsaufsicht der Bundesregierung und der Dienstaufsicht des Bundesministers des Innern, bei dem er eingerichtet war, unterstellt. Seine Aufgabe bestand in der Kontrolle der „öffentlichen Stellen des Bundes“, wobei sich diese

auch auf die personenbezogenen Daten in Akten erstreckte, soweit Anhaltspunkte bestanden, dass Rechte von Betroffenen verletzt worden sind.

Das neue Bundesdatenschutzgesetz kam nicht allein, sondern war Teil eines Gesetzespakets. Zu diesem Paket gehörte vor allem eine Reihe von Sicherheitsgesetzen, mit denen u.a. dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst (MAD) und dem Bundesnachrichtendienst (BND) Rechtsgrundlagen für deren Datenverarbeitung geschaffen wurden. Dies war die Folge der Volkszählungsentscheidung des Bundesverfassungsgerichts, nach der für jede Datenverarbeitung spezifische gesetzliche Regelungen erforderlich waren. So sehr man dies auf Seiten der Datenschützer begrüßte, so sehr sprach man später von einer „Vergesetzlichungsfalle“. Diese „Falle“ konnte darin gesehen werden, dass der Gesetzgeber wegen der verfassungsrechtlichen Notwendigkeit von bereichsspezifischen Einzelfallregelungen alles gesetzlich erlaubte, was der Verwaltung sinnvoll oder notwendig erschien.

4. Nach dem Inkrafttreten dieses Gesetzespakets änderte auch der rheinland-pfälzische Landtag im Jahre 1991 sein Landesdatenschutzgesetz, indem es u.a. an die Stelle der bisherigen Datenschutzkommission einen – nebenamtlich tätigen – Landesbeauftragten für den Datenschutz setzte. Die Datenschutzkommission blieb als beratendes Organ für den Landesdatenschutzbeauftragten bestehen. Erster Landesbeauftragter für den Datenschutz wurde Prof. Dr. Walter Rudolf, der sein Amt bis zum Jahre 2007 wahrnahm.

Zu einer inhaltlichen Novellierung des rheinland-pfälzischen Landesdatenschutzgesetz kam es allerdings erst im Jahre 1994. Klargestellt wurde jetzt, dass es unabhängig davon anwendbar war, ob personenbezogene Daten automatisiert oder nicht automatisiert verarbeitet werden und ob sie in Dateien, Akten oder sonstigen Unterlagen gespeichert oder aufgezeichnet sind. Hervorzuheben sind außerdem die gesetzliche Ausgestaltung des Zweckbindungsgrundsatzes, die Weiterentwicklung der Auskunftsrechte des Bürgers, die gegenüber früherem Datenschutzrecht weiterreichenden Kontrollbefugnisse des Datenschutzbeauftragten und die Pflicht der Behörden des Landes und der Kommunen, interne Datenschutzbeauftragte zu bestellen.

Damit war die zweite Phase des Datenschutzes, die 1983 mit der Volkszählungsentscheidung begonnen hatte, abgeschlossen. Die Gesetzeslandschaft hatte sich grundlegend verändert. Aber auch die Datenverarbeitung stand an der Schwelle einer Revolution. Am 30. April 1993 war nämlich die Freigabe des World Wide Web für die allgemeine Nutzung erfolgt. Es begann sich innerhalb kürzester Zeit ein globales Kommunikationsnetz für alle zu etablieren. Es war höchste Zeit, dass sich jetzt auch die Europäische Union des Datenschutzes annahm.

Dritte Phase

1. Auf europäischer Ebene lagen die Interessengegensätze auf der Hand. Für die Europäische Kommission hatte die Sicherstellung des freien Waren- und Dienstleistungsverkehrs innerhalb der Gemeinschaft Vorrang vor allen anderen Überlegungen. Sonderregelungen für den Umgang mit personenbezogenen Daten waren aus dieser Sicht ebenso unerwünscht, wie jede andere Ausnahmevorschrift für marktfähige Güter. Andererseits war klar geworden, dass Datenverarbeitung nicht mehr auf Ländergrenzen zu beschränken war, und dass die ganz unterschiedliche Rechtslage in den verschiedenen Mitgliedstaaten in Bezug auf Datenschutz und Datensicherung sich zu einem ernsthaften Hemmnis für den Austausch elektronisch basierter Dienstleistungen entwickelte. Hinzu kam die Orientierung der Gemeinschaft an den Menschen- bzw. Grundrechten mit und nach den Maastrichter Verträgen. Klar war das Ziel, durch eine Richtlinie einen Ausgleich des Datenschutzniveaus in den einzelnen Mitgliedstaaten herbeizuführen.

Die Schwierigkeit bestand darin, unterschiedliche nationale Rechtskulturen auf einen Nenner zu bringen. Dies geschah mit der „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ vom 24. Oktober 1995. Ohne Zweifel stellt diese Richtlinie keinen konzeptionellen Neuentwurf „aus einem Guss“ dar, sondern ein „Patchwork“ aus unterschiedlichen einzelnen staatlichen Datenschutzsystemen. Der Sonderschutz für die

sensitiven Daten (Art. 8) stammt u.a. aus Frankreich, das Registrierungssystem (Art. 18 f.) kennen fast alle unserer Nachbarländer, die Anerkennung der von Verbänden ausgehandelten Verhaltensregeln (Art. 27) kommt aus den Niederlanden usw. Die Struktur der Richtlinie ist allerdings sehr „deutsch“ ausgefallen. Belege für diese These sind u.a. die Begriffsbestimmungen, das Prinzip des „Verbots mit Erlaubnisvorbehalt“ sowie die Enumerierung von Zulässigkeitstatbeständen, die denen des Bundesdatenschutzgesetzes sehr ähnlich sind. Ein wesentlicher Unterschied zum deutschen Datenschutzsystem findet sich allerdings bei der Datenschutzkontrolle (Art. 28). Die Richtlinie geht von einem einheitlichen Überwachungsstandard in Verwaltung und Wirtschaft aus. Die Unterscheidung zwischen Datenschutzbeauftragten und sonstigen Aufsichtsbehörden für die Privatwirtschaft wird nicht aufgegriffen. Im Gegenteil: Die Richtlinie fordert, dass die externe Datenschutzkontrolle auch in der Privatwirtschaft „völlig unabhängig“ wahrgenommen wird.

2. Die deutschen Gesetzgeber im Bund und in den Ländern waren verpflichtet, die Vorgaben der europäischen Datenschutzrichtlinie bis zum 24. Oktober 1998 in nationales Recht umzusetzen. Es gab also eine dreijährige Übergangsfrist. Sie wurde nicht eingehalten, weder vom Bund noch von den Ländern. Die Novellierung des Datenschutzrechts genoss wieder einmal keinen Vorrang. In Rheinland-Pfalz kam es statt dessen in der ersten Hälfte des Jahres 2000 zu einer Verankerung des Datenschutzes in der Landesverfassung. Dies ging zurück auf eine Empfehlung der Enquete-Kommission „Verfassungsreform“ aus dem Jahr 1994. In dem neuen Art. 4a LV heißt es seither:

„(1) Jeder Mensch hat das Recht, über die Erhebung und weiterere Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen. Jeder Mensch hat das Recht auf Auskunft über ihn betreffende Daten und auf Einsicht in amtliche Unterlagen, soweit diese solche Daten enthalten.

(2) Diese Rechte dürfen nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern.“

Der rheinland-pfälzische Verfassungsgeber folgte damit einer Reihe von Bundesländern. Im Bund sind dagegen bis heute Versuche, den Datenschutz ausdrücklich in den Grundrechtekatalog des Grundgesetzes aufzunehmen, gescheitert.

Dafür gelang es dem Bund im Jahr 2001 endlich die europäische Datenschutzrichtlinie umzusetzen. Die entsprechende Novellierung des Bundesdatenschutzgesetzes trat am 23. Mai 2001 in Kraft. Sie brachte die Einführung von Grundsätzen wie sie im datenschutzrechtlichen Schrifttum schon längst gefordert worden waren. Dazu zählen u.a. die Grundsätze der Datenvermeidung und Datensparsamkeit in § 3a, der Aspekt „Datenschutz durch Technik“, pseudonymes und anonymes Handeln und die Verankerung einer Regelung zum Datenschutzaudit in § 9a. Neu ist auch die Anerkennung der Selbstregulierung durch die Anwender in § 38a, in dem das Gesetz die Einführung von „Codes of Conduct“ als bereichs- oder branchenspezifische Standesregeln ausdrücklich unterstützt. Aufgenommen wurden auch Regelungen zur Videoüberwachung in § 6b und zu mobilen Speicher- und Verarbeitungsmedien in § 6c. Ferner wurde der sachliche Anwendungsbereich des Gesetzes insbesondere für die Privatwirtschaft erweitert, in dem nunmehr jede unter Einsatz von Datenverarbeitungsanlagen erfolgte Verarbeitung personenbezogener Daten erfasst wird. Ferner finden sich Regelungen für die Rechtsanwendung bei grenzüberschreitenden Tätigkeiten in §§ 4b und c. Erfolgen diese von einer deutschen Niederlassung aus, gilt deutsches Recht und im Übrigen das Datenschutzrecht des Sitzstaates. Erweitert wurde auch die Datenschutzkontrolle durch die Aufsichtsbehörde, die nunmehr generell von Amts wegen tätig wird und ein eigenes Strafantragsrecht hat. Wenn man so will, war dies das dritte Bundesdatenschutzgesetz. 1977 war das erste erlassen worden, 1990 war es in Folge der Volkszählungsentscheidung novelliert worden und das Gesetz vom Jahre 2001 war eben die Umsetzung der EG-Datenschutzrichtlinie. Immer war der Bund einigen fortschrittlicheren Ländern hinterher gehinkt, in der Regel dem Bundesland Hessen und seinem Datenschutzbeauftragten Simitis.

3. Rheinland-Pfalz setze mit seinem Landesgesetz vom 8. Mai 2002 die Europäische Datenschutzrichtlinie um. Als wesentliche Neuregelungen sind hervorzuheben:

- der Grundsatz der Datensparsamkeit und der Datenvermeidung (§ 1 Abs. 3),
- der besondere Schutz für „besondere Arten von personenbezogenen Daten“ wie z.B. Angaben über die ethnische Herkunft oder die Gesundheit (§ 3 Abs. 9),
- Schranken für automatisierte Einzelentscheidungen (§ 5 Abs. 5),
- die Verfügbarkeits-, Zeckbindungs-, Dokumentations- und Verarbeitungskontrolle (§ 9 Abs. 2 Nr. 7 bis 10) sowie die Vorabkontrolle (§ 9 Abs. 5),
- das Recht auf Benachrichtigung (§ 18 Abs. 1 und 2) und
- das Widerspruchsrecht auch für die Fälle einer rechtmäßigen Datenverarbeitung (§ 19 Abs. 4).

