Datenschutzbericht

2008/2009

Der Landesbeauftragte
für den Datenschutz Rheinland-Pfalz

Zweiundzwanzigster
Tätigkeitsbericht nach § 29 Abs. 2
Landesdatenschutzgesetz (LDSG)
für die Zeit vom 1. Oktober 2007
bis 30. September 2009
LT-Drs. 15/4300

HERAUSGEBER
Der Landesbeauftragte
für den Datenschutz 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

5. März 2010

Datenschutzbericht

2008/2009

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 LfD unter folgender URL abrufbar: http://www.datenschutz.rlp.de/de/ds.php?submenu=grem

Einführung

1. Der Datenschutz ist wieder in aller Munde. Dafür haben eine Vielzahl von Datenschutzskandalen gesorgt und mehrere Entscheidungen des Bundesverfassungsgerichts, mit denen Gesetze des Bundes und einzelner Länder in Teilen als verfassungswidrig verworfen wurden, weil sie dem Datenschutz nicht Rechnung getragen haben.

Trotzdem ist der Datenschutz nicht in jedermanns Bewusstsein. Das gilt für den Staat und die Wirtschaft, aber vor allem auch für die Bürger[1]. Für eine kleine Aufmerksamkeit, für drei Prozent Rabatt oder für eine minimale Gewinnchance sind viele bereit, private Daten von sich preiszugeben. In sozialen Netzwerken, beim Einsatz von Kundenkarten oder im Rahmen von Preisausschreiben. Das Datenschutzbewusstsein ist nicht besonders ausgeprägt. Im Gegenteil: Einschlägigen Studien zu Folge hat die Bundesrepublik Deutschland ihre Spitzenposition in Sachen Datenschutz längst eingebüßt. Die Defizite sind groß und werden im Zuge der technologischen Entwicklung immer größer. Das kann nicht einfach achselzuckend hingenommen werden. Denn der Datenschutz ist Teil der Menschenwürde und gehört zu den Grundlagen unserer freiheitlichen Ordnung.

In diesem Datenschutzbericht soll die Entwicklung, die der Datenschutz in den vergangenen beiden Jahren vor allem in Rheinland-Pfalz genommen hat, nachvollzogen und die Tätigkeit des LfD und seiner Mitarbeiter dargestellt werden. Der Bericht unterscheidet sich in Darstellung, Aufbau und Inhalt von seinen 21 Vorgängern. Das hängt zum einen damit zusammen, dass er erstmals auch den Datenschutz im nicht-öffentlichen Bereich einbezieht und ist zum Anderen dem Versuch geschuldet, nicht die gesamte Arbeit des LfD zu dokumentieren, sondern nur bestimmte Tätigkeitsschwerpunkte. Diese Konzentration hat auch zur Folge, dass der Bericht kürzer ausgefallen ist als die Tätigkeitsberichte der letzten Jahre.

Die Erweiterung der Zuständigkeit des LfD um den nicht-öffentlichen Datenschutz und die Umgestaltung des Tätigkeitsberichtes haben dazu geführt, dass er gute zwei Monate später vorgelegt wird als dies in der Vergangenheit der Fall war. Allerdings hat dies den Vorteil, dass der Bericht nicht nur die Zeit vom 1. Oktober 2007 bis zum 30. September 2009 betrifft, sondern auch den Rest des Jahres 2009 mit einschließt, jedenfalls was die wichtigsten Vorkommnisse und Entwicklungen anbelangt. Insoweit ist er besonders aktuell.

2. Auch in den letzten beiden Jahren ist der LfD auf vielfältige Weise unterstützt worden: durch die Abgeordneten des Landtags, namentlich durch die Mitglieder der Datenschutzkommission, durch die Landesregierung und durch eine Vielzahl nachgeordneter Behörden, nicht zuletzt auch durch die Aufsichts- und Dienstleistungsdirektion Trier, die bis September 2008 für den Datenschutz im nicht-öffentlichen Bereich zuständig war. Ihnen allen ist zu danken, ebenso den Vertretern der öffentlichen und privaten Stellen,

[1] Im Sinne einer besseren Lesbarkeit werden Begriffe wie Bürger, Betroffener, Beschwerdeführer etc. geschlechtsneutral verwendet, wenngleich immer beide Geschlechter gemeint sind.

die Interesse an der Arbeit des LfD gezeigt und seine Tätigkeit gefördert haben.

Danken möchte ich auch meinen Mitarbeitern für ihren engagierten Einsatz, für ihre Anregungen und ihre Unterstützung. Ihre Belastung ist groß, nicht nur wegen der neuen Zuständigkeiten, sondern auch wegen der erheblichen Zunahme der Eingaben. Diese lassen sich z.T. nicht mehr zeitnah bearbeiten. Sie bewirken im Übrigen, dass auch die Prüfungen vor Ort nur noch eingeschränkt durchgeführt werden können. Wenn allseits in Sachen Datenschutz von einem Vollzugsdefizit die Rede ist, dann ist dies sicherlich auch auf ein Kontrolldefizit zurückzuführen. Ohne Personalverstärkung wird sich dies auf absehbare Zeit nicht abbauen lassen.

Edgar Wagner

Übersicht über die Prüfungsergebnisse

1. Landtag und Landesregierung haben mit den im Berichtszeitraum verabschiedeten Landesgesetzen dem Datenschutz weitgehend Rechnung getragen. Das gilt vor allem für das Kinderschutzgesetz, das vom Verfassungsgericht als datenschutzgerecht bewertet wurde. Mit der Novellierung des Landesdatenschutzgesetzes, die dem LfD auch die Funktion einer Aufsichtsbehörde im nicht-staatlichen Bereich übertragen hat, wurde der Datenschutz gestärkt. Es sind aber weitere Änderungen des Landesdatenschutzgesetzes notwendig, um den Datenschutz an die Entwicklung der modernen Informations- und Kommunikationstechnologien anzupassen (S. 23).

2. Die Landesregierung hat sich im Bundesrat für eine Verbesserung des Datenschutzes auf Bundesebene eingesetzt und zwar vor allem im Zusammenhang mit der jüngsten Novellierung des Bundesdatenschutzgesetzes und mit Blick auf die Einführung eines Arbeitnehmerdatenschutzgesetzes. Ihre kritische Haltung gegenüber Google Street View ist in datenschutzrechtlicher Hinsicht hilfreich (S. 43). Andererseits hat die Landesregierung im Bundesrat dem ELENA-Verfahrensgesetz zugestimmt, das in datenschutzrechtlicher Hinsicht kritisch zu bewerten ist. Entsprechendes gilt für die Vorratsdatenspeicherung, die zurzeit vom Bundesverfassungsgericht überprüft wird, aber von der Landesregierung ebenfalls unterstützt worden ist.

3. Die Landesverwaltung ist seit vielen Jahren dem Datenschutz gegenüber aufgeschlossen. Das war auch im Berichtszeitraum der Fall. Die behördlichen Datenschutzbeauftragten haben daran einen wichtigen Anteil. Anders als im nicht-öffentlichen Bereich sind sie in der Regel überall dort eingesetzt, wo das Landesdatenschutzgesetz dies verlangt. Trotzdem gibt es innerhalb der Landesverwaltung noch genügend Sachgebiete, in denen der Datenschutz verbessert werden kann.

4. Bei der Umsetzung des Landeskinderschutzgesetzes gibt es in datenschutzrechtlicher Hinsicht immer noch Defizite (S. 72).

5. Die POLIS-Abfragen durch rheinland-pfälzische Polizeistellen sind effektiver zu kontrollieren (S. 70).

6. Der Umgang der Finanzverwaltung mit dem Auskunftsrecht der Steuerpflichtigen ist zu kritisieren (S. 91).

7. Die anerkennenswerten Bemühungen des Bildungsministeriums, dem Datenschutz im schulischen Unterricht den notwendigen Platz einzuräumen, müssen verstärkt werden (S. 28). Überhaupt haben die Bildungseinrichtungen im Lande die notwendigen Schlussfolgerungen daraus zu ziehen, dass der Datenschutz nicht nur eine Angelegenheit von Recht und Technik ist, sondern auch eine Aufgabe von Erziehung und Bildung.

8. Der auch im öffentlichen Bereich um sich greifenden Videoüberwachung müssen stärker als bisher Grenzen gezogen werden (S. 31). Dies gilt vor allem im Schulbereich (S. 77).

9. In Teilbereichen der Landesverwaltung wird Google Analytics eingesetzt. Solange Google die Konfiguration dieses Dienstes nicht ändert, sollte seine Nutzung durch öffentliche Stellen unterbunden werden (S. 43).

10. Die systematische Verwendung und Auswertung von Internetprofilen in Bewerbungsverfahren öffentlicher Arbeitgeber hat zu unterbleiben (S. 61).

11. Die Ausübung von Telearbeit ist in datenschutzrechtlicher Hinsicht unzulässig, wenn von den Heimarbeitsplätzen aus der Zugriff auf bundes- bzw. landesweite Datenbestände möglich ist (S. 62).

12. Die Qualität des Datenschutzes in den Kommunen hängt wesentlich von den dortigen behördlichen Datenschutzbeauftragten ab, von ihrem Fachwissen und der Zeit, die ihnen für den Datenschutz zur Verfügung steht. Vor allem in den großen Städten des Landes wird auf beides Wert gelegt. Es gibt aber auch Kommunen, in denen die Verwaltungen mehr als bisher dafür sorgen müssen, dass die Stellung ihrer Datenschutzbeauftragten der Bedeutung ihrer Aufgabe entsprechend verbessert wird.

13. Die Videoüberwachung von öffentlichen Plätzen ist nur ausnahmsweise zulässig. Wenn sie der Bekämpfung von Kriminalitätsschwerpunkten dient, ist sie nicht Sache der Kommunen, sondern Aufgabe der Polizei. Den Versuchen, diese Einschränkungen zu ignorieren, wird der LfD auch weiterhin entgegengetreten.

14. Die IT-Sicherheit in der Landesverwaltung wurde durch die Einrichtung einer entsprechenden Informationsplattform verbessert. Die kontinuierliche Weiterentwicklung dieser Plattform ist notwendig (S. 96).

15. Der Datenschutz im nicht-staatlichen Bereich weist gravierende Defizite auf. Auch in Rheinland-Pfalz, auch nach der Aufgabenübertragung an den LfD. Es fehlen wichtige Gesetze, etwa ein Arbeitnehmerdatenschutzgesetz. Viele Gesetze werden nicht vollzogen, etwa im Telemedienbereich. Wegen begrenzter Kapazitäten ist außerdem die Datenschutzkontrolle auf stichprobenhafte Untersuchungen begrenzt. Vollzugs- und Kontrolldefizite sind gravierend und bedingen einander (S. 48).

16. Dass vor allem in der mittelständischen Wirtschaft – es ist von 200.000 privaten geschäftsmäßig tätigen Datenverarbeitern in Rheinland-Pfalz die Rede – nicht nur in Einzelfällen keine betrieblichen Datenschutzbeauftragten eingesetzt werden, ist Ausdruck eines mangelhaften Datenschutzbewusstseins.

17. Dieses mangelhafte Datenschutzbewusstsein schlägt sich auch im unzureichenden Schutz von Unternehmensdatenbanken nieder. Dies gilt vor allem dann, wenn Aufgaben der Kundenbetreuung und

-akquise ausgelagert werden, etwa in Callcenter und diese ohne hinreichende Absicherung Zugang zu unternehmenseigenen Kundendaten erhalten. Diese Auftragsdatenverarbeitung ist die offene Flanke des Datenschutzes, auch in der rheinland-pfälzischen Privatwirtschaft (S. 49).

18. Die Überprüfung der in Rheinland-Pfalz ansässigen Versandapotheken offenbarte erhebliche Sicherheitsdefizite bei den Online-Zugängen. Dies ist deshalb problematisch, weil jeder 10. der 40 Millionen Internetnutzer in Deutschland im Berichtszeitraum mindestens einmal eine Online-Apotheke besucht hat (S. 97).

19. Die Überprüfung aller rheinland-pfälzischen Wohnbaugesellschaften ergab, dass mehr als die Hälfte dieser Gesellschaften Bonitätsauskünfte über mögliche Mieter einholt, ohne dabei die einschlägigen gesetzlichen Bestimmungen zu beachten (S. 58).

20. Nicht nur die großen sozialen Netzwerke wie schülerVZ, facebook und wer-kennt-wen bereiten in datenschutzrechtlicher Hinsicht Probleme. Entsprechendes gilt auch für die in Rheinland-Pfalz betriebenen Netzwerke. Minderjährige werden nicht ausreichend geschützt und die Mitgliedsdaten nicht hinreichend gesichert.

21. Im nicht-staatlichen Bereich breitet sich die Videoüberwachung in allen Lebensbereichen rasant aus. Nicht nur Tankstellen, Supermärkte und Einkaufspassagen werden videoüberwacht, auch in Gaststätten, Cafés, Eisdielen, Arztpraxen, Friseursalons und in Freizeiteinrichtungen finden sich solche Anlagen. Dies geschieht ohne Rücksicht auf die Gesetzeslage und weitgehend kontrollfrei (S. 31).

22. Private Arbeitgeber schenken dem Schutz von Beschäftigtendaten nicht immer die gebotene Aufmerksamkeit. Die präventive Korruptionsbekämpfung erfolgt oft am Rande des gesetzlich Zulässigen und die Videoüberwachung sogar oft in unzulässiger Weise. Selbst Ortungssysteme werden datenschutzrechtswidrig eingesetzt, um vor allem Außendienstmitarbeiter zu überwachen (S. 63).

23. Auch die rund 32.000 Vereine im Lande haben den gesetzlich vorgeschriebenen Datenschutz zu gewährleisten. Stichproben zeigen, dass sie dies nur eingeschränkt tun. Vor allem die jeweiligen Internetangebote sind in datenschutzrechtlicher Hinsicht verbesserungsbedürftig (S. 51).

24. Das Datenschutzbewusstsein der Rheinland-Pfälzer dürfte sich nicht wesentlich von dem anderer Landsmannschaften unterscheiden. Es ist nicht besonders ausgeprägt. Das gilt für junge, aber auch für ältere Menschen. Es gibt aber auch ermutigende Anzeichen einer Besserung. Ausdruck dafür ist die ernorm wachsende Zahl der Eingaben beim LfD und erste Verhaltensänderungen in den sozialen Netzwerken (S. 48).

25. Wesentlichen Anteil an dieser positiven Entwicklung haben die Medien, die im bisher nicht gekannten Umfange über Datenschutzskandale, Datenschutzpannen und Datenschutzprobleme berichten. Diese durchaus aufklärende und informative Berichterstattung war eine der erfreulichsten Entwicklungen im Bereich des Datenschutzes während des Berichtszeitraums.

1. Stellenwert des Datenschutzes

Es hat sich einiges getan in Sachen Datenschutz. Eine Reihe von Datenschutzskandalen und einige einschlägige Entscheidungen des Bundesverfassungsgerichts haben den Datenschutz in den Mittelpunkt der öffentlichen Aufmerksamkeit gerückt. Die informationelle Freigiebigkeit vieler Bürger kam hinzu. Für etwas Beachtung in wer-kennt-wen, für drei Prozent Rabatt bei Payback oder für eine kleine Gewinnchance bei einem Preisausschreiben geben sie Daten und Informationen von sich preis, die sie unter vier Augen kaum ihren Freunden oder Nachbarn anvertrauen würden. Manche prophezeien bereits das „Ende der Privatheit". Das mag übertrieben sein. Aber es beschreibt das Problem.

Wie wichtig ist uns unser Recht auf informationelle Privatheit? Wie ernst nehmen wir den Datenschutz? Es wird Zeit, dass wir uns darüber klar werden. Denn im digitalen Zeitalter werden alle unsere Aktivitäten im World Wide Web gespeichert: wonach ich bei Google suche, was ich bei Amazon kaufe und was ich meinen Freunden maile. RFID wird über kurz oder lang unser Konsumverhalten und unseren Alltag erforschen und speichern: wann ich nachts meinen Kühlschrank öffne und wie lange mein Fernseher eingeschaltet ist. Wir hinterlassen endlose Datenspuren. Wer will, kann sie lesen. Nicht nur heute, auch noch in Jahrzehnten. Das Internet vergisst nichts, und auch das Internet der Dinge wird ein ewiges Gedächtnis haben. Wie sehr verändert diese Entwicklung unser Denken und Handeln, unsere Kommunikation und unser Zusammenleben mit anderen?

Längst geht es nicht mehr nur darum, wer welche Daten von uns unter welchen Bedingungen erhalten darf. Die Frage ist vielmehr, in welche Gesellschaft und in welchen Staat uns die Entwicklung der Informations- und Kommunikationstechnologien führt und wie sie unser Denken und unser Bewusstsein verändert. Wir müssen uns darüber verständigen, wie wir leben wollen, was wir als Zumutung begreifen und wie wir im grenzenlosen World Wide Web ein menschliches Maß wahren und in den virtuellen Datengebirgen die Orientierung behalten können. Beim Datenschutz werden die Weichen gestellt. Er bestimmt die Richtung, in die es gehen wird.

Es hat den Anschein, als entwickle sich in Staat und Gesellschaft dafür ein Gespür. Die Medien berichten und klären auf, über Datenskandale und Datenpannen und über irrationales Verhalten im Netz. Auf dem Buchmarkt finden sich kluge und hellsichtige Beschreibungen über die „Digitale Verdummung", über „Den Zauber des Privaten", über die „Generation Internet" und darüber, „wie wir die Kontrolle über unser Denken zurückgewinnen können". Im Bundestag und im Landtag werden Enquete-Kommissionen eingesetzt, in denen mit Hilfe von Sachverständigen nach den richtigen Strategien – auch in datenschutzrechtlicher Hinsicht – gesucht wird. Das Bundesverfassungsgericht erfindet ein neues Datenschutzgrundrecht, um wenigstens von Verfassungs wegen eine Richtung vorzugeben. Die Interessen formieren sich. Dem Datenschutzgipfel folgt der IT-Gipfel. Während in der Politik die Rufe nach gesetzlichen Regelungen lauter werden, halten sich viele Wirtschaftsvertreter die Ohren zu.

Wir leben in einer Zeit des Umbruchs. Manche sprechen sogar von einer digitalen Revolution. Die Bedeutung des Datenschutzes wird dies weiter befördern. Der Koalitionsvertrag der die neue Bundesregierung tragenden Parteien macht dies deutlich. Noch nie war in einem Regierungsprogramm so viel vom Datenschutz zu lesen, wie in diesem.

So gesehen hat der Datenschutz in den letzten Jahren durchaus einen neuen, höheren Stellenwert erhalten. Dieser Stellenwert gründet sich zwar eher auf Fragen als auf Antworten und geht deshalb auch noch nicht mit einer Verbesserung des Datenschutzniveaus einher. Aber wir sind auf dem Weg dahin. Im Bund und auch in Rheinland-Pfalz.

Das Land gehörte in den 1970er Jahren zu den Vorreitern des Datenschutzes. Die datenschutzrechtlichen Debatten im Landtag, die Datenschutzaktivitäten der Landesregierung und das offenkundige Interesse der Justiz am Datenschutz zeigen, dass wir wieder auf einem guten Weg sind. Der Bericht enthält eine Reihe von Anregungen, die auf diesem Weg berücksichtigt werden sollten.

2. Entwicklung des Datenschutzrechts

2.1 Europarecht

2.1.1 Das „SWIFT“-Abkommen

Bereits im letzten Tätigkeitsbericht wurden das SWIFT-Verfahren, der Zugriff der US-Behörden auf diese Zahlungsdaten und die erheblichen datenschutzrechtlichen Bedenken ausführlich dargestellt (21. Tb., Tz. 2.7 und Tz. 22.3).

Das bislang in den USA befindliche Rechenzentrum wurde von SWIFT mittlerweile nach Europa verlagert. Dennoch verlangen die US-Behörden weiter Zugriff auf die dort verarbeiteten Daten mit dem Ziel der Terrorismusbekämpfung. Daher haben die USA mit der Europäischen Union im Berichtszeitraum über ein Abkommen verhandelt, das ihnen weiterhin Zugang zu den 15 Millionen dort täglich verarbeiteten Zahlungsnachrichten verschafft. Im September hat das Europäische Parlament in einer Entschließung seine Bedenken und Anforderungen an ein solches Abkommen zum Ausdruck gebracht (Entschließung des Europäischen Parlaments vom 17. September 2009).

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009-0016+0+DOC+XML+V0//DE).

Auch die Datenschutzbeauftragten des Bundes und der Länder haben ihre Kritik erneuert. Die entsprechende Entschließung kann unter http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=078_finusa abgerufen werden.

Dennoch wurde das Abkommen Ende November vom Rat der Europäischen Justiz- und Innenminister gebilligt (Beschluss des Rates über die Unterzeichnung vom 27. November 2009, Nr. 16110/09, http://register.consilium.europa.eu/). Damit hat sich der EU-Ministerrat über die Bedenken des Europäischen Parlaments und der Datenschutzbeauftragten hinweggesetzt. Deutschland hat sich zwar enthalten, doch hätte nur eine Gegenstimme den Beschluss aufhalten können. Bei Redaktionsschluss war offen, ob das Europäische Parlament seine erforderliche Zustimmung verweigern wird.

Besonders kritisch ist bei dem Abkommen zu sehen, dass damit die Übermittlung einer Vielzahl von Daten über Zahlungsvorgänge mit kaum vorhandenem Bezug zum Terrorismus in die USA legitimiert wird. Es steht zu befürchten, dass die Daten auch dann für mehrere Jahre gespeichert bleiben, wenn sich nach der Übermittlung keine ergänzenden und weiterführenden Anhaltspunkte für einen Terrorismusbezug ergeben. Datenschutzrechtliche Kontrolle oder gerichtliche Überprüfungen sind für die Betroffenen nicht möglich.

2.1.2 Klage gegen die Bundesrepublik Deutschland

Mit ihrer seit 2007 anhängigen Klage vor dem Europäischen Gerichtshof verfolgt die Kommission der Europäischen Gemeinschaft das Ziel, die Verletzung der europäischen Datenschutzrichtlinie 45/46/EG durch die Bundesrepublik Deutschland festzustellen. In Artikel 28 dieser EG-Richtlinie ist festgehalten, dass die Kontrollstellen der Mitgliedsstaaten (also die Datenschutzbehörden) die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen (Artikel 28 Abs. 1 Satz 2 EG-Richtlinie). Diese Verpflichtung der Mitgliedsstaaten sieht die Kommission dadurch verletzt, dass in Deutschland die Datenschutzbehörden nach Landesrecht der staatlichen Aufsicht unterstellt sind, soweit sie nicht-öffentliche Stellen überwachen. Dieses Verfahren ist auch für den LfD Rheinland-Pfalz von Bedeutung, da er als Aufsichtsbehörde über nicht-öffentliche Stellen der Rechtsaufsicht der Landesregierung unterliegt (§ 24 Abs. 1 Satz 2 2. Halbsatz LDSG).

Der Europäische Gerichtshof hat noch nicht entschieden, was unter „völliger Unabhängigkeit“ der Datenschutzbehörden zu verstehen ist und ob die Eingliederung der Aufsichtsbehörden in eine Rechts- oder sogar Fachaufsicht der Exekutive gegen diese Unabhängigkeit verstößt. Am 12. November 2009 legte allerdings der Generalanwalt in der anhängigen Rechtssache C-518/07 seinen Schlussantrag vor, mit dem er einer Verurteilung der Bundesrepublik entgegentritt. Es lägen bislang keine Anzeichen dafür vor, dass staatliche Aufsichtsmaßnahmen gegenüber den Datenschutzbehörden negative Auswirkungen auf ihre Unabhängigkeit gehabt hätten; insoweit habe die Kommission jedenfalls ihrer Beweislast nicht genügt.

Die Entscheidung des Gerichtshofs wird noch im Frühjahr 2010 erwartet.

2.1.3 Terrorlisten

Personen, die auf EU-Terrorverdächtigenlisten erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen. Die Listen sind öffentlich; es handelt sich dabei um eine verschärfte Form eines modernen Prangers.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Jahr 2006 eine Entschließung zum Problem dieser Listen verabschiedet (71. Konferenz vom 16./17. März 2006; s.a. 21. Tb., Tz. 5.14.2).