Mit der Anpassung des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder war die nächste – die dritte – Phase des Datenschutzes in der Bundesrepublik Deutschland abgeschlossen. Und wiederum hatten sich die Informations- und Kommunikationstechniken beinahe revolutionär weiterentwickelt. Der PC war zu einem Arbeitsmittel für jedermann, zu einem multimedialen Endgerät mit nahezu unbegrenzter Kommunikationsfähigkeit geworden. In Mailinglisten, Foren und Chaträumen diskutierten Menschen, die sich nie zuvor gesehen haben und die sich in den allermeisten Fällen auch nie sehen werden, über eine schier unerschöpfliche Vielfalt an Haupt- und Nebensächlichkeiten. Die Welt war zum Dorf geworden. Das „Netz der Netze“ war zum Medium für alle geworden, und zwar in seiner neuen interaktiven Form des Web 2.0. „Electronic Commerce“ ist eine Zukunftsvision des Handels, „Electronic Government“ die entsprechende der Verwaltung.

Vierte Phase

1. Der Beginn der vierten und bisher letzten Phase des Datenschutzes geht einher mit der Globalisierung der Datenverarbeitung und insbesondere der Existenz des Internets auf der einen Seite und dem 11. September 2001, also den terroristischen Anschlägen in den USA, auf der anderen Seite. Der Anschlag auf das World Trade Center hatte auch in der Bundesrepublik Deutschland eine Vielzahl von gesetzgeberischen Maßnahmen im Sicherheitsbereich zur Folge, die tief in das informationelle Selbstbestimmungsrecht eingriffen, so tief, dass sie zum Teil vom Bundesverfassungsgericht als verfassungswidrig aufgehoben worden sind. Seine Entscheidung über die geheime Online-Durchsuchung von Computern ist nur ein Beispiel hierfür. Das neue Grundrecht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme ist jedenfalls ein Ausdruck dieser Entwicklung.

2. Die Globalisierung der Datenverarbeitung, die Weiterentwicklung der Informations- und Kommunikationstechnologie und die zunehmenden Präventionsaktivitäten des Staates machen eine Modernisierung des Datenschutzes überfällig. Dafür hat sich seit vielen Jahren auch der Deutsche Bundestag ausgesprochen. Allerdings ist es dazu bisher noch nicht gekommen. Nicht zuletzt deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2010 das Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ beschlossen. Darin wird eine Vielzahl von Vorschlägen aufgelistet, mit denen man den Datenschutz an das Internetzeitalter anpassen will. U.a. wird vorgeschlagen, zentrale Prinzipien, insbesondere die Erforderlichkeit, die Zweckbindung und das Verbot der heimlichen Profilbildung ausdrücklich gesetzlich zu regeln, um auf diese Weise einen verbindlichen Mindeststandard festzulegen. Außerdem müsse die Datenverarbeitung transparenter werden. Insbesondere müssten die Betroffenen in die Lage versetzt werden, ihre Rechte auf Auskunft, Berichtigung oder Löschung auf einfache Weise, insbesondere auf elektronischem Wege wahrnehmen zu können. Entwickler und Verwender informationstechnischer Systeme sollten gesetzlich verpflichtet werden, datenschutzfreundliche Techniken bereitzustellen und einzusetzen („Privacy by Design“). Den Betroffenen, die zunehmend selbst aktive Teilnehmer an IT-Verfahren seien und dabei persönliche Daten von sich und Dritten verwendeten, sollten IT-Produkte und Dienste mit dem jeweils datenschutzfreundlichsten Einstellungen zur Verfügung gestellt werden („Privacy by Default“).

Im Übrigen wird in dem Eckpunktepapier – wie gesagt – betont, dass das Datenschutzrecht endlich internetfähig werden müsse. Dabei komme der grundsätzlich unbeobachteten Nutzung elektronischer Dienste besondere Bedeutung zu. Ebenso wie das Internet global sei, müssten auch datenschutzrechtliche Mindeststandards global gelten und durchgesetzt werden können. Zusätzlich müssten aber auch die Anreize gestärkt werden, dass die verantwortlichen Stellen den Datenschutz als eigenes Anliegen begriffen. Dies könne beispielsweise durch ein Datenschutzaudit geschehen, also durch die Zertifizierung der Datenschutzeigenschaften von Produkten und Diensten, und zwar auf der Basis unabhängiger Begutachtung.

Für die Gewährleistung des technischen und organisatorischen Datenschutzes und der Datensicherheit sollten allgemeinverbindliche Schutzziele festgeschrieben werden. Auf diese Weise würde ein technikneutraler und flexibler Ansatz geschaffen, der den grundsätzlichen Vorgaben des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch bei sich verändernden technologischen oder organisatorischen Rahmenbedingungen Rechnung trage. Da die bei Verstößen gegen das Datenschutzrecht vorgesehenen Sanktionen sich nicht als ausreichend erwiesen hätten, müsste die Durchsetzung von Schadensersatzansprüchen sowie die Verfolgung von Ordnungswidrigkeiten erleichtert werden.

3. Ausgelöst durch eine Reihe von Datenschutzskandalen und das dadurch neu geweckte Interesse der Öffentlichkeit am Datenschutz hatten sich die parlamentarischen Gremien mit mehreren Änderungsgesetzen zum Bundesdatenschutzgesetz zu befassen. Nach langer Vorbereitung ist als erstes der Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BT-Drs 16/10529) im August 2008 eingebracht worden, der verbesserte Datenschutzregelungen für die Tätigkeit von **Auskunfteien** und erstmals auch gesetzliche Vorgaben für **Scoringverfahren** enthielt. Das Gesetz wurde im Mai 2009 beschlossen (BGBl. IS. 2254) und ist am 1. April 2010 in Kraft getreten.

Um das zweite Änderungsgesetz gab es sehr viel heftigere Diskussionen. Als Reaktion auf die durch Datenskandale einer breiten Öffentlichkeit deutlich gewordenen erheblichen Defizite beim Umgang mit personenbezogenen Daten zahlreicher Bürgerinnen und Bürger sollte § 9a BDSG durch eine gesetzliche Regelung zum **Datenschutzaudit** ausgefüllt und der Handel mit **Adressdaten zu Werbezwecken** eingeschränkt bzw. von der ausdrücklichen Einwilligung der Betroffenen abhängig gemacht werden (Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011). Dieses Vorhaben der Bundesregierung stieß aber auf erheblichen Widerstand. Der Entwurf wurde deshalb entscheidend verändert. Als „Kompensation“ sind im Gesetzgebungsverfahren eine Reihe von zusätzlichen positiv zu bewertenden Änderungen in anderen Bereichen aufgenommen worden, z.B. Regelungen über die **Auftragsdatenverarbeitung** und die **Informationspflicht bei Datenschutzpannen**. In § 32 BDSG wurde zudem eine Grundregelung zum **Beschäftigtendatenschutz** verabschiedet.

Ausgelöst durch die intensiven Diskussionen um den Google-Dienst „Street View“ fand im September 2010 ein „Datenschutzgipfel“ beim Bundesinnenminister statt, der zwei Resultate hatte: Zum einen verpflichtete sich der Bundesverband der Internet-Unternehmen („Bitkom“) dazu, einen Verhaltenskodex seiner Mitgliedsunternehmen für die Veröffentlichung solcher Dienste im Internet zu erstellen. Zum andern legte der Bundesinnenminister einen Gesetzentwurf vor, der durch neue Regelungen im Bundesdatenschutzgesetz nicht überschreitbare Grenzen für Internet-Veröffentlichungen aller Art (sog. „Rote Linien“) markieren sollte. Dazu soll z.B. das Verbot der Erstellung von Persönlichkeitsprofilen durch die Auswertung der Aktivitäten von Netznutzern gehören, aber auch das Verbot des Einsatzes von Bilderkennungssoftware zur Identifizierung Einzelner im Netz. Dieses Gesetzgebungsvorhaben ist derzeit ins Stocken geraten und deshalb noch nicht abgeschlossen.

4. Parallel zu dieser in Deutschland zu führenden Diskussion hat die europäische Kommission einen Prozess der grundlegenden Überarbeitung der Europäischen Datenschutzrichtlinie eingeleitet (Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der

Regionen: Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endg.). Dieser Prozess hat mittlerweile u.a. zum Entwurf einer europäischen Datenschutz-Grundverordnung geführt, die auch im europäischen Parlament abschließend behandelt wurde. Allerdings ist es bis jetzt noch nicht zu einer Einigung zwischen Parlament, Kommission und Rat gekommen.

A.2 Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Datenschutz-Grundverordnung KOM (2012) 11 endg. vom 25. Januar 2012 – Stand 11. Juni 2012

Angesichts des rasanten technologischen Fortschritts, zunehmender Vernetzung und Globalisierung ist der grundrechtsorientierte Ansatz des europäischen Datenschutzrechts mit vielfältigen Herausforderungen konfrontiert. Das durch Art. 8 der Europäischen Grundrechtecharta garantierte Grundrecht auf den Schutz personenbezogener Daten ist seit dem Inkrafttreten des Vertrags von Lissabon unmittelbar anwendbares Recht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) begrüßt deshalb das von der Kommission verfolgte Ziel eines hohen gemeinsamen Datenschutzniveaus in der gesamten Europäischen Union.

Mit der Datenschutz-Grundverordnung (Verordnung) strebt die Kommission eine Harmonisierung des Datenschutzrechts an. Die Konferenz hält es für sinnvoll und erforderlich, einen effektiven Datenschutz für alle Bürgerinnen und Bürger in Europa zu gewährleisten. Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Verordnung auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungen im öffentlichen Bereich erstreckt, ist die Konferenz der Auffassung, dass auch insoweit ein möglichst hoher Mindeststandard gewährleistet werden muss. Es darf insgesamt zu keiner Absenkung des in den Mitgliedsstaaten bereits erreichten Schutzniveaus kommen. Die Mitgliedsstaaten sollten daher auch in Zukunft – vor allem bei besonders sensiblen Datenverarbeitungen – gesetzliche Regelungen mit einem möglichst hohen Schutzniveau erlassen dürfen. Die Verordnung muss in jedem Fall den Verfassungs- und Rechtstraditionen der Mitgliedsstaaten Rechnung tragen.

Der Entwurf ermächtigt die Kommission in einer Vielzahl von Vorschriften zu einer näheren Regelung durch delegierte Rechtsakte. Die Konferenz appelliert an das Europäische Parlament und den Rat, die Notwendigkeit jeder einzelnen Delegationsermächtigung kritisch zu überprüfen. Im Hinblick auf den Wesentlichkeitsgrundsatz müssen entsprechend Art. 290 AEUV die entscheidenden Regelungen in der Verordnung selbst getroffen oder aber im Hinblick auf fachspezifische Regelungen dem nationalen Gesetzgeber überlassen werden. Auch wenn das Parlament bei einer Ausübung der Delegationsrechte durch die Kommission auf den Erlass dieser Rechtsakte einwirken kann, ist deren demokratische Legitimation deutlich geringer, als bei einer Regelung der wesentlichen Punkte in der Verordnung selbst. Die Konferenz lehnt daher insbesondere solche delegierten Rechtsakte ab, bei denen grundlegende materiell- und verfahrensrechtliche Regelungen (wie z.B. in Art. 6 bei der Rechtmäßigkeit der Verarbeitung) konkret ausgestaltet werden sollen.