Mit Urteil vom 3. September 2009 hat der Europäische Gerichtshof (Az. C-402/05 P und C-415/05) entschieden, dass die Gemeinschaftsgerichte für die Prüfung der von der Gemeinschaft erlassenen Maßnahmen, mit denen Resolutionen des Sicherheitsrats der Vereinten Nationen umgesetzt werden, zuständig sind. In Wahrnehmung dieser Zuständigkeit hat er festgestellt, dass die Verordnung Nr. 881/2002/EG des Rates vom 27. Mai 2002 über die Anwendung bestimmter spezifischer restriktiver Maßnahmen gegen bestimmte Personen und Organisationen, die mit Osama bin Laden, dem Al-Qaida-Netzwerk und den Taliban in Verbindung stehen, und zur Aufhebung der Verordnung Nr. 467/2001/EG – Amtsblatt L 139, S. 9, die Grundrechte der Betroffenen verletzt.

Der Gerichtshof gelangte zu dem Schluss, dass angesichts der konkreten Umstände, unter denen die Namen der Rechtsmittelführer in die Liste der vom Einfrieren von Geldern betroffenen Personen und Organisationen aufgenommen worden sind, ihre Verteidigungsrechte, insbesondere der Anspruch auf rechtliches Gehör, sowie das Recht auf effektive gerichtliche Kontrolle offenkundig nicht gewahrt worden sind. Die Verordnung sehe kein Verfahren für die Mitteilung der Umstände, die die Aufnahme der Namen der Betroffenen in die Liste rechtfertigen, gleichzeitig mit der Aufnahme oder im Anschluss daran vor. Der Rat habe die Betroffenen zu keinem Zeitpunkt die ihnen zur Last gelegten Umstände mitgeteilt, die die erstmalige Aufnahme ihrer Namen in die Liste gerechtfertigt haben sollen. Diese Verletzung der Verteidigungsrechte führe außerdem zu einem Verstoß gegen das Recht auf gerichtlichen Rechtsschutz, da sie ihre Rechte auch vor dem Gemeinschaftsrichter nicht zufrieden stellend verteidigen konnten (siehe Pressemitteilung des Europäischen Gerichtshofs Nr. 60/08 vom 3. September 2008).

Mit diesem Urteil ist der Gerichtshof den Bedenken gefolgt, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erhoben worden sind.

2.2 Bundesrecht

2.2.1 Das neue „IT-Grundrecht“

Mit Urteil vom 27. Februar 2008 (Az. 1 BvR 370/07, 1 BvR 595/07) hat das Bundesverfassungsgericht in einem Verfassungsbeschwerdeverfahren gegen das Verfassungssschutzgesetz Nordrhein-Westfalen die Vorschriften zur Online-Durchsuchung sowie zur Aufklärung des Internet für verfassungswidrig und nichtig erklärt (s.a. Tz. 2.2.5, Tz. 6.2.2, Tz. 7.3, Tz. 13.3). Die „Online-Durchsuchung“ verletze das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sei nichtig.

Den wesentlichen Inhalt dieses Grundrechts beschreibt das Bundesverfassungsgericht wie folgt:

„Die Nutzung informationstechnischer Systeme ist für die Persönlichkeitsentfaltung vieler Bürger von zentraler Bedeutung, begründet gleichzeitig aber auch neuartige Gefährdungen der Persönlichkeit. Eine Überwachung der Nutzung solcher Systeme und eine Auswertung der auf den Speichermedien befindlichen Daten können weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen. Hieraus folgt ein grundrechtlich erhebliches Schutzbedürfnis. Das allgemeine Persönlichkeitsrecht trägt dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Grundrecht ist anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. Angesichts der Schwere des Eingriffs ist die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allge-

meinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann allerdings schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Weiter muss eine Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme mit geeigneten gesetzlichen Vorkehrungen verbunden werden, um die Interessen des Betroffenen verfahrensrechtlich abzusichern. Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen."

Die Bedeutung und Reichweite des „neuen Grundrechts" ist allerdings noch nicht in allen Facetten klar. Die Diskussion hierüber wird auf vielen Ebenen geführt. Daran beteiligen sich auch die Datenschutzbeauftragten des Bundes und der Länder. Die Kontroversen beginnen schon bei der Frage, ob es sich wirklich um ein neues Grundrecht oder nur um eine Ausprägung des allgemeinen Persönlichkeitsrechts handelt und wie man dieses Grundrecht benennen solle: kurz als „IT-Grundrecht" oder besser in seiner Langform, die allerdings den Nachteil einer gewissen schwer merkbaren Komplexität hat.

Es ist hier nicht der Ort, alle Zweifelsfragen zu erörtern. Aus der Sicht des LfD bleibt festzuhalten, dass das Verfassungsgericht mit seiner verbindlichen Grundrechtsinterpretation die Rechte der Betroffenen im Internet-Zeitalter erheblich gestärkt und heimliche staatliche Eingriffe in die Internet-Nutzung nur bei Beachtung relativ enger Schranken ermöglicht hat. Dies ist ein großer Erfolg für den Datenschutz.

2.2.2 Novellierung des Bundesdatenschutzgesetzes 2009

Als Reaktion auf die gravierenden Datenschutzskandale der Jahre 2008 und 2009 hat sich der Bundestag zu einer Novellierung des Bundesdatenschutzgesetzes entschlossen. Mit insgesamt über 90 Änderungen des Bundesdatenschutzgesetzes ist dieses wichtige Gesetz zwar weder übersichtlicher noch lesbarer geworden, weist jedoch eine ganze Reihe begrüßenswerter Neuregelungen auf.

Besonders hervorzuheben sind hier etwa die Änderungen zu automatisierten Einzelentscheidungen (§ 6a BDSG), die Neufassung der Vorschrift zur Auftragsdatenverarbeitung (§ 11 BDSG), die gesetzliche Einschränkung der Datenübermittlung an Auskunfteien (§ 28a BDSG, gilt ab 1. April 2010) sowie des im Lebensalltag besonders relevanten Scorings (§ 28b BDSG, gilt ab 1. April 2010).

In der öffentlichen Diskussion spielte insbesondere die „Abschaffung des Listenprivilegs" in § 28 Abs. 3 BDSG eine erhebliche Rolle. Angesichts der hierzu gleichzeitig beschlossenen sehr langen Übergangsregelungen bis ins Jahr 2012 (§ 47 BDSG) und umfangreicher Ausnahmenkataloge kann man am Erfolg dieser Novellierung jedoch Zweifel haben.

Für die Datenschutzaufsichtsbehörde von besonderer Bedeutung sind drei Änderungskomplexe. Zum einen wurde die Handlungsfähigkeit und Durchschlagskraft der Aufsichtsbehörden durch die Neufassung des § 38 Abs. 5 BDSG verbessert: Nunmehr sind die Datenschutzaufsichtsbehörden befugt, bei jedem Verstoß gegen datenschutzrechtliche Vorschriften Maßnahmen zur Beseitigung festgestellter Verstöße verbindlich anzuordnen. Damit wird den Aufsichtsbehörden aus der misslichen Situation geholfen, festgestellte Datenschutzverstöße, für die nicht zugleich ein Bußgeldtatbestand einschlägig ist, nicht effektiv bekämpfen zu können.

Bei besonders schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer erheblichen Gefährdung des Persönlichkeitsrechts verbunden sind, kann die Aufsichtsbehörde der Anordnung zur Mängelbeseitigung sogar durch die Durchführung eines Verwaltungszwangsverfahrens mit Verhängung eines Zwangsgeldes weiteren Nachdruck verleihen. Diese erweiterten Handlungsoptionen der Aufsichtsbehörde sind zwar ihrerseits wiederum zeit- und personalintensiv, können jedoch eindeutig als Stärkung der Aufsichtsbehörde gewertet werden. Gleichzeitig wurde in § 43 BDSG der Bußgeldrahmen erheblich – nämlich auf bis zu 300.000 Euro – erweitert. Auch die nunmehr in § 43 Abs. 3 Satz 2 BDSG geschaffene Möglichkeit, rechtswidrige wirtschaftliche Vorteile im Rahmen der Geldbuße abzuschöpfen, stärkt die Aufsichtsbehörde erheblich.

In Punkto Öffentlichkeitswirksamkeit des Datenschutzes ist eine zweite gesetzliche Ergänzung von besonderem Interesse: In § 42a BDSG ist erstmals eine Informationspflicht nicht-öffentlicher Stellen bei Datenpannen festgehalten. Erkennt eine verantwortliche Stelle danach, dass sie unrechtmäßig mit personenbezogenen Daten umgegangen ist und drohen hierdurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, so hat sie dies nicht nur der zuständigen Aufsichtsbehörde, sondern auch dem Betroffenen selbst unverzüglich mitzuteilen. Dies wird einerseits zu einer erheblichen Publizität von Datenschutzverstößen führen, zum anderen viele Betroffene überhaupt erst in die Lage versetzen, den rechtswidrigen Umgang mit ihren personenbezogenen Daten zu erkennen und Gegenmaßnahmen bis hin zu Schadensersatzforderungen

einzuleiten. Da der Verstoß gegen diese Informationsverpflichtung der verantwortlichen Stelle zugleich als Bußgeldtatbestand ausgestaltet ist, kann die Aufsichtsbehörde gegen Verletzungen dieser Informationsverpflichtung auch effektiv vorgehen.

Schließlich wurde in § 4f BDSG auch die Rechtsstellung der betrieblichen Datenschutzbeauftragten gestärkt. Für sie wurde ein erweiterter Kündigungsschutz eingerichtet, gleichzeitig stehen ihnen nunmehr Ansprüche auf Fort- und Weiterbildung zu.

Als Reaktion auf die zahlreichen Datenschutzverstöße im Rahmen von Beschäftigungsverhältnissen hat der Bundesgesetzgeber mit § 32 BDSG eine „Auffangnorm" geschaffen, die von ihm selbst als Einstieg in eine grundsätzlichere Regelung zu personenbezogenen Daten von Beschäftigten verstanden wird. Bereits diese „deklaratorische" Vorschrift hat in der Arbeit der Aufsichtsbehörden eine beträchtliche Resonanz erfahren. Dies hängt insbesondere damit zusammen, dass in § 32 Abs. 1 Satz 2 BDSG erstmals gesetzlich festgeschrieben wird, was Arbeitgeber zur Aufdeckung von Straftaten von Beschäftigten unternehmen dürfen; zum anderen wurde der Anwendungsbereich des Bundesdatenschutzgesetzes im nicht-öffentlichen Bereich durch § 32 Abs. 2 BDSG erheblich ausgeweitet, weil das BDSG nunmehr auch Anwendung auf (handschriftliche) Personalakten findet. Hier bleibt abzuwarten, in welcher Weise der Bundesgesetzgeber seiner Ankündigung, ein Arbeitnehmerdatenschutzgesetz zu schaffen bzw. zumindest ein eigenes Kapitel im Bundesdatenschutzgesetz hierfür vorzusehen, zukünftig gerecht wird (s.a. Tz. 2.2.4).

2.2.3 Weiterer Novellierungsbedarf

Trotz der zahlreichen Novellierungen der vergangenen Jahre bleibt das Bundesdatenschutzgesetz in vielen Bereichen unzeitgemäß. Zahlreiche seiner Vorschriften muten antiquiert an, das Datenschutzrecht ist im „Internetzeitalter" noch lange nicht angekommen. Dementsprechend haben auch die Regierungsparteien in ihrem Koalitionsvertrag eine Modernisierung des Datenschutzrechts als wichtiges Ziel beschrieben.

Die Datenschutzbeauftragten der Länder und des Bundes leisten ihren Beitrag zu einer solchen Modernisierung dadurch, dass sie in einer eigens hierfür eingerichteten Arbeitsgruppe ein Eckpunktepapier erarbeiten und noch im Frühjahr 2010 vorlegen werden.

Wesentliche Zielsetzung ist hierbei die Ent-Bürokratisierung, Ent-Technisierung und Ent-Spezialisierung des Bundesdatenschutzgesetzes und – diesem folgend – der Landesdatenschutzgesetze. Angestrebt wird eine gut lesbare, auf die wesentlichen Gesichtspunkte reduzierte Regelung des Datenschutzes (Allgemeiner Teil BDSG), der ggf. um Spezialregelungen mit Technikbezug (Besonderer Teil BDSG) ergänzt werden kann.

Dieses Eckpunktepapier wird in den kommenden Monaten der Öffentlichkeit vorgestellt und sodann den Bundestagsfraktionen zugeleitet werden.

2.2.4 Arbeitnehmerdatenschutzgesetz

Die Bespitzelungs- und Datenmissbrauchsaffairen in einer Reihe großer Unternehmen und öffentlicher Stellen (Videoüberwachung und Erhebung von Gesundheitsdaten von Mitarbeitern in Discountern, massenhafte Datenabgleiche und Überwachung der E-Mail-Kommunikation zur Korruptionsbekämpfung) haben der politischen Diskussion zur Notwendigkeit eines Arbeitnehmerdatenschutzgesetzes neues Leben eingehaucht. Die Datenschutzbeauftragten des Bundes und der Länder fordern seit mehr als 25 Jahren ein eigenes Arbeitnehmerdatenschutzgesetz; trotz entsprechender Absichtserklärungen, Koalitionsvereinbarungen oder sonstiger Verlautbarungen aus dem politischen Umfeld wurde ein entsprechendes Gesetz jedoch nie auf den Weg gebracht.

Die Notwendigkeit einer gesetzlichen Ausgestaltung des Schutzes von Beschäftigtendaten liegt dabei auf der Hand:

Im Arbeitsverhältnis werden eine Vielzahl von hochsensiblen Informationen über Beschäftigte verarbeitet. Es geht dabei um Personalstammdaten (einschließlich Scheidung, Unterhaltspflichten, Religionszugehörigkeit, Pfändungsbeschlüsse), Leistungsbeurteilungen, Zeiterfassungs- und Telekommunikationsdaten sowie um Daten über die Gesundheit. Durch den Einsatz neuer Informations- und Kommunikationstechniken können diese Daten beliebig ausgewertet, zusammengeführt und anderweitig verwendet werden. Neue Softwareprogramme ermöglichen die heimliche Ortung des dienstlichen Mobiltelefons ebenso wie eine heimliche Totalüberwachung der PC-Nutzung durch sog. Keylogger, die jeden Tastaturanschlag aufzeichnen und unbemerkt Screenshots vom Bildschirm anfertigen können. Die Weiterentwicklung der IT-Anwendungen ermöglicht damit neue Kontrollpotentiale auf Seiten des Arbeitgebers, die im Verhältnis zu den Persönlichkeitsrechten der Beschäftigten gesetzlich austariert werden müssen.

Richtig ist, dass Arbeitnehmer derzeit, was ihre Persönlichkeitsrechte im Arbeitsverhältnis angeht, nicht rechtlos gestellt sind: Es gibt das Bundesdatenschutzgesetz, das

Allgemeine Gleichbehandlungsgesetz, das Telemediengesetz, das Telekommunikationsgesetz und das neue Gendiagnostikgesetz, in denen jeweils auch Fragen des Mitarbeiterdatenschutzes geregelt sind. Das Problem liegt aber gerade in der Zersplitterung der einschlägigen Bestimmungen. Die Rechtsanwendung ist dadurch erheblich erschwert. Hinzu kommt, dass etwa das Fragerecht im Einstellungsverfahren weitgehend von den Arbeitsgerichten entwickelt wurde und man dem Betroffenen nicht zumuten kann, zunächst eine höchstrichterliche Entscheidung herbeizuführen, bevor er zu seinem Recht kommt. Außerdem fehlen derzeit abschreckende Sanktionsbestimmungen und solche, die den Betroffenen eine Entschädigungszahlung für erlittene Verletzungen ihres Persönlichkeitsrechts zugestehen.

Angesichts dessen hat auch der LfD im Berichtszeitraum seine Bemühungen zur Schaffung eines Arbeitnehmerdatenschutzgesetzes auf Bundesebene intensiviert. Mit seiner Unterstützung brachte die Landesregierung 2008 einen eigenen Entschließungsantrag zur „eigenständigen gesetzlichen Ausgestaltung des Arbeitnehmerdatenschutzes“ im Bundesrat ein (BR-Drs. 665/2/08), der dort am 7. November 2008 einstimmig verabschiedet wurde. Auf Initiative des LfD formulierte die Konferenz der Datenschutzbeauftragten im März 2009 Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz. Dabei erhielten die Datenschützer unerwartet Unterstützung von prominenter Seite. Die Präsidentin des Bundesarbeitsgerichts, Ingrid Schmidt, hatte bei der Vorstellung ihres Jahresberichtes Änderungen beim Datenschutzrecht im Arbeitsleben angemahnt.

Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.
- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u.a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)
- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z.B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.
- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z.B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.
- Der Einsatz von Überwachungssystemen, wie z.B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.
- Es bedarf der Festlegung der Rechte der Beschäftigten, z.B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.
- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.
- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.
- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

Der von der Vorgänger-Regierung kurz vor Ablauf der Legislaturperiode noch eilig eingebrachte Gesetzesentwurf zum Datenschutz im Beschäftigungsverhältnis (BT-Drs. 17/69 vom 25. November 2009) griff viele dieser Forderungen auf. Eine Realisierungschance bestand wegen der unmittelbar bevorstehenden Bundestagswahl nicht. Sie war mit dem Gesetzentwurf offenbar auch gar nicht angestrebt worden. Das ist bedauerlich, weil eine rechtzeitige Einbringung des Gesetzentwurfs immer wieder angemahnt worden war und auch möglich gewesen wäre.

Es ist erfreulich, dass im Koalitionsvertrag der die neue Bundesregierung tragenden Parteien ein neuer Anlauf angekündigt wird. Dass allerdings kein eigenes Gesetz, sondern nur ein Abschnitt im Bundesdatenschutzgesetz

angestrebt wird, lässt aufhorchen. Denn ganz offensichtlich ist mit dieser Festlegung auch die Federführung für den einzubringenden Gesetzentwurf vorentschieden worden. Dies macht skeptisch.

2.2.5 BKA-Gesetz

Die Neufassung des BKA-Gesetzes (durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt) wurde vom Deutschen Bundestag am 12. November 2008 verabschiedet. Sie ist zum 1. Januar 2009 in Kraft getreten und räumt dem Bundeskriminalamt Befugnisse ein, die bislang nur Landespolizeien und Nachrichtendiensten zustanden. Neben der umstrittenen Online-Durchsuchung (vgl. Tz. 2.2.1, Tz. 6.2.2, Tz. 7.3, Tz. 13.3) haben die neuen §§ 20a bis 20x des Gesetzes unter anderem folgende Befugnisse der Gefahrenabwehr neu geregelt:

- Raster- und Schleierfahndung,
- Einsatz von verdeckten Ermittlern,
- Lauschangriff (auch innerhalb der Wohnung dritter Personen),
- Videoüberwachung innerhalb der Wohnung.

Mit der Neufassung hat das Bundeskriminalamt außerdem das Recht erhalten, präventive Ermittlungen ohne konkreten Tatverdacht in eigener Regie durchzuführen. Im Rahmen der „Vorfeldermittlungen“ unterliegt das Bundeskriminalamt nicht mehr der Leitungsbefugnis der Staatsanwaltschaft. Abhörmaßnahmen dürfen auch gegen Berufsgeheimnisträger (§ 53 StPO), mit Ausnahme der Verteidiger, Abgeordneten und Geistlichen einer staatlich anerkannten Religionsgemeinschaft, durchgeführt werden (§ 20u BKAG).

Im April 2009 haben verschiedene Journalisten sowie der ehemalige Innenminister Gerhart Baum und der Präsident der Bundesärztekammer Verfassungsbeschwerde gegen dieses Gesetz eingelegt, die vom Deutschen Journalisten-Verband unterstützt wird. Zur Begründung wurde darauf verwiesen, Sicherheitsbelange würden auf Kosten der Freiheit der Bürger ausgeweitet, zum Beispiel durch die Möglichkeiten der Online-Durchsuchung und der Überwachung der Telekommunikation. Der Schutz des Kernbereichs privater Lebensgestaltung werde verletzt und der Schutz von Patienten, Mandanten und Informanten relativiert. Von den Auswirkungen des Gesetzes seien nicht nur einige Berufsgruppen, sondern alle Bürger betroffen (Presseerklärung des Deutschen Journalisten-Verbandes vom 23. April 2009).

Über diese Verfassungsbeschwerde ist bislang noch nicht entschieden worden.

Der Bundesdatenschutzbeauftragte hat begrüßt, dass im Laufe des parlamentarischen Gesetzgebungsverfahrens Änderungen beschlossen wurden, wonach nunmehr die Anordnung der Online-Durchsuchung ausnahmslos dem Richtervorbehalt unterstellt wird und die Durchsicht der durch diese Maßnahme erlangten Daten auf kernbereichsrelevante Inhalte ebenfalls nur dem Richter obliegt. Der verfassungsrechtlich gebotene Schutz kernbereichsrelevanter Informationen auf der ersten Stufe schon bei der Datenerhebung bleibe jedoch weiterhin defizitär. Auch wenn es den Anschein habe, dass in dem Gesetz im Übrigen die Vorgaben des Bundesverfassungsgerichts zur Ausgestaltung der Online-Durchsuchung umgesetzt seien, habe er weiterhin Zweifel, inwieweit eine derartige, tief in die Privatsphäre eingreifende Befugnis im Hinblick auf den damit verfolgten Zweck vertretbar sei. Gegen die Eignung der Online-Durchsuchung spreche, dass sie in jedem Einzelfall die Entwicklung maßgeschneiderter Software erforderlich mache und damit technisch sehr aufwendig sei. Damit seien Zweifel angebracht, dass das BKA hiermit entsprechenden Gefahrenlagen rasch begegnen könne. Außerdem bleibe fraglich, ob die mit der Online-Durchsuchung verbundenen Risiken für die informationstechnischen Systeme, z.B. im Zusammenhang mit der Aufbringung entsprechender Software auf dem Zielsystem, wirksam zu beherrschen seien (22. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 2007-2008, S. 47).

Diese Zweifel teilt der LfD. In jedem Fall müssen die Erfahrungen mit dieser neuen Befugnis sorgfältig beobachtet werden. Entscheidend ist die Frage, ob mit dieser Maßnahme ein adäquater Gewinn an Sicherheit erzielt werden kann und ob die gesetzlich vorgegebenen Schutzvorkehrungen die erforderliche Wirkung entfalten. Die Befristung der Befugnis zur Online- Durchsuchung informationstechnischer Systeme bis zum 31. Dezember 2020 ist aus der Sicht des LfD jedenfalls zu lang; eine entsprechende Bewertung muss früher zu gesetzgeberischen Konsequenzen führen.

2.2.6 Personalausweisgesetz

Im letzten Tätigkeitsbericht (21. Tb., Tz. 21.3.4) wurden der elektronische Reisepass der zweiten Generation – Gesichtsbild und Zeigefinger als elektronisch lesbare biometrische Merkmale – sowie der weiterentwickelte Zugriffs- bzw. Ausleseschutz vorgestellt.

Als nächsten Schritt sieht das am 18. Juni 2009 verkündete Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) mit seinem – weitgehenden – Inkrafttreten am 1. November 2010 die Einführung bzw. erste Ausgabe neuer Personalausweise vor. Zusätzlich zu seiner

biometriegestützten Ausweisfunktion für hoheitliche Kontrollen kann der neue Personalausweis optional mit einer Authentisierungsfunktion zum elektronischen Nachweis der Identität (eID-Funktion) sowie mit einer elektronischen Signaturfunktion versehen werden.

Auf die ursprünglich verpflichtend vorgesehene Ausstattung des neuen Personalausweises mit digitalisierten Abdrücken beider Zeigefinger wurde aufgrund datenschutzrechtlicher Bedenken verzichtet. Nach § 5 Abs. 9 PAuswG werden die Fingerabdrücke nur auf Antrag, d.h. mit Einwilligung des Ausweisinhabers gespeichert. Wenn sich der Ausweisinhaber gegen die Aufnahme seiner Fingerabdrücke in den Ausweis entscheidet, darf ihm daraus kein Nachteil entstehen (§ 5 Abs. 9 PAuswG). Trotzdem bleibt der neue Personalausweis – wie schon während des Gesetzgebungsverfahrens – in datenschutzrechtlicher Hinsicht umstritten.