Die Konferenz weist auch darauf hin, dass der Entwurf in zahlreichen Regelungen unbestimmte Rechtsbegriffe sowie Interessenabwägungen enthält, deren hoher Abstraktionsgrad einen großen Spielraum bei der Auslegung und Anwendung zulässt. Sie empfiehlt dringend, die notwendigen Klarstellungen in den Regelungen selbst vorzunehmen.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf vorgesehene Kohärenzverfahren, welches in der gegenwärtigen Ausgestaltung die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb stark vereinfacht und praktikabler gestaltet werden. Die durch Art. 8 der Grundrechtecharta und Art. 16 AEUV gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete

Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Die Konferenz hält es für erforderlich, die in den Art. 8 (3), 12 (6), 14 (7) und 22 (4) vorgesehenen Ausnahmen für die Datenverarbeitung kleiner und mittlerer Unternehmen (KMU) zu überprüfen. Ausnahmen sollten sich generell weniger an der Größe eines Unternehmens, sondern vielmehr an den Gefahren und Risiken für die Rechte und Freiheiten des Einzelnen orientieren. Auch von sehr kleinen Unternehmen können erhebliche Gefährdungen für den Datenschutz ausgehen.

Der Entwurf der Verordnung führt in erheblichem Umfang zu Abgrenzungsschwierigkeiten mit der RL 2002/58/EG. Art. 89 (1) ist insoweit zu abstrakt und unklar formuliert. Welche besonderen Pflichten gibt es konkret, die in der Richtlinie 2002/58/EG festgelegt sind? Weder Art. 89 noch die einschlägige Erwägung 135 geben hierüber Aufschluss.

Die Konferenz schlägt vor, eine Regelung „Erziehung und Bildung“ aufzunehmen. Der Datenschutz dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

„Art. Xx – Erziehung und Bildung

Um sich in der Informationsgesellschaft behaupten zu können, ist den Bürgerinnen und Bürgern durch geeignete Maßnahmen Datenschutzkompetenz zu vermitteln. Sie ist Teil der übergreifenden Medienkompetenz; ihre Vermittlung ist eine gesamtgesellschaftliche Aufgabe in den Mitgliedstaaten, die hierbei von der Union unterstützt werden.“

Zu den einzelnen Regelungen nimmt die Konferenz wie folgt Stellung:

Kapitel I – Allgemeine Bestimmungen

Zu Art. 2:

Die Konferenz spricht sich dafür aus, dass auch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union entweder in den Geltungsbereich der Verordnung einbezogen werden (Art. 2 (2) lit. b)) oder die Verordnung 45/2001 zeitgleich angepasst wird. Es wäre nicht vertretbar, wenn sich die EU selbst von der angestrebten Modernisierung des Datenschutzrechts ausnehmen würde. Zudem spricht auch das Ziel der Harmonisierung für eine Einbeziehung der Organe der Union, da zunehmend auch zwischen diesen und den Mitgliedstaaten ein Austausch personenbezogener Daten stattfindet.

Die Beibehaltung der Ausnahme der Datenverarbeitung durch natürliche Personen zu ausschließlichen persönlichen oder familiären Zwecken in Art. 2 (2) lit. d) wird grundsätzlich begrüßt. Allerdings wäre eine Klarstellung wünschenswert, die in einer differenzierten Regelung die datenschutzrechtlichen Pflichten von natürlichen Personen angemessen ausgestaltet. Dies könnte beispielsweise in einer eigenständigen Regelung zur Veröffentlichung personenbezogener Daten an einen unbestimmten Personenkreis geschehen.

Zu Art. 3:

Die Konferenz begrüßt die Einführung des Marktortprinzips in der Verordnung.

Zum räumlichen Anwendungsbereich für Verarbeitungen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen weist sie darauf hin, dass Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland nur nach Maßgabe bislang nicht existierender zwischenstaatlicher Verträge bestehen. In Vorentwürfen der Verordnung war deshalb bereits vorgesehen, dass der innerhalb der EU zu bestellende Vertreter (Art. 25) umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten solle. Dessen zusätzliche Einbeziehung in die Rechte und Pflichten wäre aus Sicht der Konferenz zu begrüßen.

Der Begriff der „Beobachtung“ sollte konkretisiert werden (Art. 3 (2) lit. b)), weil nicht hinreichend klar ist, welche Anwendungsfälle hierdurch erfasst werden sollen.

Zu Art. 4:

Die Definition der „betroffenen Person“ sollte ohne die Formulierung „nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde“, die damit eine subjektive Komponente impliziert, wie folgt gefasst werden: „eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt von der für die Verarbeitung verantwortlichen oder jeder sonstigen natürlichen oder juristischen Person bestimmt werden kann“ (Art. 4 (1)).

Es sollte auch klargestellt werden, dass Kennnummern, Standortdaten usw. zu den personenbezogenen Daten zählen (siehe Erwägungsgrund 23 der bekannt gewordenen Entwurfsfassung 56; Art. 4 (1) und (2)).

Es sollte definiert werden, was „automatisiert“ bedeutet (Art. 4 (3)).

In der Definition der „Datei“ sollte klargestellt werden, dass die Zugänglichkeit nach mindestens einem bestimmten Kriterium ausreicht (Art. 4 (4)).

Die Definition der „biometrischen Daten“ sollte nicht nur auf die eindeutige Identifizierbarkeit abstellen, sondern auch das harmonisierte biometrische Vokabular verwenden: „Daten zu den physischen, physiologischen oder verhaltenstypischen Charakteristika eines Menschen wie Gesichtsbilder oder daktyloskopische Daten“ (Art. 4 (11)).

Für Betroffene und Aufsichtsbehörden fehlt es an Transparenz und Verlässlichkeit, wenn die Hauptniederlassung über unternehmensinterne Regelungen („Ort [...], an dem die Grundsatzentscheidungen [...] getroffen werden“) bzw. über den Schwerpunkt der Verarbeitung („Ort, an dem die Verarbeitungstätigkeiten [...] hauptsächlich stattfinden“) definiert wird. Eine Präzisierung wird dringend für erforderlich gehalten, insbesondere im Hinblick auf die Regelungen des „One-Stop-Shops“ in Art. 51 (2) sowie die Regelungen des gerichtlichen Rechtschutzes in Kapitel VIII.

Die Definition des „Dritten“ sollte in Art. 4 aufgenommen werden, um insbesondere die Figur des Auftragsdatenverarbeiters entsprechend Art. 2 lit. f)) der RL 95/46/EG klarer zu fassen.

Die Begriffe „Anonymisierung“ und „Pseudonymisierung“ sollten ebenfalls definiert werden, da beiden Vorgängen materiell-rechtlich eine größere Bedeutung eingeräumt wird und aus Sicht der Konferenz auch eingeräumt werden sollte.

Kapitel II – Grundsätze

Zu Art. 5:

Als weiterer Grundsatz sollte in Art. 5 die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind, um die hohe Bedeutung des technologischen Datenschutzes zu unterstreichen.

Die Zweckbindung ist bei der Verarbeitung personenbezogener Daten eines der wichtigsten Grundprinzipien zur Gewährleistung des Datenschutzes. Im Hinblick auf Art. 5 lit. b) sollte die Zweckbindung deshalb strikter gefasst werden. Zumindest erwartet die Konferenz die Klarstellung, dass der in der Verordnung gewählte Begriff der Zweckvereinbarkeit der Zweckbindung im Sinne des deutschen Datenschutzrechts entspricht.

In Art. 5 lit. e) sollte zusätzlich die anonyme und pseudonyme Nutzung der Daten als Gestaltungsauftrag mit aufgenommen werden. Dies sollte im Weiteren mit Regelungen zu einer Privilegierung der pseudonymen Datenverarbeitung flankiert werden.

Zu Art. 6:

Die Abwägungsklausel des Art. 6 (1) lit. f) wird in der Praxis eine herausragende Bedeutung erlangen. Die Vorgaben und Maßstäbe, anhand derer die Interessenabwägung innerhalb dieser Auffangregelung vorzunehmen ist, müssen daher hinreichend klar sein. In Art. 6 (1) lit. f) sollte eine Regelungsstruktur gefunden werden, die branchen- und situationsspezifischen Konkretisierungen Rechnung trägt. Die Verordnung sollte dabei beispielsweise auf die spezifischen Datenschutzaspekte der Auskunfteien

und des Scorings eingehen. Im Hinblick auf die Verarbeitung von personenbezogenen Daten zu Direktmarketingzwecken sollte – wie in der bekannt gewordenen Entwurfsfassung 56 – grundsätzlich ein Einwilligungserfordernis (opt-in) vorgesehen werden.

Zudem erscheint es – wie Art. 20 des Vorschlags zeigt – auch denkbar, abschließende Fallgruppen zu definieren, die einer Interessenabwägung aufgrund des hohen Gefährdungspotentials der Datenverarbeitung von vornherein nicht zugänglich sind.

Vor dem Hintergrund des in Art. 290 AEUV niedergelegten Wesentlichkeitsgrundsatzes sollten die hier geforderten Konkretisierungen in der Verordnung selbst formuliert werden, da es sich um wesentliche Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten handelt. Art. 6 (5) wäre daher zu streichen.

Ausgehend von Art. 6 (3) lit. b) ist sicherzustellen, dass durch den Verweis auf das mitgliedstaatliche Recht im öffentlichen Bereich ein über die Anforderungen der Verordnung hinausgehendes Datenschutzrecht erhalten bleiben kann, wie dies in verschiedenen bundes- und landesrechtlichen Regelungen bereits jetzt verwirklicht ist. Es muss auch weiterhin ohne Zweifel gewährleistet sein, dass in einem ausdifferenzierten bereichsspezifischen Datenschutzrecht dem erhöhten Schutzbedarf staatlicher Datenverarbeitung auch in Zukunft Rechnung getragen wird. Dies muss sich eindeutig und ausdrücklich aus dem Wortlaut von Art. 6 (3) lit. b) ergeben. Anderenfalls wäre der derzeit bestehende besondere Schutz, beispielsweise der in der Bundesrepublik Deutschland bestehende Schutz von Sozialdaten, durch die Verordnung gefährdet.