Die optionalen Zusatzfunktionen werden dem elektronischen Rechtsverkehr im Rahmen von E-Business und E-Government neue Möglichkeiten z.B. im Hinblick auf die Online-Authentisierung bieten. Damit verbunden sein wird aber möglicherweise auch eine höhere Missbrauchsgefahr als beim elektronischen Reisepass. Ein unberechtigtes Auslesen der Daten und der PIN muss zuverlässig unterbunden werden. Der Zugriff auf Identitätsdaten im Rahmen der eID-Funktion sollte nur solchen privaten Stellen gewährt werden, die sich einem Datenschutzaudit unterwerfen.

Den ab Januar 2010 bei der Stadtverwaltung Neuwied stattfindenden Feldtest wird der LfD begleiten. Es geht bei dem Test um den Nachweis der Integrationsfähigkeit der neuen Verfahrensmodule in die bei den Pass- und Personalausweisbehörden vorhandene technische Umgebung sowie um die Prüfung der Praxistauglichkeit des gesamten Verfahrens. Mit der Einführung des neuen Ausweises wird bei den Behörden ein hoher Schulungsbedarf entstehen, da die auf freiwilliger Basis einzurichtende Identitätsnachweis-Funktion von den Personalausweisbehörden zu betreuen ist (§ 10 PAuswG).

2.2.7 ELENA-Verfahrensgesetz

Mit den im Frühjahr 2009 beschlossenen Regelungen des Gesetzes über den elektronischen Entgeltnachweis (ELENA-Verfahrensgesetz, BGBl. I, S. 634) ist die Einführung eines aus datenschutzrechtlicher Sicht höchst umstrittenen Verfahrens kaum noch aufzuhalten. Das Gesetz sieht die Schaffung einer bundesweiten Zentraldatei vor, an die ab dem 1. Januar 2010 von den Arbeitgebern monatlich die Einkommensdaten der über 30 Millionen abhängig Beschäftigten, Beamten, Richter und Soldaten übermittelt werden müssen. Damit erhofft sich der Gesetzgeber wie so oft massive Kosteneinsparungen: Die zur Vorlage bei der Beantragung bestimmter Sozialleistungen wie z.B. Arbeitslosengeld, Wohngeld oder Elterngeld benötigten und bisher von den Arbeitgebern auf Papier erstellten Gehaltsbescheinigungen sollen künftig von einer bei der Deutschen Rentenversicherung Bund eingerichteten Datenbank aus den Sozialbehörden elektronisch zur Verfügung gestellt werden. Nach den in den §§ 95 ff. SGB IV enthaltenen Vorgaben soll das Abrufverfahren zum 1. Januar 2012 funktionsfähig sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben das Projekt von Anfang an kritisch begleitet. Zweifel an der datenschutzrechtlichen Vereinbarkeit des ELENA-Verfahrens ergeben sich insbesondere aus der Tatsache, dass in einer Zentraldatei massenhaft schutzbedürftige Daten von Beschäftigten auf Vorrat vorgehalten werden sollen, deren konkrete Verwendung im Einzelfall jedoch überhaupt nicht absehbar ist. Denn auch die Daten desjenigen, der niemals eine der gesetzlich vorgesehenen Sozialleistungen beantragen wird, müssen jahrelang in der ELENA-Datenbank gespeichert werden. Dies stellt im Ergebnis einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Zudem besteht wie immer bei der Schaffung derartiger Zentraldateien die Gefahr, dass weitere Begehrlichkeiten zum Einsatz dieser Daten geweckt werden und die zunächst noch gesetzlich bestehende Beschränkung der Datennutzung auf den o.g. Zweck nach und nach aufgeweicht wird.

Vor diesem Hintergrund hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt, zuletzt auf ihrer 76. Sitzung am 6./7. November 2008, in Entschließungen auf die bestehenden verfassungsrechtlichen Bedenken gegen das ELENA-Verfahren hingewiesen.

Auszug aus der Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder – Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren – vom 6./7. November 2008

[…]

Die Datenschutzbeauftragten des Bundes und der Länder haben *[…]* wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass

derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.
Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden, (z.B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.
- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.
- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.
- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.
- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.
- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.
- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

In der jüngsten Vergangenheit konzentrierte sich die öffentliche Diskussion auf den Umfang der von den Arbeitgebern an die ELENA-Datenbank zu meldenden Daten. Der zunächst von den beteiligten Bundesbehörden vereinbarte Multifunktionale Verdienstdatensatz sah u.a auch die Übermittlung von Arbeitskampfdaten, Abmahnungen und Freitextfeldern vor, obwohl deren Erforderlichkeit für die Erstellung der verschiedenen Entgeltnachweise nicht belegt war. Auf Intervention der Datenschutzbeauftragten werden nun unter Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sämtliche Datenfelder auf ihre Rechtmäßigkeit hin überprüft.

2.3 Landesrecht

Der moderne Staat hat viele Aufgaben wahrzunehmen, vor allem in seiner Funktion als Leistungs- und Sozialstaat. Dafür benötigt er Daten und Informationen von und über seine Bürger. Allerdings gibt es dafür Grenzen, vor allem in datenschutzrechtlicher Hinsicht. Diese Grenzen hat auch das Land zu beachten, vor allem der Landesgesetzgeber.

Da bei den meisten Gesetzen persönliche Daten von Bürgern eine Rolle spielen, sind diese Gesetze in der Regel auch datenschutzrechtlich relevant. Dies zeigt ein Überblick über die Gesetze, die in den Jahren 2008 und 2009 vom Landtag verabschiedet worden sind. Von diesen rund 80 Gesetzen bzw. Gesetzesänderungen warfen rund zwei Drittel datenschutzrelevante Fragen auf. Zum Teil ging es dabei um Randfragen, zum Teil stand der Datenschutz im Mittelpunkt der Betrachtungen. Stets wurde der LfD um Stellungnahme gebeten, und zwar von der Landesregierung, zum Teil auch vom Landtag. Die Mehrzahl der Anregungen wurde aufgegriffen und umgesetzt. Dies belegt die datenschutzrechtliche Sensibilität von Landtag und Landesregierung bei der Wahrnehmung ihrer Gesetzgebungsfunktion.

2.3.1 Novellierung des Landesdatenschutzgesetzes 2008

Durch Änderung des Landesdatenschutzgesetzes ist der LfD seit dem 1. Oktober 2008 vom Landtag mit der Aufgabe betraut worden, zusätzlich zum Datenschutz im öffentlichen Bereich auch die Funktion einer Datenschutzaufsichtsbehörde im nicht-öffentlichen Bereich zu übernehmen. Seit Januar 2009 wurde die Dienststelle des LfD hierfür personell verstärkt.

2.3.2 Weiterer Novellierungsbedarf

Mit Blick auf die jüngsten Novellierungen des Bundesdatenschutzgesetzes, die aktuelle Rechtssprechung des Bundesverfassungsgerichts sowie Erfahrungswerte aus der Praxis der Datenschutzbehörde sieht der LfD auch hinsichtlich des Landesdatenschutzgesetzes weiteren Änderungsbedarf. Hierbei soll es in einem ersten Schritt nicht um eine grundsätzliche Neuausrichtung des Landesdatenschutzrechts vor dem Hintergrund der rasant fortschreitenden technologischen Entwicklung gehen, sondern im Wesentlichen um sechs einzelne Änderungsvorschläge, die überwiegend die Novellierungen des Bundesdatenschutzgesetzes auf Landesebene nachvollziehen:

- Die Erfahrung der Datenschutzskandale der letzten zwei Jahre und die Reaktionsmöglichkeiten der zuständigen Aufsichtsbehörden lassen aus Sicht des LfD erkennen, dass alleine mittels Gesetzgebung und aufsichtbehördlicher Kontroll- und Vollzugsmaßnahmen ein angemessenes Datenschutzniveau nicht sichergestellt werden kann. Damit rückt die Aufgabe des „Selbstdatenschutzes“ immer weiter ins Zentrum. Deshalb müssen die Bürger auch durch staatliche Bildungsmaßnahmen in die Lage versetzt werden, verantwortlich mit dem eigenen Recht auf informationelle Selbstbestimmung und respektvoll mit den Daten anderer umzugehen. Adressat dieses Bildungsauftrags, mit dem der Staat seiner Schutzpflicht gegenüber (insbesondere minderjährigen) Grundrechtsträgern nachkommt, sind alle Bildungsträger in Rheinland-Pfalz.
  Durch die Aufnahme einer entsprechenden Bestimmung in § 1 oder an anderer Stelle des Landesdatenschutzgesetzes könnte die „Bildungsaufgabe Datenschutz“ an sämtliche Bildungsträger in Rheinland-Pfalz adressiert und so eine Grundlage dafür geschaffen werden, dass zukünftig nicht nur in Schulen, sondern auch im Rahmen der politischen Bildungsarbeit, in Volkshochschulen, Ausbildungseinrichtungen und anderen Bildungsstätten Datenschutz als eigenständige Bildungsaufgabe verstanden und wahrgenommen wird (s.a. Tz. 3.1).
- Mit Wirkung zum 1. September 2009 ist der neue § 42a BDSG in Kraft getreten, der im Fall einer „Datenpanne“ umfangreiche Informationspflichten vorsieht. Insbesondere sind von der verantwortlichen Stelle unverzüglich die Betroffenen sowie die Aufsichtsbehörde über die Datenpanne zu unterrichten. § 42a BDSG gilt jedoch nur für nicht-öffentliche Stellen, nicht aber für Landesbehörden. Für eine solche unterschiedliche Behandlung ist kein überzeugender Grund ersichtlich, weswegen eine entsprechende Anpassung des Landesdatenschutzgesetzes vorgeschlagen wird.
- Ziel der Novellierung des Bundesdatenschutzgesetzes war insbesondere eine Besserstellung und Stärkung der betrieblichen Datenschutzbeauftragten. Demgemäß sieht der neue § 4f BDSG einen umfassenden Kündigungsschutz sowie einen Anspruch des betrieblichen Datenschutzbeauftragten auf Fort- und Weiterbildung vor. Eine entsprechende Vorschrift zur Fort- und Weiterbildung ist auch für die behördlichen Datenschutzbeauftragten nach dem Landesdatenschutzgesetz zu schaffen.
- Zahlreiche Landesbehörden arbeiten im IT-Bereich, etwa bei der Wartung der EDV-Anlagen, der Archivierung von Behördendaten oder bei der Aktenvernichtung, mit anderen öffentlich-rechtlichen oder privaten Dienstleistern zusammen. Für diese Formen der Auftragsdatenverarbeitung sieht die Novelle des Bundesdatenschutzgesetzes in § 11 seit dem 1. September 2009 besondere Vertragsinhalte für die Vertragsgrundlage zwischen Behörde und Auftragsdatenverarbeiter vor. Entsprechend spezifizierte Vorgaben enthalten die Regelungen des Landesdatenschutzgesetzes nicht, so dass sich auch insoweit eine Übernahme der bundesrechtlichen Vorschriften empfiehlt. Außerdem ist an dieser Stelle über mögliche Sanktionsmaßnahmen für den Fall nachzudenken, dass der Auftragnehmer vertragliche Vorgaben im Rahmen der Auftragsdatenverarbeitung verletzt.
- Aus der Praxis des LfD – insbesondere aus der umfassenden Umfrage zur Videoüberwachung in Rheinland-Pfalz – ist bekannt, dass die Regelung des § 34 LDSG zur Videoüberwachung durch Landesbehörden weiterer Klärung bedarf. Dies gilt insbesondere für die durch den Landesgesetzgeber zu entscheidende Frage, ob zukünftig von Landesbehörden Videoüberwachungs-Attrappen eingesetzt werden sollen und dürfen. Klärungsbedarf gibt es weiterhin hinsichtlich der Abgrenzung von Videobeobachtung (Monitoring) und Videoaufzeichnung und zu hierfür vorzusehende gesetzliche Eingriffshürden (Videoüberwachung nur bei konkreter Gefahr für erhebliche Rechtsgüter).

Diese Vorschläge wurden bereits mit den Mitgliedern der Datenschutzkommission erörtert und werden den Fraktionen zugeleitet.

2.3.3 Landeskinderschutzgesetz

Mit dem am 21. März 2008 in Kraft getretenen Landeskinderschutzgesetz gehörte Rheinland-Pfalz zu einem der ersten Länder bundesweit, das aufgrund gesetzlicher Regelungen die Förderung des Kindeswohls und die Verbesserung des Kinderschutzes durch vom Gesetzgeber festgelegte Maßnahmen verlangte. Vorangegangen war ein über ein Jahr andauernder intensiver politischer Meinungsbildungsprozess mit zwei parlamentarischen Anhörungen, in dem von Anfang an auch der LfD eng eingebunden war (vgl. 21. Tb., Tz. 11.2).

Von besonderem Interesse ist aus datenschutzrechtlicher Sicht das in dem Gesetz verankerte Einladungs- und Erinnerungsverfahren zu den nach § 26 SGB V angebotenen Früherkennungsuntersuchungen für Kinder (§§ 5 bis 10 LKindSchuG). Eine beim Landesamt für Soziales, Jugend und Versorgung (LSJV) eingerichtete Zentrale Stelle lädt hiernach auf der Basis der ihr übermittelten Meldedaten alle zu einer konkreten Untersuchung anstehenden Kinder bzw. deren Sorgeberechtigte zur Wahrnehmung des Vorsorgeangebots ein. Mittels eines

Datenabgleichs ermittelt die Stelle die bis zu einem bestimmten Zeitpunkt trotz Erinnerung nicht nachweislich untersuchten Kinder und meldet diese dem örtlich zuständigen Gesundheitsamt. Die Gesundheitsbehörden klären dann die Betroffenen gezielt über die Untersuchungsangebote auf und wirken auf deren Inanspruchnahme hin. Erfolgt diese nicht, werden die jeweiligen Jugendämter unterrichtet, um bei einem ggf. vorliegenden Hilfebedarf die notwendigen und erforderlichen Maßnahmen zur frühen Förderung zur Verfügung zu stellen.

Mit dem gesetzlich vorgesehenen Verfahren werden in beträchtlichem Maße personenbezogene Daten verarbeitet. So erhält die neu geschaffene Zentrale Stelle von den Meldebehörden kontinuierlich Meldedaten der betroffenen Kinder und deren Sorgeberechtigter. Zugleich sind die untersuchenden Ärzte verpflichtet, innerhalb von drei Arbeitstagen der Zentralen Stelle die Durchführung der Untersuchung zu bestätigen. Unterbleibt dies, werden die zuständigen Gesundheits- und ggf. Jugendämter unterrichtet, obwohl die Teilnahme an den Untersuchungen weiterhin freiwillig ist und die Tatsache einer Nichtteilnahme für sich genommen noch kein Indiz einer drohenden Kindeswohlgefährdung ist.

Trotz der mit dem Gesetz verbundenen Grundrechtseingriffe hielt der LfD das Einladungsverfahren noch mit dem informationellen Selbstbestimmungsrecht für vereinbar. Denn die gesetzlich vorgesehenen Maßnahmen stehen angesichts des staatlichen Wächteramts im überwiegenden Allgemeininteresse und sind zur Erreichung der gesetzgeberischen Ziele einer Stärkung der Kindergesundheit und einer Verbesserung des Kinderschutzes verhältnismäßig. Durch die datenschutzgerechte Ausgestaltung des Einladungsverfahrens gelang ein angemessener Interessenausgleich zwischen dem Recht auf informationelle Selbstbestimmung und einem effektiven Kinderschutz. Hervorzuheben sind dabei folgende Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts, die überwiegend auf Anregung des LfD in den Gesetzentwurf aufgenommen wurden:

- Auf eine Befugnis zur Auslagerung von Teilaufgaben der Zentralen Stelle auf private Auftragnehmer wurde verzichtet. Zur Erfüllung ihrer gesetzlichen Verpflichtungen kann sich die Zentrale Stelle ausschließlich anderer öffentlicher Stellen bedienen (§ 5 Abs. 2 Satz 2 LKindSchuG). Dies hat sie mittlerweile mit der Beauftragung des Zentrums für Kindervorsorge an der Universitätsklinik des Saarlandes auch umgesetzt.
- Die zunächst vorgesehene Möglichkeit eines Onlinezugangs der Zentralen Stelle auf sämtliche Meldedaten wurde verworfen. Der Zentralen Stelle stehen lediglich die zuvor von den Meldebehörden bereit gestellten und von ihr zur Aufgabenerfüllung benötigten Meldedaten zur Verfügung (§ 6 Abs. 2 LKindSchuG).
- Die untersuchenden Ärzte sind gesetzlich verpflichtet, innerhalb von drei Arbeitstagen gegenüber der Zentralen Stelle die Durchführung der Untersuchung zu bestätigen. Die Weitergabe medizinischer Informationen ist hierzu nicht erforderlich (§ 7 Abs. 2 LKindSchuG).
- Durch verfahrenstechnische Vorgaben ist bei der Zentralen Stelle, den Gesundheits- und den Jugendämtern die Verarbeitung der Daten durch Unbefugte auszuschließen (§§ 7 Abs. 2, 8 Abs. 1 Satz 4, 9 Abs. 1 Satz 4, 10 LKindSchuG). Zudem unterliegen die Daten des Einladungsverfahrens einer strikten Zweckbindung; die allgemeinen Anforderungen an eine angemessene Datensicherheit gelten auch hier (§ 10 Abs. 4 LKindSchuG).
- Die in § 10 LKindSchuG festgelegten Speicherfristen verhindern eine dauerhafte Sammlung von Daten zu Personen, die sich nach dem Verständnis des Gesetzes unauffällig verhalten haben.
- Die auf Anregung des LfD in § 11 LKindSchuG aufgenommene Pflicht zur Evaluation der gesetzlich vorgesehenen Maßnahmen stellt sicher, einen möglicherweise bestehenden Korrekturbedarf des Verfahrens zu erkennen und vorzunehmen.

Zwischenzeitlich hat der Verfassungsgerichtshof Rheinland-Pfalz über eine Verfassungsbeschwerde gegen das Landeskinderschutzgesetz entschieden und in seinem Urteil vom 28. Mai 2009 Bedenken gegen die verfassungsrechtliche Vereinbarkeit der im Gesetz enthaltenen Grundrechtseingriffe zurückgewiesen. Insbesondere sei mit den gesetzlich vorgesehenen Maßnahmen keine übermäßige Einschränkung des Grundrechts auf informationelle Selbstbestimmung verbunden. Der Verfassungsgerichtshof bestätigte damit die bisherige Einschätzung des LfD und unterstrich dabei die hohe Bedeutung der in dem Gesetz enthaltenen verfahrensmäßigen Sicherungen zum Schutz des betroffenen Grundrechts. Ungewöhnlich deutlich fordert das Gericht in seiner Entscheidung eine Löschung der gespeicherten personenbezogenen Daten nach Erreichen des mit dem Landeskinderschutzgesetz verfolgten Zwecks der Datenerhebung und gestattet die Ausschöpfung der gesetzlich zulässigen Maximalspeicherfrist nur in den erforderlichen Fällen.

2.3.4 Novellierung des Landesbeamtengesetzes

Im Zuge der Föderalismusreform sind die Gesetzgebungszuständigkeiten im Bereich des öffentlichen Dienstrechts neu geregelt worden. So wurde dem Bund im Rahmen der konkurrierenden Gesetzgebungskompetenz die Aufgabe zugewiesen, die Statusrechte und -pflichten der Beamten der Länder, Gemeinden und anderer Körperschaften des öffentlichen Rechts zu regeln. Hiervon hat der Bund mit

dem Beamtenstatusgesetz, welches in weiten Teilen zum 1. April 2009 in Kraft getreten ist, Gebrauch gemacht. Den Ländern obliegt es nunmehr, die gewonnenen Handlungsspielräume im Bereich des Berufsbeamtentums und des Laufbahnrechtes gesetzgeberisch umzusetzen.

Der LfD wurde frühzeitig in das Verfahren zum Neuerlass des Landesbeamtengesetzes eingebunden. Sein Hauptanliegen bestand darin, für alle öffentlich Bediensteten einheitliche Rechtgrundlagen bei der Verarbeitung von Personaldaten zu erreichen. Dies ist auch gelungen: Zwar gelten für die Beamten auch in Zukunft die beamtenrechtlichen Vorschriften zur Personalaktenführung und für die Tarifbeschäftigten § 31 LDSG als spezialgesetzliche Vorschrift zum Arbeitnehmerdatenschutz. Doch künftig verweisen beide Regelungsbereiche ergänzend auf die jeweils anderen Bestimmungen, so dass ein einheitliches Datenschutzniveau für alle öffentlich Bediensteten im Bereich Personaldatenschutz sichergestellt ist.

Die sonstigen Forderungen des LfD, die ebenfalls weitgehend berücksichtigt wurden, betrafen das Einsichtsrecht in Personal- und Sachakten, die Datenverarbeitung im Einstellungsverfahren, Rechtsfragen zur Datenübermittlung sowie die Dauer von Aufbewahrungsfristen.

Datenschutzrechtliche Verschlechterungen wird es jedoch im Bereich der Beihilfebearbeitung geben: Zum einen wurde die Aufbewahrungsfrist für die Geltendmachung etwaiger Schadensersatzansprüche des Dienstherrn gegen Leistungserbringer (z.B. Ärzte) von bisher fünf auf zehn Jahre heraufgesetzt; zum anderen wurde die Rechtslage an die fortschreitende automatisierte Verarbeitung im Bereich der Beihilfe, insbesondere was das beabsichtigte Einscannen der eingereichten Unterlagen angeht, angepasst. Die Verpflichtung der Beihilfestelle, die eingereichten Unterlagen an den Betroffenen zurückzusenden, entfällt in diesen Fällen. Stattdessen sind die Daten zu sperren und dürfen bis zur Löschung nur unter sehr restriktiven Voraussetzungen genutzt werden. Der LfD wird die Einführung einer neuen Software im Bereich der Beihilfe, die für die o.g. Änderungen mitursächlich ist, auch weiterhin kritisch begleiten.

2.3.5 Novellierung des Landesarchivgesetzes

Anlass der Novellierung ist die Anpassung an die seit 1990 weiter entwickelten Grundsätze des Archivrechts und das vielfach aus Wissenschaftskreisen vorgebrachte Anliegen nach einer Liberalisierung des Zugangs zu zeithistorisch relevantem Daten- und Aktenmaterial in öffentlichen Archiven. Für Forschungsarbeiten werden Quellen leichter zugänglich gemacht. Maßgeblich geändert wird daher mit § 3 LArchG die Vorschrift, die die Nutzung öffentlichen personenbezogenen Archivguts regelt.

Insbesondere werden die Sperrfristen für die Nutzung personenbezogenen Archivguts verkürzt. Außerdem wird eine Verkürzung dieser Sperrfristen im Einzelfall erleichtert, indem den Archiven ein größerer Ermessensspielraum eingeräumt wird. Von Bedeutung ist auch die Möglichkeit der Verkürzung von Sperrfristen ausdrücklich auf Dokumentationsvorhaben und die Schaffung einer wissenschaftlichen Infrastruktur auszudehnen. Denn nach der noch geltenden Rechtslage kann entsprechenden Anträgen zur Übernahme von Daten in Datenbanken ohne konkretes Forschungsvorhaben, beispielsweise von der Gedenkstätte Yad Vashem (Jerusalem) oder dem Institut für Zeitgeschichte (München), nicht entsprochen werden.

Der LfD unterstützte diese Änderungen nicht zuletzt wegen der vergleichbaren Rechtslage in den meisten anderen Bundesländern und dem geltend gemachten öffentlichen Interesse. Die schutzwürdigen Belange Betroffener werden weiterhin gewahrt.

3. Arbeitsschwerpunkte

3.1 Datenschutz als Bildungsauftrag

Datenschutz ist nicht nur eine Angelegenheit von Recht und Gesetz, sondern auch eine Frage von Bildung und Erziehung. Zu den Arbeitsschwerpunkten des LfD zählte deshalb vor allem die Befassung mit dem Thema „Datenschutz als Bildungsaufgabe“. Unter dieser Überschrift lassen sich eine Reihe von Initiativen, Maßnahmen und sonstige Aktivitäten zusammenfassen. In erster Linie ging es darum,

- die Situation zu analysieren,
- Handlungsempfehlungen zu entwerfen und
- daraus die notwendigen Forderungen abzuleiten.