Zu Art. 7:

Die Konferenz unterstützt die Absicht der Kommission, in Art. 7 (4) die Freiwilligkeit von Einwilligungen zu konkretisieren. Sie weist allerdings darauf hin, dass ein erhebliches Ungleichgewicht nur ein Indiz für Unfreiwilligkeit sein kann.

Zu Art. 8:

Der besondere Schutz von Kindern und Jugendlichen bei der Verarbeitung der auf sie bezogenen Daten ist der Konferenz ein besonderes Anliegen. Insofern begrüßt sie, dass sich der Verordnungsentwurf dieser Thematik annimmt und sie in einer spezifischen Regelung verankern will. Die Vorschrift sollte sich jedoch stärker an den konkreten, für diese Altersgruppe spezifischen Gefährdungen orientieren. Aus diesem Grunde sollte bei Einwilligungen auch stärker auf die Einsichtsfähigkeit des Kindes und weniger auf starre Altersgrenzen abgestellt werden.

In Art. 8 (1) sollte das Regelungsziel der Norm präzisiert werden. Es ist zu klären, ob eine Beschränkung auf Dienste der Informationsgesellschaft ausreichend ist, da es sich gemäß der Begriffsbestimmung aus der Richtlinie 98/34/EG hierbei in der Regel um gegen Entgelt erbrachte Dienste handelt, obwohl offensichtlich auch entgeltfreie Dienste erfasst werden sollen. Einer Klarstellung bedarf auch, wann einem Kind solche Dienste „direkt“ angeboten werden. Es ist ebenfalls zu klären, ob sich Art. 8 (1) ausschließlich auf solche Datenverarbeitungen bezieht, bei denen die Rechtmäßigkeit nach Art. 6 (1) lit. a) auf die Einwilligung gestützt wird oder ob bei jeder Datenverarbeitung der Einwilligungsvorbehalt der Eltern bzw. gesetzlichen Vertreter gelten soll.

Zudem ist das Verhältnis zwischen den Absätzen 1 und 2 des Art. 8 klärungsbedürftig.

Die Profilbildung (Art. 20) sollte bei Minderjährigen generell verboten sein.

Zu Art. 9:

Art. 9 soll den bedeutsamen Bereich der Zulässigkeit der Verarbeitung von besonderen Kategorien personenbezogener Daten regeln. Die Konferenz sieht hier den aus Art. 8 der RL 95/46/EG übernommenen Ansatz eines abschließenden Katalogs sensitiver Daten kritisch. Vorzugswürdig wäre es, auf den tatsächlichen Verarbeitungskontext abzustellen und den Katalog der sensitiven Daten als Regelbeispiele auszugestalten.

Die Vorgaben sind im Sinne des Wesentlichkeitsgrundsatzes in der Verordnung selbst zu treffen, die entsprechend zu ergänzen ist. Die in Art. 9 (3)

enthaltene Delegationsermächtigung wird deshalb abgelehnt.

Zu Art. 10:

Das von der Verordnung hier offenbar verfolgte Regelungsziel wird in Erwägungsgrund 45 deutlich. Dort wird ausführt, dass der für die Verarbeitung Verantwortliche nicht verpflichtet sein sollte, zusätzliche Daten einzuholen, um eine betroffene Person zu bestimmen. Er sollte das Recht haben, bei der betroffenen Person, falls diese von ihrem Auskunftsrecht Gebrauch macht, weitere Informationen einzuholen, um die zu dieser Person gesuchten personenbezogenen Daten zu lokalisieren. Dies spiegelt sich im Wortlaut des Art. 10 jedoch nicht wider. Dieser sollte deshalb so gefasst werden, dass sich der Erwägungsgrund 45 im Regelungstext selbst niederschlägt.

Kapitel III – Rechte der betroffenen Person

Zu Art. 11:

Der Vorschlag wird grundsätzlich begrüßt. Es sollte jedoch in Abs. 1 klargestellt werden, was der für die Verarbeitung Verantwortliche (konkret) leisten muss.

Zu Art. 12:

Aus Gründen der Bestimmtheit und wegen der Erheblichkeit der hier zu treffenden Konkretisierungen sollte unmittelbar in der Verordnung selbst dargelegt werden, unter welchen Voraussetzungen ein Antrag offenkundig unverhältnismäßig ist, insbesondere auch, wann eine missbräuchliche Häufung von Betroffenenrechten vorliegt (vgl. Art. 12 (4)). Die Befugnis der Kommission zu delegierten Rechtsakten in Art. 12 (5) sollte daher entfallen.

Die Konferenz spricht sich gegen eine Missbrauchsgebühr aus. Aus ihrer Sicht reicht es aus, dass in Missbrauchsfällen das jeweilige Betroffenenrecht nicht in Anspruch genommen werden kann. Sofern an der Missbrauchsgebühr festgehalten wird, muss vermieden werden, dass sich Betroffene völlig unerwartet Gebührenforderungen gegenübersehen. Deshalb sollte der für die Verarbeitung Verantwortliche die betroffene Person im konkreten Einzelfall darüber informieren müssen, wenn er die Ausübung der Betroffenenrechte für offenkundig unverhältnismäßig erachtet und aus diesem Grund ein Entgelt verlangen will. Die Höhe des Entgelts muss verhältnismäßig sein und sich an dem tatsächlichen Aufwand bemessen.

Art. 12 sollte um das Erfordernis sicherer Übertragungswege für personenbezogene Daten nach dem Stand der Technik ergänzt werden.

Zu Art. 13:

Die Regelung wird grundsätzlich begrüßt. Die Nachberichtspflicht gemäß Art. 13 sollte sich jedoch auch auf Widersprüche nach Art. 19 erstrecken.

Zu Art. 14:

In der Verordnung ist unter Art. 14 (4) lit. b) klarzustellen, was unter einer „angemessenen“ Frist zu verstehen ist. Ferner ist zu prüfen, ob anstatt dieser nicht ein „unverzügliches Handeln“ geboten ist. Benachrichtigungen erst bei Datenübermittlungen dürfen nur bei Datenverarbeitern möglich sein, die geschäftsmäßig Daten zur Übermittlung vorhalten (u. a. Auskunfteien, Adresshandel, Detekteien).

Zu Art. 15:

In Art. 15 (1) lit. g) sollte die Einschränkung auf die (lediglich) „verfügbaren“ Herkunftsdaten gestrichen werden, da eine Angabe über die Herkunft personenbezogener Daten stets geboten ist und diese nicht verschleiert werden darf.

Die Aufklärungspflicht nach Art. 15 (1) lit. h) sollte auf die „Bedeutung und Tragweite“ der Verarbeitung erstreckt werden. Ein (ausdrücklicher) Hinweis auf besondere Risiken bei der Profilbildung, Auskunfteien oder dem Scoring ist aufzunehmen.

Es muss zudem sichergestellt werden, dass für eine Mitteilung in elektronischer Form gemäß Art. 15 (2) nur sichere Übertragungswege nach dem Stand der Technik in Betracht kommen.

Zu Art. 16:

Es ist klarzustellen, ob unter einem Korrigendum eine Richtigstellung zu verstehen ist. Zudem regelt

die Vorschrift nicht, wie zu verfahren ist, wenn sich die Unrichtigkeit oder Richtigkeit der Daten nicht beweisen lässt, bzw. wer die Beweislast trägt. Dieser Punkt sollte ergänzt werden. Denkbar wäre z.B. eine Verpflichtung, diese Daten im Sinne von Art. 17 (4) zu beschränken.

Zu Art. 17:

In Art. 17 (2) sollte eine Pflicht der Dritten zur Löschung der Daten analog Art. 17 (1) geregelt werden. Insbesondere sollte klargestellt werden, ob die Regelung auf den Bereich des Internets beschränkt ist und ob sie nach Maßgabe des Lindqvist-Urteils auch für Privatpersonen gilt.

Das Verhältnis der „umgehenden" Löschungspflicht in Art. 17 (3) zu der in Art. 12 (2) geregelten Monatsfrist ist klärungsbedürftig. Es erscheint jedenfalls nicht sinnvoll, wenn der für die Verarbeitung Verantwortliche zwar einerseits die personenbezogenen Daten umgehend löschen müsste, andererseits aber für die Benachrichtigung des Betroffenen über die Löschung einen Monat Zeit hätte.

Die Formulierung in Art. 17 (2) „alle vertretbaren Schritte" bedarf insbesondere aus technischer Sicht der Präzisierung.

Die Beschränkung nach Art. 17 (4) sollte verpflichtend vorgegeben werden.

Zu Art. 18:

Die Konferenz unterstützt die Einführung eines Rechts auf Datenportabilität in Art. 18 (1). Dieses Recht sollte aber nicht davon abhängen, ob der für die Verarbeitung Verantwortliche seine Verarbeitungen in einem gängigen Format tätigt. Vielmehr sollte durch die Streichung des Wortes „gängige" eine allgemeine Konvertierungspflicht geregelt werden. Es ist klärungsbedürftig, ob Art. 18 (1) auch den öffentlichen Bereich erfasst.

Die in Art. 18 (2) verwandten Begriffe des Zur-Verfügung-Stellens und des Entziehens von Daten sollten in der Verordnung definiert werden, falls auf diese Begriffe nicht in Gänze verzichtet werden kann.

Zu Art. 19:

In Art. 19 (1) sollte der Begriff „schutzwürdige Gründe" durch „berechtigte Interessen" ersetzt werden. Es sollte zudem geprüft werden, ab wann und wie der Nachweis für das überwiegende Verarbeitungsinteresse des für die Verarbeitung Verantwortlichen als erbracht gelten soll.

Kommerzielle Werbung sollte, wie bereits zu Art. 6 angemerkt, grundsätzlich nur mit Einwilligung des Betroffenen gestattet sein. Art. 19 (2) sollte deshalb entsprechend angepasst werden. Die Konferenz empfiehlt zudem, den Begriff „unentgeltlich" in Art. 19 (2) zu streichen, da sich die Unentgeltlichkeit bereits aus Art. 12 (4) Satz 1 ergibt. Andernfalls wäre im Einzelnen darzulegen, weshalb welche Maßnahmen nach Kapitel III jeweils entgeltfrei sein sollen oder nicht.

Unter Hinweis zu den Anmerkungen zu Art. 13 sollte auch Art. 19 entsprechend angepasst werden.

Zu Art. 20:

Die Konferenz unterstützt grundsätzlich die Aufnahme einer speziellen Regelung zur Profilbildung. Allerdings hält sie den Vorschlag für stark ergänzungsbedürftig.

Schon die Profilbildung selbst (z.B. in sozialen Netzwerken, beim Scoring und bei Auskunfteien) greift in erheblicher Weise in das Grundrecht auf Datenschutz ein und ist deshalb regelungsbedürftig.

Art. 20 (1) sollte zudem auf jede – auch nur teilweise automatisierte – systematische Verarbeitung zur Profilbildung Anwendung finden und daher das Wort „rein" gestrichen werden.