Parallel dazu bemühte sich die Dienststelle des LfD darum, die zuständigen Stellen in Staat und Wirtschaft zu sensibilisieren und sie bei ihren entsprechenden Bemühungen zu unterstützen.

3.1.1 Ausgangssituation

Bereits im 21. Tätigkeitsbericht im Dezember 2007 war unter „Ausblick“ (vgl. 21. Tb., Tz. 25) die Rede davon, dass jeder Nutzer des Internet zwar selbst dafür verantwortlich sei, in welchem Umfang er persönliche Daten preisgebe. Überwiegend fehle den Betroffenen aber die Kenntnis davon, dass jede Nutzung des Internet persönliche Spuren im Netz hinterlasse, die auch nach Jahren und Jahrzehnten noch feststellbar seien. Insoweit müsse bei den Bürgern ein Bewusstsein dafür geschaffen werden, dass das Internet ein ewiges Gedächtnis habe und dass dies nicht nur mit Gefahren für unsere Gesellschaft, sondern für jeden Einzelnen verbunden sei.

Diese Feststellung trifft immer noch zu. Zugleich ist in den beiden zurückliegenden Jahren noch deutlicher geworden, dass es den Internetnutzern immer schwerer gemacht wird, ihrer eigenen Verantwortung gerecht zu werden. Es bleibt zunehmend im Verborgenen, welche digitalen Aktivitäten welche Datenspuren hinterlassen und wer diese zu lesen in der Lage ist. Gleichzeitig wird die Handhabung der digitalen Medien immer einfacher. Dies fördert die Illusion, Computer, Mobiltelefone oder das Internet mit leichter Hand beherrschen und beinahe automatisch, also gedankenlos, bedienen zu können. Dabei bleiben auch Gedanken auf der Strecke, die angebracht wären: Welche Daten gebe ich von mir preis, wer hat Zugriff darauf und welche Folgen hat dies für mich. So produziert der informationstechnische Fortschritt auch den uninformierten und deshalb weitgehend unmündigen Verbraucher und digitalen Surfer.

Es überrascht deshalb nicht, dass nach den vorliegenden Untersuchungen die Datenschutzkompetenz der Bürger gering und ihr Datenschutzbewusstsein wenig ausgeprägt ist.

Dies ist deshalb problematisch, weil mangelndes Datenschutzbewusstsein eine der Ursachen dafür ist, dass die Bürger in großem Umfange persönliche Daten von sich preisgeben, im Internet aber auch in der physischen Welt. Die massenhafte Preisgabe persönlicher Daten wiederum hat schwerwiegende Folgen für den einzelnen Nutzer, sie kann aber auch gravierende Auswirkungen auf den gesellschaftlichen Zusammenhalt haben. Eine zivilisierte Gesellschaft lebt davon, dass Geheimnis und Öffentlichkeit, Scham und Offenheit in einem ausgewogenen Verhältnis zueinander stehen. Dieses ausgewogene Verhältnis scheint aber vor allem durch die Entwicklung im Internet zunehmend verloren zu gehen. Angesichts dieser weit reichenden Konsequenzen, die mit der digitalen Unbekümmertheit verbunden sind, spielen wir mit dem Feuer, wenn wir nicht endlich nachhaltig und ernsthaft damit beginnen, die Onliner und Digitalisten, Jung und Alt, über die digitale Realität aufzuklären.

3.1.2 Inhalt eines Unterrichts- und Bildungskonzeptes

Es ist nicht notwendig, dass die Bürger den Inhalt der vielen Datenschutzgesetze kennen. Es ist aber notwendig, dass sie verantwortungsvoll von ihren Datenschutzgrundrechten Gebrauch machen können. Im Mittelpunkt einer Bildungsaufgabe „Datenschutz“ steht deshalb die informationelle Selbstverantwortung. Alles, was an Wissen und Einsicht notwendig ist, um diese Selbst- und Eigenverantwortung wahrnehmen zu können, gehört deshalb zu den datenschutzrechtlichen Bildungs- und Erziehungszielen. Dies läuft auf sechs Forderungen hinaus:

- Die Menschen müssen in die Lage versetzt werden, die Bedeutung der Privatsphäre für ein freiheitliches Leben zu erkennen. Wenn man nichts zu verbergen hat, muss dies noch lange nicht bedeuten, dass man alles offenbart. Wäre es anders, könnten nur noch Übeltäter auf ihre Privatsphäre pochen.
- Die Bürger müssen über die Gefahren, die ihren Datenschutzgrundrechten drohen, aufgeklärt werden: über die Gefahren, die vom Staat ausgehen, von der Wirtschaft, aber auch von ihnen selbst. Es geht um die Gefahren, die ihnen im Internet drohen, durch die sonstigen digitalen Medien und auch in der physischen Welt. Es geht um Vorratsdatenspeicherung und Adresshandel, um Online-

Durchsuchung und personalisierte Werbung, um Datenklau und Identitätsdiebstahl, um nur ein paar Stichworte zu nennen, die ohnehin austauschbar sind, weil die rasante technische Entwicklung stets neue Risiken und Gefahren hervorbringt.

- Es muss vor allem vermittelt werden, welche Möglichkeiten die Bürger haben, um diesen Gefahren selbst begegnen zu können. Selbstdatenschutz ist deshalb das Stichwort, digitale Selbstverteidigung das Gebot der Stunde. Viele Vorschläge sind bereits entwickelt worden. Die Bandbreite reicht von Ratschlägen für das digitale Verhalten in sozialen Netzwerken, über Selbsthilfemaßnahmen beim Adresshandel bis zu Anregungen für eine effektive Verschlüsselung und eine sichere Passwortgestaltung. Es geht aber auch um die Löschung von Cookies und um Identitätsmanagement, auch und natürlich um Alternativen bei der Nutzung von Suchmaschinen. Denn es gibt Suchmaschinen, die – anders als Google – überhaupt keine Nutzerdaten speichern: Ixquick.com ist ein solcher Geheimtipp.
- Die allgemeinen und bereichsspezifischen Datenschutzvorschriften enthalten eine Vielzahl von Rechten, die den Bürgern helfen sollen, ihre grundgesetzlich verbürgten informationellen Rechtspositionen zu verteidigen. Diese Rechte reichen von Auskunfts- bis zu Löschungsansprüchen. Den meisten Menschen sind diese Rechte aber nicht bekannt. Sie werden deshalb überwiegend auch nicht wahrgenommen.
- Bei allen Bemühungen um digitale Selbstverteidigungsmöglichkeiten und informationelle Selbstschutzaktivitäten darf nicht verloren gehen, dass es auch im Internet nicht nur um Datenschutzrechte, sondern auch um Datenschutzpflichten geht. Das Web 2.0 verleiht Macht, nicht zuletzt wegen seiner scheinbaren Anonymität. Damit muss verantwortungsvoll umgegangen werden. Das gilt insbesondere für die Daten und Informationen über Dritte. Über diese Daten darf nicht beliebig verfügt werden. Sie sind zu respektieren. Letztlich geht es also um die Entwicklung einer Online-Ethik, um digitale Moral. Auch sie entsteht nicht von alleine, sondern muss anerzogen werden.
- Die Auseinandersetzung mit den Risiken der digitalen Entwicklung und ihren Vorteilen sollte am Ende auch dazu befähigen, kritisch mit den neuen Medien umzugehen und Heilsversprechungen der neuen Technologien auch zu misstrauen, sie zumindest zu hinterfragen. Es geht um einen „kritischen Realismus“, der die Fähigkeit beinhalten muss, nicht jeder digitalen Mode hinterherzulaufen und nicht jedes mediale Angebot bis zur Erschöpfung zu konsumieren.

3.1.3 Bildungspolitische Forderungen

Erziehung zum Datenschutz ist eine Gemeinschaftsaufgabe von Staat, Wirtschaft und Gesellschaft, wobei allerdings das staatliche Schulsystem sicherlich die Hauptverantwortung zu tragen hat. Die Anstrengungen, die bereits jetzt unternommen werden, um den Schülerinnen und Schülern „informationelle Selbstbestimmung“ und „informationelle Selbstverantwortung“ zu vermitteln, sind anzuerkennen. Sie genügen allerdings noch nicht. Dies gilt erst recht für die Beiträge, die von den sonstigen staatlichen und nicht-staatlichen Bildungseinrichtungen erwartet werden können. Es muss also mehr getan werden. Die Vorschläge des LfD lassen sich in 10 Punkten zusammenfassen:

- Es ist notwendig, für das Thema „Datenschutz als Bildungsaufgabe“ zu werben, auch in den Parteien und vor allem in den Parlamenten. Es ist hilfreich, dass sich auch die Enquete-Kommission „Verantwortung in der medialen Welt“ mit dieser Thematik befasst.
- Es fehlen immer noch ausreichende empirische Erkenntnisse, vor allem zu der Frage, was Jugendliche und Erwachsene unter Datenschutz verstehen und inwieweit sie sich zutrauen, ihre Daten ein Stück weit selbst zu schützen. Entsprechende Untersuchungen müssen deshalb initiiert und durchgeführt werden.
- Die Datenschutzbeauftragten und die mit Bildungsfragen befassten Fachleute sollten die vorhandenen Vorschläge für eine bessere unterrichtliche Vermittlung des Datenschutzes überprüfen, ergänzen und zu einem geschlossenen Unterrichtskonzept zusammenfassen.
- Die Grundzüge eines solchen Unterrichtskonzeptes sollten in einer ministeriellen Richtlinie geregelt werden. Solche Richtlinien gibt es bei allen fächerübergreifenden Unterrichtsinhalten, etwa bei der Sexualerziehung. Für die Datenschutzerziehung kann nichts anderes gelten.
- Die Notwendigkeit, den Datenschutz im schulischen Unterricht zu verbessern und auszuweiten, sollte außerdem in einer schulpolitischen Grundsatzentscheidung des zuständigen Ministeriums zum Ausdruck gebracht werden. Ohne eine solche Grundsatzentscheidung wird sich am schulischen Unterricht, aber auch an der Ausbildung der Lehrkräfte, nichts ändern.
- Es ist an der Zeit, dass sich auch die Kultusministerkonferenz mit diesem Thema befasst. Dies hat sie bisher noch nicht getan.
- Auch die schulischen Datenschutzbeauftragten, die nach dem Landesdatenschutzgesetz in allen Schulen einzurichten sind, sollten für das Thema gewonnen werden. In Rheinland-Pfalz sind dies gut 1.500 schulische Datenschutzbeauftragte. Sie sollen nicht nur ein Auge auf die Verarbeitung personenbezogener Daten im Schulbereich werfen, sondern sich auch für eine verbesserte Daten-

schutzkompetenz der Schüler sowie der Lehrer und der Eltern einsetzen. Sie bilden ein großes Potential, das nicht ungenutzt bleiben darf.

- Auch außerhalb der Schule besteht Handlungsbedarf, etwa bei den Hochschulen. Auch dort sollte der Datenschutz in den elementaren Bildungskanon aufgenommen werden. Deshalb sollte sich auch die Gemeinsame Wissenschaftsministerkonferenz mit dem Thema „Datenschutz als Bildungsaufgabe“ befassen. Ähnliches gilt auch für die Zentralen für politische Bildung und die Landesmedienanstalten.
- Die Förderung des Datenschutzbewusstseins in der Bevölkerung ist nicht nur eine staatliche Aufgabe. Vor allem die Wirtschaft ist gefordert. Denn zu einem großen Teil entstehen die Gefahren für das Datenschutzgrundrecht der Bürger in ihrem Bereich. Sie hat sich deshalb – bei allem Respekt vor ihren bisherigen Leistungen – stärker um die digitalen Kompetenzen der Bürger zu kümmern.
- Auch der Gesetzgeber sollte sich der Problematik annehmen. Der Ausbau der Datenschutzkompetenz sollte nicht nur bildungspolitisch gefordert, sondern gesetzlich vorgeschrieben werden. Dies würde eine entsprechende Verpflichtung von Staat, Wirtschaft und Gesellschaft am nachhaltigsten zum Ausdruck bringen.