Bei Minderjährigen (Art. 8) sollte die Profilbildung generell verboten sein.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wird wegen ihrer besonderen Sensitivität äußerst kritisch gesehen. Dort, wo sensitive Daten für eine Prognose unerlässlich sind, wie z.B. bei der Risikobeurteilung im Krankenversicherungsbereich, müssen enge, branchenspezifische Ausnahmetatbestände eingeführt werden, die an

dem Grundsatz der Erforderlichkeit auszurichten sind. In Art. 20 (3) ist zudem klarzustellen, ob die Voraussetzungen des Art. 9 kumulativ gelten sollen. Dies würde sicherstellen, dass die Verwendung besonderer Kategorien personenbezogener Daten materiell-rechtlichen Beschränkungen unterliegt und sie nicht beliebig in Profilbildungen einfließen können.

Im Hinblick auf die besonderen Risiken der Bildung von Profilen, die auf einzelne Personen bezogen werden können, ist die Wiederherstellung eines Personenbezugs bei unter Pseudonym oder einem technischen Identifikationsmerkmal geführten Profilen grundsätzlich zu untersagen.

Wegen der Erheblichkeit der in Art. 20 (5) zu treffenden Konkretisierungen und aus Gründen der Bestimmtheit sollte eine entsprechende Reglung in die Verordnung aufgenommen und die Befugnis der Kommission zu delegierten Rechtsakten gestrichen werden.

Zu Art. 21:

Statt einer Öffnungsklausel für den nationalen Gesetzgeber nur zur Beschränkung der Rechte Betroffener (Art. 21) sollten weiter reichende Betroffenenrechte gewährt werden dürfen. Dies gilt ungeachtet der bereits zu Art. 6 geforderten generellen Öffnungsklausel für den öffentlichen Bereich.

Art. 21 (1) lit. c) sollte gestrichen werden. Es ist nicht nachvollziehbar, weshalb die bisher in der RL 95/46/EG nicht vorgesehene Beschränkung in Bezug auf den Schutz sonstiger öffentlicher Interessen geboten sein soll. Zumindest sollten die Anforderungen an die Beschränkung strikter formuliert werden, damit die Betroffenenrechte nicht leerlaufen.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Ein zukunftsfähiger Datenschutz umfasst technische und organisatorische Maßnahmen, die Datenschutz und Datensicherheit angemessen berücksichtigen. Um dies zu gewährleisten, sind die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technische und organisatorische Maßnahmen in die Bestimmungen der Art. 23 ff. aufzunehmen.

Zu Art. 22:

Um sicherzustellen, dass eine Verarbeitung personenbezogener Daten erst dann erfolgt, wenn die geeigneten Strategien und Maßnahmen auch umgesetzt sind, sollte Art. 22 (1) wie folgt formuliert werden: „Der für die Verarbeitung Verantwortliche stellt durch die Umsetzung geeigneter Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann."

Art. 22 (3) sollte dahingehend ergänzt werden, dass die Entscheidung über Konsequenzen aus der Überprüfung der in den Absätzen 1 und 2 genannten Maßnahmen nicht dem Prüfer, sondern weiterhin dem für die Verarbeitung Verantwortlichen obliegt.

Zu Art. 23:

In Art. 23 (1) könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der Implementierungskosten zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden. Zumindest müssen – wie in Art. 30 (1) – die Implementierungskosten technisch-organisatorischer Maßnahmen in ein angemessenes Verhältnis zum konkreten Gefahrenpotential der Datenverarbeitung gesetzt werden, um eine Relation zwischen Kosten und Eingriffstiefe in das Recht auf informationelle Selbstbestimmung herzustellen.

Art. 23 (2) sollte präzisiert und um Kriterien und Anforderungen in Bezug auf die zu treffenden Maßnahmen und Verfahren ergänzt werden. Hierbei sind insbesondere Anonymisierung und Pseudonymisierung nach dem Stand der Technik zu fordern, sofern dies nicht bereits in Art. 5 geregelt wird.

Es sollte klargestellt werden, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft.

Die Grundeinstellungen von Produkten und Diensten sind so zu gestalten, dass so wenig personenbe-

zogene Daten wie möglich erhoben oder verarbeitet werden und bereits ohne Zutun der Nutzer eine datenschutzfreundliche Nutzung sichergestellt wird.

Die Regelung sollte ausdrücklich auch für Verhaltensbeobachtungen („Tracking“) im Internet durch den für die Verarbeitung Verantwortlichen oder durch Dritte gelten.

Satz 2 des Art. 23 (2) sollte wie folgt lauten: „Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nur den von der betroffenen Person zu bestimmenden Personen zugänglich gemacht werden.“ Damit soll erreicht werden, dass die betroffene Person den Personenkreis selbst bestimmt, dem ihre personenbezogenen Daten zugänglich gemacht werden dürfen, und der für die Verarbeitung Verantwortliche hierfür die entsprechenden Vorkehrungen zu treffen hat.

Zu Art. 24:

In Art. 24 sollte im Text ausdrücklich ergänzt werden, dass sich die betroffene Person zur Wahrnehmung ihrer Rechte an jeden der für die gemeinsame Verarbeitung Verantwortlichen wenden kann.

Zu Art. 25:

Die Konferenz schlägt vor, auch in den Fällen des Art. 25 (2) lit. a) einen Vertreter zu bestellen. Art. 25 (2) lit. a) sollte daher gestrichen werden.

Der in Art. 25 (2) lit. b) geplante Verzicht bei Unternehmen mit weniger als 250 Mitarbeitern auf die Benennung eines Vertreters, der umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten sollte, stellt eine Ausnahme dar, die nicht nachvollziehbar ist. Die Konferenz schlägt daher vor, diese Ausnahmeregelung ebenfalls zu streichen. Diese Klausel eröffnet weitgehende Umgehungsmöglichkeiten, da nicht geprüft werden kann, wie viele Beschäftigte bei einem nicht in der Union niedergelassenen Unternehmen tatsächlich tätig sind.

Zu Art. 26:

Der in Art. 26 (2) geregelte Mindestinhalt eines Vertrages oder Rechtsaktes zur Auftragsdatenverarbeitung sollte die wesentlichen Aspekte enthalten und daher um die Angabe von Gegenstand und Dauer des Auftrags sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung, der Art der Daten und den Kreis der Betroffenen ergänzt werden. In lit. a) sollte durch Streichung des 2. Halbsatzes sichergestellt werden, dass der Auftragsverarbeiter in jedem Fall ausschließlich auf Weisung des für die Verarbeitung Verantwortlichen tätig wird und nicht nur in besonderen Fällen, in denen die Übermittlung der Daten nicht zulässig ist.

Der Schutz der betroffenen Person erfordert die Klarstellung, dass sie sich bei gemeinsam für die Verarbeitung Verantwortlichen gemäß Art. 24 sowohl an den für die Verarbeitung Verantwortlichen als auch an den Auftragsverarbeiter wenden kann.

Eine wirksame Kontrolle des Auftragsverarbeiters kann nur umfassend erfolgen, wenn dem für die Verarbeitung Verantwortlichen in Art. 26 (2) auch ein Kontrollrecht, beispielsweise durch einen Treuhänder, eingeräumt wird und den Auftragsverarbeiter entsprechende Mitwirkungspflichten treffen. Dies gilt auch für etwaige Unterauftragsverhältnisse.

Die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragsverarbeiters sind wesentliche Fragen, die letztlich auch die Zulässigkeit der Auftragsdatenverarbeitung insgesamt berühren. Insbesondere wäre etwa die Einführung und nähere Ausgestaltung eines Konzernprivilegs eine wesentliche Frage, die im Sinne von Art. 290 AEUV – soweit in den Absätzen 1 bis 4 nicht ohnehin bereits geschehen – in der Verordnung selbst geregelt werden sollte. Die Konferenz sieht daher die in Art. 26 (5) vorgesehene Ermächtigung zu delegierten Rechtsakten kritisch.

Zu Art. 28:

In Art. 28 sollte geregelt werden, dass die Dokumentation grundsätzlich vor Aufnahme der Verarbeitung personenbezogener Daten zu erstellen ist. Zudem sollte der für die Verarbeitung Verantwortliche verpflichtet werden, die Dokumentation dem Datenschutzbeauftragten (soweit vorhanden) zur Verfügung zu stellen.

Die zeitliche Befristung einer Verarbeitung personenbezogener Daten ist im Sinne des Erforderlichkeitsprinzips ein wesentlicher Grundsatz. Art. 28 (2) lit. g) sollte daher in „eine konkrete Angabe der Fristen für die Löschung der verschiedenen Datenkategorien“ geändert werden.

Zu Art. 30 bis 32 allgemein:

Verfahren mit Personenbezug müssen durch technische und organisatorische Maßnahmen, ausgerichtet an den Datenschutzzielen, geschützt werden. Dieser Grundsatz ist in der Verordnung selbst zu verankern. Die Konferenz verweist in diesem Zusammenhang auf Vorbemerkungen zu Kapitel IV. Im Übrigen sollten Aufzählungen technischer und organisatorischer Maßnahmen durch entsprechende Verweise ersetzt werden.

Zu Art. 30:

Die in Art. 30 (1) geforderten angemessenen technischen und organisatorischen Maßnahmen können nur durch eine vorab und kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet werden. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Art. 30 (1) sollte daher durch die Forderung nach einem Sicherheitskonzept ergänzt werden, welches Teil der Verfahrensdokumentation gemäß Art. 28 (2) lit. h) werden muss.

Wie in Art. 23 (1) sollte auch in Art. 30 (1) die Bezugnahme auf Implementierungskosten gestrichen werden.

Zu Art. 32:

Die in Art. 32 (3) geforderte Verschlüsselung personenbezogener Daten muss dahingehend präzisiert werden, dass sie durch Verfahren nach dem Stand der Technik erfolgen muss.

Zu Art. 33:

Eine Regelung der Datenschutz-Folgenabschätzung (Art. 33), die nachhaltig dem Schutz personenbezogener Daten dienen soll, muss die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit umsetzen, um vollumfänglich Risiken und dafür angemessene Maßnahmen identifizieren zu können. Die Ergebnisse sind in einem regelmäßigen Monitoring zu überprüfen.

Die Begriffe der Datenschutz-Folgenabschätzung und der Vorab-Genehmigung bzw. -Zurateziehung sollten voneinander abgegrenzt werden, da sich diese wechselseitig nicht ersetzen können.

Da jede der in Art. 33 (2) lit. a) genannten Auswertungen bereits erhebliche Risiken mit sich bringt, sollten die Worte „systematische und umfassende“ entfallen.

Die Konferenz schlägt vor, in Art. 33 (2) lit. c) das Wort „weiträumig“ zu streichen, da der Begriff zu unbestimmt ist und aus Sicht der betroffenen Person kein Unterschied besteht, ob die Überwachung weiträumig oder kleinräumig stattfindet.

In Art. 33 (2) lit. d) sollte die Durchführung einer Datenschutz-Folgenabschätzung für die Verarbeitung personenbezogener Daten aus Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten, nicht vom Umfang der Datei abhängen, sondern in jedem Fall erfolgen. Das Wort „umfangreich“ sollte daher gestrichen werden.

Für die Datenschutz-Folgenabschätzung muss auch zwingend in Art. 33 (3) eine Dokumentationspflicht aufgenommen werden.

Schließlich sollte Art. 33 um einen zusätzlichen Absatz ergänzt werden, der das Verbot der Datenverarbeitung bei unangemessen hohen Eingriffen in die Rechte der Betroffenen fordert. Grundsätzlich sollten Verfahren ausgewählt werden, die den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung mit sich bringen.

Zu Art. 34:

Die Konferenz hält den Vorschlag, dass der interne Datenschutzbeauftragte die Beantragung einer vorherigen Genehmigung bzw. Zurateziehung nach Art. 37 (1) lit. f) nur überwachen soll, für nicht ausreichend. Zur Entlastung der Aufsichtsbehörden und zur Stärkung des betrieblichen Datenschutzes

sollte ihm diese Aufgabe komplett übertragen werden können. Deutschland hat mit der Durchführung der Vorabkontrolle durch die internen Datenschutzbeauftragten gute Erfahrungen gemacht.

Zu Art. 35:

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv.

Es sollte eine Frist geregelt werden, innerhalb derer der Datenschutzbeauftragte nach Aufnahme der Daten verarbeitenden Tätigkeit zu bestellen ist. Die Konferenz schlägt hierfür eine Frist von einem Monat vor.

Die Konferenz bedauert, dass in Art. 35 (1) lit. b) eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten vorgesehen ist. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Art. 35 (1) lit. c) sollte dahingehend geändert werden, dass bei jeder risikobehafteten Datenverarbeitung (z.B. Auskunfteien, Detekteien, Callcenter, Lettershops etc.) unabhängig von der Mitarbeiterzahl eine Bestellungspflicht für einen Datenschutzbeauftragten besteht. Das Gleiche gilt für Unternehmen, bei denen eine Datenschutzfolgenabschätzung erforderlich ist. Die Anknüpfung an die „regelmäßige und systematische Beobachtung von betroffenen Personen“ ist insoweit nicht ausreichend.

Durch die in Art. 35 (7) geregelte Möglichkeit der Befristung der Amtszeit des Datenschutzbeauftragten kann die Unabhängigkeit beeinträchtigt werden. Die Amtszeit des internen Datenschutzbeauftragten sollte daher nicht befristet werden und das dem Amt zugrunde liegende Arbeitsverhältnis nur aus wichtigem Grund kündbar sein. Die Amtszeit von externen Datenschutzbeauftragten sollte mindestens vier Jahre betragen.

Art. 35 (11) ist zu streichen. Die Fälle, in denen unabhängig von der Mitarbeiterzahl ein Datenschutzbeauftragter zu bestellen ist, betreffen eine wesentliche Frage und sind deshalb in der Verordnung selbst zu regeln.

Zu Art. 36:

Der Datenschutzbeauftragte sollte nicht nur ein unmittelbares Vorspracherecht gegenüber der Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters haben, sondern dieser – als Ausdruck seiner Unabhängigkeit – unmittelbar unterstellt sein. Außerdem sollte für interne Datenschutzbeauftragte ein wirksamer arbeitsrechtlicher Kündigungsschutz sowie die Aufnahme eines Benachteiligungsverbots vorgesehen werden, um seine Unabhängigkeit besser zu sichern.

In Art. 36 (3) ist das Recht des Datenschutzbeauftragten auf Fort- und Weiterbildung sowie die Kostenübernahme hierfür zu normieren. Zudem sind Regelungen zur Verschwiegenheit des Datenschutzbeauftragten sowie zum Zeugnisverweigerungsrecht aufzunehmen.

Zu Art. 37:

Die Aufgaben des Datenschutzbeauftragten sind in der deutschen Sprachfassung missverständlich formuliert. So wird sprachlich nicht hinreichend deutlich, ob der Datenschutzbeauftragte beispielsweise selbst die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 31 vornehmen muss oder diese Meldung nur zu überwachen hat (Art. 37 (1) lit. e).

In diesem Zusammenhang sollte auch klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten den für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter nicht von seinen Pflichten entbinden bzw., dass keine Möglichkeit zur Exkulpation bei Nicht- oder Schlechterfüllung seitens des Datenschutzbeauftragten besteht.

Zu Art. 38 und Art. 39:

In Art. 39 (2) sollten die wesentlichen Regelungstatbestände einer Zertifizierung und der Vergabe eines

Siegels und Zeichens direkt aufgenommen und nicht an die Kommission delegiert werden. Die Zertifizierungs- und Vergabekriterien sind insbesondere an den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5, der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6, der Betroffenenrechte und an den Datenschutzzielen in Art. 30 nach Maßgabe der Verordnung auszurichten.

Zertifizierungs-, Vergabe- und Widerrufsverfahren müssen den Anforderungen des Grundsatzes der Transparenz hinsichtlich der Kriterien, des Verfahrens und der wesentlichen Evaluierungsergebnisse genügen. Die Unabhängigkeit und Fachkunde der Zertifizierungs- und Vergabestellen und der Evaluatoren sind zu gewährleisten.

Eine datenschutzspezifische Zertifizierung gemäß Art. 39 (1) beinhaltet stets auch eine Bewertung der IT-Sicherheit. Diese sollte sich an europäischen und internationalen Standards orientieren und die Datenschutzziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit aus Betroffenensicht einbeziehen. Ein entsprechender Zusatz – unter Einbeziehung des Ergänzungsvorschlags der Konferenz zu Kapitel IV (elementare Datenschutzziele) – ist daher vorzusehen.

Zertifizierungen sind zeitlich zu befristen. Eine Rücknahme eines Zertifikates bei gravierenden Mängeln muss auch vor Fristablauf möglich sein.

Bei der Ausgestaltung der Verhaltensregeln und Zertifizierungsverfahren ist der Europäische Datenschutzausschuss zu beteiligen.

Kapitel V – Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Zu Art. 41:

Die Kommission sollte bei der Angemessenheitsprüfung nach Art. 41 (2) stets auch die Stellungnahme des Europäischen Datenschutzausschusses einholen und berücksichtigen müssen. Im Zusammenhang mit Art. 41 (6) muss klargestellt werden, dass in den Fällen, in denen die Kommission durch Beschluss feststellt, dass kein angemessenes Datenschutz-Niveau gegeben ist, die Datenübermittlung automatisch verboten ist, so dass es keines weiteren Umsetzungsaktes durch die Aufsichtsbehörde bedarf.

Ferner muss klargestellt werden, ob die Formulierung „unbeschadet der Art. 42 – 44“ bedeutet, dass bei einem Negativ-Beschluss gleichwohl Datenübermittlungen nach allen diesen Vorschriften vorgenommen werden können. Insbesondere die Vorschriften des Art. 41 (6) und des Art. 42 (1) erscheinen in dieser Frage widersprüchlich.

Zu Art. 42:

Da die Genehmigungsfähigkeit der Datenflüsse von vornherein fraglich ist, wenn keine geeigneten Garantien vorliegen, ist der Anwendungsbereich der Regelung des Art. 42 (5) unklar (Auffangtatbestand?). Deshalb sollte der Absatz 5 (bis auf den letzten Satz) entweder gestrichen oder um die genehmigungspflichtigen Fälle präzisiert werden.

Zu Art. 43:

In Art. 43 (1) sollte die Rechtsfolge der Genehmigung der BCR durch die Aufsichtsbehörde explizit aufgenommen werden, z.B. durch folgenden Satz 2: „In diesem Fall gilt die Genehmigung in der gesamten EU.“

Die in Art. 43 (3) genannten Kriterien und Anforderungen an BCR sollten nicht von der Kommission, sondern ausschließlich von dem Europäischen Datenschutzausschuss festgelegt werden.

Zu Art. 44:

Es sollte eine Klausel zum Umgang mit Aufforderungen zur Datenübermittlung durch Gerichte oder Behörden aus Drittstaaten eingefügt werden. Eine (interne) Vorversion des Vorschlags der Kommission beinhaltete eine solche explizite Klausel. Derartige Aufforderungen sollten hiernach grundsätzlich unbeachtlich sein und unter Genehmigungsvorbehalt durch zuständige nationale Behörden stehen. Die Konferenz fordert, dass Datentransfers grundsätzlich nur auf der Basis gegenseitiger Rechtshilfeabkommen (Mutual Legal Assistance Treaties, MLATs) zulässig sind.

In Art. 44 (1) müssen bei sensitiven Daten zusätzlich zur informierten Einwilligung geeignete Garantien vorgesehen werden, weil sonst zwar die Datenübermittlung nach Art. 44 (1) lit. a) legitimiert ist, die Datenverarbeitung im Drittland aber keinen besonderen Anforderungen unterliegt. Das Wort „zugestimmt“ sollte durch „eingewilligt“ (entsprechend Art. 7) ersetzt werden.

Art. 44 (1) lit. d) darf nicht für den Datenaustausch „zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten zuständigen Behörden“ gelten, wie Erwägungsgrund 87 es vorsieht. Dies würde im Widerspruch zum sachlichen Anwendungsbereich der Verordnung nach Art. 2 (2) lit. e) stehen. Deshalb sollten diese Fälle in Erwägungsgrund 87 gestrichen werden.

Der Anwendungsbereich des Art. 44 (1) lit. h) ist unklar. Insbesondere ist fraglich, ob es sich um einen Auffangtatbestand handeln soll. Die Regelung muss konkretisiert werden. In jedem Fall muss eine Abwägung der berechtigten Interessen des für die Verarbeitung Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person vorgesehen werden.

Die Anwendungsbereiche der Art. 44 (3), (4), (6) und (7) sind unklar und müssen konkretisiert werden.

Zu Art. 45:

Art. 45 (2) sollte dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Datenschutz.

Kapitel VI – Unabhängige Aufsichtsbehörden

Zu Art. 47 und 48:

Die Regelung zur völligen Unabhängigkeit der Aufsichtsbehörden in Art. 47 (1) ist grundsätzlich positiv zu werten. Es sollte allerdings überdacht werden, wie die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit den anderen Aufsichtsbehörden, insbesondere im Rahmen des Kohärenzverfahrens, garantiert werden kann (Art. 46 (1) Satz 2).

Zu Art. 51:

Die Regelung des „One-Stop-Shops“ gemäß Art. 51 (2) ist nur praktikabel, wenn sie nicht im Sinne einer ausschließlichen Zuständigkeit, sondern im Sinne einer „Federführung“ der Aufsichtsbehörde des Mitgliedstaates der Hauptniederlassung zu verstehen ist, falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über mehrere Niederlassungen innerhalb der EU verfügt.

Der One-Stop-Shop-Grundsatz sollte dann nicht gelten, wenn es sich um einen Sachverhalt handelt, der im Schwerpunkt die Anwendung nationalen Datenschutzrechts eines Mitgliedstaats im Sinne des Kapitels IX betrifft, so dass es hier bei der allgemeinen Zuständigkeit nach Art. 51 (1) bleiben sollte.

Mangels eines einheitlichen Verwaltungsverfahrens-, -prozess- und -vollstreckungsrechts kann die Aufsichtsbehörde in anderen Mitgliedsstaaten grundsätzlich nicht selbst tätig werden. Derartige hoheitliche Maßnahmen sollten daher nur im Wege der Amtshilfe möglich sein. Diese Klarstellung ist auch im Hinblick auf Art. 55 (1) und (2) sowie Art. 63 notwendig.

Es sollte überprüft werden, ob die sich aus Erwägungsgrund 19 ergebende Einbeziehung rechtlich selbständiger Tochtergesellschaften in die One-Stop-Shop-Regelung tatsächlich erforderlich ist. Diese könnten aufgrund ihrer rechtlich selbständigen Handlungsfähigkeit auch getrennt betrachtet werden. Sofern eine Einbeziehung für erforderlich gehalten wird, sollte dies einschließlich einer Definition des Begriffs Tochtergesellschaft unmittelbar im Verordnungstext und nicht nur in einem Erwägungsgrund geregelt werden.

Zu Art. 52:

Ausgehend von dem Vorschlag, eine Regelung zu „Erziehung und Bildung“ aufzunehmen (s.o.), sollten auch die Aufgaben der Aufsichtsbehörden entsprechend erweitert werden. Die Konferenz schlägt für Art. 52 (2) daher folgenden Wortlaut vor:

„Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien

und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und über geeignete Maßnahmen zum eigenen Schutz. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder."

Die in Art. 52 (6) vorgesehene Missbrauchsgebühr sollte gestrichen werden, da nach den Erfahrungen der deutschen Aufsichtsbehörden derartige Beschwerden äußerst selten vorkommen, so dass – auch im Hinblick auf den Verwaltungsaufwand – eine Erhebung von Gebühren unverhältnismäßig wäre.

Zu Art. 53:

Die Konferenz weist darauf hin, dass auch die EU-rechtlich gebotene Unabhängigkeit der Aufsichtsbehörden nur im Rahmen der jeweiligen verfassungsrechtlichen Staatsstrukturprinzipien bestehen kann (Art. 4 Abs.2 EUV). Dies gilt insbesondere für deren Sanktionsbefugnisse und Sanktionspflichten.

Art. 53 (2) sollte auch den anlasslosen Zugang zu Geschäfts- und Diensträumen umfassen. Unklar ist, was in Art. 53 (3) mit der Formulierung, dass Verstöße gegen die Verordnung den Justizbehörden zur Kenntnis zu bringen sind, gemeint ist.

Zu Art. 54:

Art. 54 sollte gestrichen werden. Hilfsweise wird angeregt, die Aufsichtsbehörden lediglich zur Erstellung eines regelmäßigen Jahresberichts zu verpflichten, der der Öffentlichkeit (und damit automatisch dem nationalen Parlament, der Kommission, dem Europäischem Datenschutzausschuss u.a.) zugänglich gemacht werden muss.

Kapitel VII – Zusammenarbeit und Kohärenz

Zu Art. 55 und Art. 56:

In dem in Art. 55, 56 geregelten Verfahren der Amtshilfe und der Zusammenarbeit sollten die betroffenen Behörden grundsätzlich sowohl im Hinblick auf die rechtliche Bewertung eines Sachverhalts als auch hinsichtlich erforderlicher aufsichtsbehördlicher Maßnahmen einvernehmlich zusammenwirken. Dies gilt insbesondere dann, wenn es sich um eine Maßnahme der federführenden Behörde i.S.d. Art. 51 (2) handelt, die von der Aufsichtsbehörde eines anderen Mitgliedstaates durchzuführen ist. Bei Divergenzen im Hinblick auf die Bewertung eines Sachverhalts oder die Vornahme aufsichtsbehördlicher Maßnahmen sollte der Europäische Datenschutzausschuss von den beteiligten Behörden angerufen werden können.

Die Gründe, aus denen Amtshilfeersuchen nach Art. 55 (4) abgelehnt werden können, sind zu eng. Sie sollten auch zwingende Hinderungsgründe nach nationalem Recht (z.B. im Falle des Sozialgeheimnisses) umfassen.

In Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter zwar über mehrere Niederlassungen innerhalb der EU verfügt, es sich aber um einen rein nationalen Sachverhalt handelt, sollte es aus Gründen der Verfahrensökonomie ebenfalls bei der allgemeine Zuständigkeitsregelung des Art. 51 (1) bleiben. Anderenfalls würde die Abstimmung mit der Hauptniederlassungsbehörde einen unverhältnismäßigen Verfahrensaufwand bedeuten. In diesen Fällen sind die Voraussetzungen der Art. 55, 56 (Betroffenheit von Personen in mehreren Mitgliedstaaten) nicht erfüllt.

Unbestimmt ist, was unter „Vorkehrungen für eine wirksame Zusammenarbeit" in Art. 55 (1) und „praktische Aspekte spezifischer Kooperationsmaßnahmen" in Art. 56 (4) zu verstehen ist. Die verfahrenstechnischen Aspekte der Amtshilfe und der Zusammenarbeit sollten in Art. 55, 56 klar formuliert werden.

Es muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggfs. durch das Sekretariat des Datenschutzausschusses).

Die Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten betreffend „Form und Verfahren der Amtshilfe (...)" in Art. 55 (10) sollte präzisiert und beschränkt werden. Das Verfahren der Amtshilfe sollte in der Verordnung, die Form der Amtshilfe und die Ausgestaltung des elektronischen Informationsaustausches im Sinne einer

Standardisierung hingegen in einem Durchführungsrechtsakt geregelt werden.

Zu Art. 58:

Im Hinblick auf Art. 58 (2) lit. a) sollte klargestellt werden, ob hiervon ausschließlich der Fall des Art. 3 (2) lit. a), b) umfasst ist, oder ob auch Fälle ohne Drittlandbezug dem Kohärenzverfahren unterfallen sollen. Ansonsten würden unübersehbar viele Fälle der Kohärenz unterfallen (z.B. Versandhandel innerhalb der EU).

Zu Art. 59 – Art. 63:

Die Kompetenzen der Kommission im Verhältnis zum unabhängigen Datenschutzausschuss sowie in Bezug auf das Kohärenzverfahren (Art. 59 – 63) sind abzulehnen. Dies gilt insbesondere im Hinblick auf die umfassenden Informationspflichten des Ausschusses gegenüber der Kommission und die Befugnis der Kommission zur Aufforderung der Aussetzung aufsichtsbehördlicher Maßnahmen. Gleiches gilt hinsichtlich der Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten über die „ordnungsgemäße Anwendung“ der Verordnung aus Anlass eines aufsichtsbehördlichen Einzelfalles und von „sofort geltenden Durchführungsrechtsakten“ in Fällen „äußerster Dringlichkeit“. Diese Kompetenzen der Kommission sind mit Art. 8 (3) Grundrechtecharta und 16 (2) Satz 2 AEUV nicht vereinbar, weil die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. Auf der Ebene der Mitgliedstaaten soll die Datenschutzkontrolle völlig unabhängig von jeglichem Einfluss erfolgen. Daher ist es widersprüchlich, wenn für die Kommission mit ihren unterschiedlichsten Aufgaben, auch solchen, die in einem Spannungsverhältnis zum Datenschutz stehen, jene Maßstäbe keine Geltung haben sollen.

Über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, sollte als Folge der Unabhängigkeit der Aufsichtsbehörden – statt der Kommission – ausschließlich der Datenschutzausschuss entscheiden. Im Hinblick auf den personellen, sächlichen und zeitlichen mit dem Kohärenzverfahren verbundenen Aufwand sollte dessen Anwendungsbereich beschränkt werden. Es wird wesentlich im Interesse der Funktionsfähigkeit des Kohärenzverfahrens und eines europaweit wirksamen Datenschutzes darauf ankommen, entsprechende Fallgruppen zu definieren. Nicht alle datenschutzrechtlichen Fragen, die auch in anderen Mitgliedstaaten der EU auftauchen können, bedürfen einer Behandlung im Kohärenzverfahren. Für dieses eignen sich insbesondere:

- Fragen des Drittstaatentransfers
- BCR mit mitgliedstaatenübergreifendem Bezug
- Konstellationen, in denen unterschiedliche Auffassungen zwischen einer nach dem One-Stop-Shop-Prinzip zuständigen Aufsichtsbehörde und einer anderen Aufsichtsbehörde nicht zu einem einvernehmlichen Ergebnis führen
- Fälle von grundsätzlicher Bedeutung für den Datenschutz in der EU, insbesondere bei einer Datenverarbeitung außerhalb der EU, falls alle Mitgliedstaaten betroffen sind und es nicht allein einer unternehmens- oder konzerninternen Verteilung von Verantwortlichkeiten überlassen bleiben kann, die verantwortliche Behörde in Europa festzulegen.

Es sollte darüber hinaus den Aufsichtsbehörden möglich sein, Fragen von sich aus an den Europäischen Datenschutzausschuss heranzutragen. Es ist zu erwägen, ob der Ausschuss in Fällen, in denen eine Aufsichtsbehörde von der Stellungnahme des Ausschusses abzuweichen beabsichtigt, eine verbindliche Stellungnahme annehmen kann, für die ein höheres Abstimmungsquorum als die einfache Mehrheit der Mitglieder zu fordern wäre.

Die Vollstreckbarkeit von Entscheidungen anderer Aufsichtsbehörden nach Art. 63 sollte unter dem Vorbehalt stehen, dass es sich hierbei um rechtmäßige Entscheidungen der nach Art. 51 zuständigen Aufsichtsbehörde handelt, die unter Beachtung der Vorschriften des Kapitel VII (Amtshilfe, Zusammenarbeit, Kohärenz) getroffen wurden.

Zu Art. 64:

Die umfassende Informationspflicht über alle Tätigkeiten des unabhängigen Ausschusses

gegenüber der Kommission nach Art. 64 (4) ist unangemessen.

Zu Art. 66:

Die Streichung der in Art. 30 (1) lit. d) RL 95/46 ausdrücklich enthaltenen Befugnis zur Abgabe von Stellungnahmen zu Verhaltensregeln auf EU-Ebene wird abgelehnt. Der Ausschuss sollte ebenfalls bei der Entwicklung von Zertifizierungsverfahren mitwirken und auch, entsprechend dem jetzigen Art. 30 (1) lit. b) RL 95/46, Stellung nehmen können zum Schutzniveau in der EU und in Drittstaaten.

Es ist abzulehnen, dass die bisherige Kompetenz der Art. 29-Gruppe gemäß Art. 30 (3) RL 95/46, „von sich aus Empfehlungen zu allen Fragen“ abzugeben, „die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen“, nach Art. 66 (1) lit. a) unter der einschränkenden Zweckbestimmung der Beratung der Kommission stehen soll.

Über die in Art. 66 genannten Kompetenzen hinaus sollte dem Ausschuss ein Stellungnahmerecht insbesondere zu Entwürfen der Kommission für delegierte Rechtsakte zukommen. Auf diesem Wege könnten die Expertise und die Kompetenz der Datenschutzbehörden in diesen Bereich eingebracht und gewahrt werden. Zudem würde hierdurch die Transparenz des Delegations- und Komitologieverfahrens erhöht.

Zu Art. 69:

Art. 69 (1) Satz 2 sollte gestrichen werden. Vorsitz- und Stellvertreterposten des Ausschusses sollten ausschließlich durch eine Wahl besetzt werden. Weshalb dem Europäischen Datenschutzbeauftragten zumindest die Funktion eines Stellvertreters zustehen soll, erscheint nicht nachvollziehbar, zumal die Verordnung in der derzeitigen Entwurfsfassung nicht für Organe und Ämter der EU gilt.

Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen

Zu Art. 73 bis Art. 79:

Es ist sicherzustellen, dass durch den neuen Rechtsrahmen auch ein EU-weit wirksamer Rechtsschutz für die Betroffenen gewährleistet wird. Die in Kapitel VIII vorgesehenen Regelungen sind unklar gefasst und erfüllen diese Voraussetzungen nicht.

Länderübergreifende Klagen durch Aufsichtsbehörden im Namen Betroffener nach Art. 74 (4) gegen Aufsichtsbehörden anderer Mitgliedsstaaten können zu gegenseitigen Kontrollen der Aufsichtsbehörden führen, die im Gegensatz zum sonst geregelten Zusammenarbeitsgebot stehen würden. Es wären Klagen möglich, die der eigenen Rechtsauffassung der Aufsichtsbehörden zuwiderliefen.

Kapitel IX – Vorschriften für besondere Datenverarbeitungssituationen

Zu Art. 80 bis Art. 85:

Die Art. 81, 82 und 84 eröffnen den Mitgliedsstaaten die Befugnis, eigene Regelungen „in den Grenzen dieser Verordnung“ zu treffen. Entscheidend ist, dass damit nicht nur Konkretisierungen auf der Ebene des durch die Verordnung geregelten Datenschutzniveaus möglich sind, sondern dass durch nationalstaatliche Regelungen im Interesse des Datenschutzes weitergehende Anforderungen normiert werden können. Es sollte eine ausdrückliche Klarstellung im Verordnungstext in diesem Sinne erfolgen. Eine solche Regelung müsste mit den unter Art. 6 und Art. 21 vorgeschlagenen Öffnungsklauseln für mitgliedsstaatliches Recht abgestimmt werden.

Soweit in den Art. 81 (3) und 82 (3) auf die Möglichkeit für die Kommission verwiesen wird, delegierte Rechtsakte zu erlassen, ist deren Geltung auf die Mitgliedstaaten zu beschränken, die keinen Gebrauch von der Möglichkeit gemacht haben, die betreffenden Sachbereiche selbst zu regeln. Anderenfalls würde sich der Rechtsakt selbst in Widerspruch setzen. Wenn die Mitgliedstaaten die Ermächtigung bekommen, diese Bereiche selbst zu regeln, ist nicht nachvollziehbar, warum der Kommission dennoch

weitreichende Regelungskompetenzen zur Konkretisierung eingeräumt werden sollen. Diese Konkretisierungen sollten dann konsequenterweise unmittelbar von den Mitgliedstaaten selbst vorgenommen werden können.

Gesundheitsdaten dürfen nach Art. 81 (2) unter den gleichen Voraussetzungen zu historischen oder statistischen Zwecken sowie zu wissenschaftlichen Zwecken verarbeitet werden wie sonstige personenbezogene Daten. Gesundheitsdaten sollten aber auch in diesem Zusammenhang stärker geschützt werden.

Anders als die Art. 80 bis 82 sieht der Art. 83 keine Ermächtigung für die Mitgliedsstaaten vor. Die Vorschrift würde also unmittelbar geltendes Recht werden. Die Konferenz erwartet hier – ebenso wie bereits bei Art. 6 (3) ausgeführt – dass das ausdifferenzierte nationale Statistikrecht und dessen vielfach strengere Vorgaben (im Vergleich zum allgemeinen Datenschutzrecht) weiterhin bestehen bleiben können. Dies sollte in Art. 83 klargestellt werden.

In Art. 85 sollte klargestellt werden, dass sich der Vorbehalt zugunsten kirchlicher Regelungen auf die Bereiche beschränkt, die von Art. 17 AEUV erfasst werden (vgl. Erwägungsgrund 128).

Kapitel X – Delegierte Rechtsakte und Durchführungsrechtsakte

Zu Art. 86 und Art. 87:

Im Hinblick auf die Rechtssicherheit sollten die Delegationsermächtigungen nach Art. 86 auf ein Mindestmaß reduziert werden. Nach Auffassung der Konferenz sind, wie bereits ausgeführt, alle wesentlichen materiellen Fragen in der Verordnung selbst bzw. durch Gesetze der Mitgliedstaaten zu regeln.

Hinsichtlich der verbleibenden Delegationsermächtigungen sollte in die Verordnung eine Verpflichtung der Kommission zur Konsultation des Europäischen Datenschutzausschusses vor dem Erlass delegierter Rechtsakte aufgenommen werden.

Anhang: Fehler und Übersetzungsfehler

In Art. 6 (1) lit. c) sollte in der deutschen Übersetzung das Wort „gesetzlichen“ durch das Wort „rechtlichen“ ersetzt werden, um auch – wie bisher in Art. 7 lit. c)) der RL 95/46/EG – untergesetzliche Normen mit einzubeziehen. Der englische Wortlaut („legal obligation“) ist in beiden Vorschriften identisch.

In Art. 26 (1) sollte „...dass die betreffenden technischen und organisatorischen Maßnahmen...“ durch „...dass geeignete technische und organisatorische Maßnahmen...“ ersetzt werden.

In Art. 26 (2) lit. f) sollte „... den Auftragsverarbeiter ...“ durch „... den für die Verarbeitung Verantwortlichen...“ ersetzt werden.

In Art. 30 (3) muss es im letzten Satz anstatt „Art. 4“ „Abs. 4“ heißen.

In den Art. 11 (1), Art. 22 (1), Art 37. (1) lit. b) und Art. 79 (6) lit. e) sollte anstatt „Strategie“ eine zutreffendere Übersetzung für „policy“ gefunden werden.

Abkürzungsverzeichnis

Gesetze und Verordnungen

AEUV	Konsolidierte Fassung des Vertrages über die Arbeitsweise der Europäischen Union
AO	Abgabenordnung
ATDG	Antiterrordateigesetz
AufenthG	Aufenthaltsgesetz
BDSG	Bundesdatenschutzgesetz
BKAG	Bundeskriminalamtgesetz
De-Mail-G	De-Mail-Gesetz
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EGovG	E-Government-Gesetz
G10AG	Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses
GBO	Grundbuchordnung
GG	Grundgesetz
LBG	Landesbeamtengesetz
LDSG	Landesdatenschutzgesetz
LernMFrhAusIV	Landesverordnung über die Lernmittelfreiheit und die entgeltliche Ausleihe von Lernmitteln
LGDIG	Landesgeodateninfrastrukturgesetz
LJVollzDSG	Landesjustizvollzugsdatenschutzgesetz
LKindSchuG	Landeskinderschutzgesetz
LuftVG	Luftverkehrsgesetz
LuftVO	Luftverkehrs-Ordnung

LuftVZO	Luftverkehrs-Zulassungs-Ordnung
LVerfSchG	Landesverfassungsschutzgesetz
MeldDÜVO	Meldedaten-Übermittlungsverordnung
MG	Meldegesetz
MiStra	Anordnungen über Mitteilungen in Strafsachen
OWiG	Ordnungswidrigkeitengesetz
POG	Polizei- und Ordnungsbehördengesetz
SchulG	Schulgesetz
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB VIII	Sozialgesetzbuch – Achtes Buch –
SGB X	Sozialgesetzbuch – Zehntes Buch –
StDAV	Steuerdatenabrufverordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
Übergreifende Schulordnung	Schulordnung für die öffentlichen Realschulen plus, Integrierten Gesamtschulen, Gymnasien, Kollegs und Abendgymnasien
UN-Zivilpakt	Internationaler Pakt über bürgerliche und politische Rechte
VwVfG	Verwaltungsverfahrensgesetz

sonstige Abkürzungen

Abs.	Absatz
AEO	Authorised Economic Operator (Zugelassener Wirtschaftsbeteiligter)
AöR	Anstalt des öffentlichen Rechts
App	Application
Art.	Artikel
BCR	Binding Corporate Rules
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BR-Drs.	Bundesratsdrucksache
BT-Drs.	Bundestagsdrucksache
BVerfGE	Entscheidungen de Bundesverfasungsgerichts
DEHOGA	Deutscher Hotel- und Gaststättenverband
DuD	Zeitschrift Datenschutz und Datensicherheit
GCHQ	Government Communications Headquarters
GPS	Global Positioning System
GVBl.	Gesetz- und Verordnungsblatt
HbbTV	Hybrid Broadcasting Broadband TV
HD	High Definition
i.S.	im Sinne
i.V.m.	in Verbindung mit
JIM-Studie	Jugend, Information, (Multi-)Media; Basisuntersuchung zum Medienumgang 12- bis 19-jähriger in Deutschland

KMK	Kultusministerkonferenz
LfDI	Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
LT-Drs.	Landtagsdrucksache
MdB	Mitglied des Deutschen Bundestages
MinBl.	Ministerialblatt
MittRA	Mitteilung des Rechtsausschusses des Europäischen Parlaments an die Mitglieder
MMS	Multimedia Messaging Service
NFC	Near Field Communication
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
PGP	Pretty Good Privacy
QR	Quick Response
RFID	Radio Frequency Identification
RL	Richtlinie
Rz.	Randzeichen
SD	Secure Digital
SIM	Subscriber Identity Module
SMS	Short Message Service
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SZ	Süddeutsche Zeitung
Tb.	Tätigkeitsbericht
TKÜ	Telekommunikationsüberwachung
Tz.	Textziffer

VPN	Virtual Private Network
WLAN	Wireless Local Area Network
ZD	Zeitschrift für Datenschutz