3.1.4 „Medienkompetenz macht Schule“

Die Landesregierung unternimmt bereits seit einiger Zeit erhebliche Anstrengungen zur Förderung des Datenschutzes. Dies gilt vor allem im Schulbereich. Im Mittelpunkt dieser Bemühungen steht das 10-Punkte-Programm der Landesregierung „Medienkompetenz macht Schule“, das auf

- die Qualifizierung der Lehrkräfte,
- die Information der Eltern,
- die Entwicklung des Unterrichts,
- die Realisierung eines Peer-Group-Konzeptes und
- auf die ergänzende Ausstattung mit Laptopwagen und dergleichen ausgerichtet ist.

Der LfD unterstützt dieses Projekt, das bundesweit auch in datenschutzrechtlicher Hinsicht beispielgebend ist und deshalb Zug um Zug auch auf die Schulen erstreckt werden sollte, die bisher noch nicht in das Programm einbezogen sind. Dabei sollte das Augenmerk vor allem auch darauf gerichtet sein, dass die Ausstattung mit Laptops und sonstiger digitaler Technik einhergeht mit einer entsprechenden Intensivierung des Schulunterrichts. Der Erfolg des Programms steht und fällt am Ende mit den Fortschritten, die im Bereich der Datenschutzsensibilisierung erzielt werden.

3.1.5 Der Staat als Vorbild

Die Erziehung zu einem verantwortungsbewussten Umgang mit den eigenen Daten und den Daten von anderen wird im Übrigen nur erfolgreich sein, wenn der Staat mit gutem Beispiel vorangeht. Wie will er glaubhaft vor allem bei jungen Menschen für eine größere informationelle Sensibilität und Zurückhaltung werben, wenn er selbst mit seinen digitalen Großprojekten oft das Gegenteil tut. Gemeint sind die Vorratsdatenspeicherung (s.a. Tz. 7.2) und das ELENA-Verfahren (s.a. Tz. 2.2.7), SWIFT (s.a. Tz. 2.1.1) und vielleicht auch die elektronische Gesundheitskarte (s.a. Tz. 8.3), um nur vier Beispiele zu nennen. Wer selbst über das notwendige Maß hinaus Daten seiner Bürger speichert und verarbeitet, hat ein Glaubwürdigkeitsproblem, wenn er vor Google und anderen „Datenkraken“ warnen will. Dies gilt in noch stärkerem Umfange für die Wirtschaft. Die größten Datenskandale im Berichtszeitraum betrafen ihren Verantwortungsbereich. Vorbildhaftes Verhalten war hier oft die Ausnahme. Staat und Wirtschaft sollten sich deshalb bewusst sein, dass ein gefestigtes Datenschutzbewusstsein in der Bevölkerung ganz wesentlich davon abhängt, dass sie sich selbst datenschutzrechtlich verantwortlich und korrekt verhalten.

3.1.6 Bildungsanstrengungen des LfD

Den Datenschutzbeauftragten des Bundes und der Länder kommt eine Schlüsselfunktion bei der Förderung des Datenschutzbewusstseins der Bürger zu. Von ihnen wird es ein Stück weit abhängen, ob der Datenschutz in Staat und Gesellschaft als Bildungsaufgabe wahrgenommen wird. Die Dienststelle des rheinland-pfälzischen LfD hat sich diesem Thema in den vergangenen beiden Jahren mit Nachdruck gewidmet. Eine wichtige Rolle spielte dabei der vom LfD wahrgenommene Vorsitz der Arbeitsgruppe „Datenschutz und Bildung“, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingerichtet worden ist und im Berichtszeitraum wiederholt getagt hat. In der Arbeitsgruppe wurde regelmäßig über die jeweiligen Aktivitäten zur Förderung des Datenschutzbewusstseins in den einzelnen Bundesländern berichtet, so dass eine Vielzahl von Anregungen gesammelt werden konnte. Die entsprechende Vernetzung führte auch zu der Abrede, Informationsmaterial, Broschüren und Orientierungshilfen gegenseitig zu nutzen und mit dem Zusatz „empfohlen von der Arbeitsgruppe ´Datenschutz und Bildung` der Datenschutzbeauftragten des Bundes und der Länder“ zu veröffentlichen. In einer von der Arbeitsgruppe erstellten Link-Liste wurden empfehlenswerte Internet-Angebote zum Thema Medienkompetenz und Datenschutz zusammengefasst und im virtuellen Datenschutzbüro unter http://www.datenschutz.de/ an zentraler Stelle zum Abruf bereitgestellt.

Daneben spielte der Gedankenaustausch mit anderen Akteuren aus dem Bereich „Medienkompetenz“ eine wichtige Rolle. U.a. wurden Referenten von Institutionen (klicksafe.de, Landeszentrale für Medien und Kommunikation, jugendschutz.net, Fachstelle für Internationale Jugendarbeit der Bundesrepublik Deutschland e.V.), die auf Bundesebene aktiv sind, angehört und Möglichkeiten der Zusammenarbeit ausgelotet. Die Arbeitsgruppe beteiligte sich auch an der Erstellung eines Unterrichtsheftes zum Datenschutz, das von klicksafe.de herausgegeben wird. Unter dem Titel „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web“ wurde zum Safer Internet Day 2010 ein entsprechendes Zusatzmodul zu den Materialen „Knowhow für junge User“ vorgelegt.

Zu den Initiativen außerhalb der Arbeitsgruppe gehörten u.a. folgende Aktivitäten des LfD:

- Im vergangenen Jahr wurde bei den Bildungsministerien der Länder eine Umfrage durchgeführt, um festzustellen, welche Rolle der Datenschutz in den Schulen, in den Landeszentralen für politische Bildung und in den Landesmedienanstalten spielt.
- Des Weiteren wurde im Rahmen der Überarbeitung der Homepage des LfD eine eigene Jugendseite eingerichtet. Sie enthält wichtige Informationen rund um das Thema Datenschutz für Schüler, Eltern und Lehrer, u.a.:
  - die vorhandenen Unterrichtsmaterialien, Lehrbücher und Schülermappen zum Thema Datenschutz,
  - alle einschlägigen Materialien zu den sozialen Netzwerken, u.a. auch eine Orientierungshilfe zum Selbstdatenschutz für jugendliche Mitglieder dieser Plattformen und
  - die wichtigsten Videoclips, mit denen das Datenschutzbewusstsein von Jugendlichen angesprochen werden soll.
- Darüber hinaus wurden eine Reihe von Unterrichtsmaterialien und Handreichungen erstellt, z.T. gemeinsam mit anderen Organisationen, z.T. auch in eigener Verantwortung. Dazu zählt auch die Mitarbeit an einem Handbuch zum Datenschutz in der Schule mit dem Titel „Schule.Medien.Recht“, das vom rheinland-pfälzischen Bildungsministerium herausgegeben wird.
- Ergänzt wurden diese Materialien durch eine Vielzahl von Veranstaltungen, u.a. zum Europäischen Datenschutztag, die in den drei zurückliegenden Jahren jeweils mehr als 300 Besucher hatten.
- Auf Anregung des LfD wurde in dem vom Landtag und der Landeszentrale für politische Bildung durchgeführten Schüler- und Jugendwettbewerb 2009 auch ein datenschutzrechtliches Thema aufgenommen. Es lautete „Vorsicht und Rücksicht im digitalen Glashaus“. Eine ganze Reihe der prämierten Arbeiten betraf dieses Thema.
- Der LfD und seine Mitarbeiter haben viele Einladungen von Schüler- und Elternvertretungen erhalten und wahrgenommen, in denen über das datenschutzbewusste Verhalten im Internet referiert wurde. Auch mit Mitgliedern der Landesschülervertretungen wurde eine Reihe von Gesprächen geführt.

Die internationale Delphi-Studie prognostiziert, dass erst ab dem Jahre 2020 damit gerechnet werden könne, dass 75 Prozent der deutschen Bevölkerung im Umgang mit persönlichen Daten versiert und kompetent sei. Diese Prognose wird nicht eintreten. Wir werden einen viel längeren Atem brauchen und überhaupt nur dann erfolgreich sein, wenn wir unsere Bildungs- und Erziehungsanstrengungen erheblich ausweiten.

3.1.7 Fortbildungsaktivitäten des LfD

Wie schon seit Jahren engagierte sich der LfD auch in diesem Berichtszeitraum wieder umfassend in der Fortbildung. Der rege Zuspruch bei den durchgeführten Veranstaltungen sowie die steigende Zahl von Anfragen anderer Stellen zeigen, dass sowohl im öffentlichen als auch im nicht-öffentlichen Bereich ein immenser Fortbildungsbedarf im Lande besteht. Trotz deutlich zu geringer Ressourcen bemüht sich der LfD, den Weiterbildungswünschen der anfragenden Stellen so weit wie möglich zu entsprechen.

Einen Schwerpunkt der Fortbildungsaktivitäten bilden die regelmäßig über die Kommunalakademie Rheinland-Pfalz bzw. die Fachhochschule für öffentliche Verwaltung, das Institut für schulische Fortbildung und schulpsychologische Beratung und das Landesmedienzentrum angebotenen Veranstaltungen. Die Seminare zielen einerseits auf die Vermittlung von rechtlichen und technischen Grundlagenkenntnissen im Datenschutz, die beispielsweise für die Tätigkeit der behördlichen Datenschutzbeauftragten oder die Lehrer von Bedeutung sind. Andererseits werden in einzelnen Veranstaltungen auch bereichsspezifische datenschutzrechtliche Themen wie das Meldewesen, der Personaldatenschutz oder der sichere Einsatz der Informationstechnik behandelt.

Darüber hinaus führte der LfD im Berichtszeitraum zahlreiche Einzelveranstaltungen zur datenschutzrechtlichen Weiterbildung durch. Genannt seien in diesem Zusammenhang u.a. die Bereiche Medienkompetenz, Datenschutz im Internet, Datensicherheit, Identitätsmanagement, Kinder- und Jugendhilfe, Datenschutz bei den Sozialgerichten sowie die Novellierung des Bundesdatenschutzgesetzes. Daneben beteiligte sich der LfD an

diversen Foren, Informationsveranstaltungen und Podiumsdiskussionen, die von anderen privaten und öffentlichen Stellen organisiert wurden.

3.1.8 Lehrveranstaltungen des LfD

Versteht man Datenschutz als Bildungsaufgabe, geht es nicht nur um die Weiterbildung und darum, was die Schulen zur Datenschutzerziehung beitragen können. Auch die Hochschulen müssen in die Pflicht genommen werden. Der LfD hat versucht im Rahmen seiner Kapazitäten selbst einen Beitrag zur Datenschutzbildung im Hochschulbereich zu leisten. Im Rahmen eines Lehrauftrags der Deutschen Hochschule für Verwaltungswissenschaften in Speyer führt er – gemeinsam mit einem Mitarbeiter der Dienststelle – seit einigen Semestern eine Lehrveranstaltung zum Datenschutz in Gesetzgebung und Praxis durch. Das Interesse von Seiten der Studierenden ist groß. Nach sehr positiver Evaluation wird die Veranstaltung auch im kommenden Semester fortgeführt.

3.2 Videoüberwachung

3.2.1 Allgemeines

Zigtausende Videokameras werden zurzeit zur Überwachung von Supermärkten und Kaufhäusern, von Einkaufspassagen und Tankstellen, von Bahnhöfen und Sparkassen, aber auch von Schulen und Hochschulen, von Gerichten und städtischen Bussen in Rheinland-Pfalz eingesetzt. Sowohl nach § 34 LDSG als auch 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 schutzwürdigen Interessen der Betroffenen müssen durch entsprechende technische und organisatorische Maßnahmen ausreichend geschützt 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 „intelligenten Videoüberwachung“, die Gesichter erkennen und auf bestimmte „auffällige“ Bewegungen von „Zielpersonen“ reagieren kann. Insbesondere die datenmäßige Vernetzung der Kameras ist in Teilbereichen bereits machbar. 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 gegenzusteuern.

3.2.2 Umfrage zur Videoüberwachung

Grundlage einer Zurückdrängung der sich epidemisch ausbreitenden Videoüberwachungsanlagen muss zunächst eine Analyse der aktuellen Situation in Rheinland-Pfalz sein. Deswegen führte der LfD in den Jahren 2008 und 2009 eine breit angelegte, in ihrem Umfang bundesweit einmalige Umfrage zur Videoüberwachung durch die öffentliche Hand durch. Befragt wurden Ministerien, Schulen, Hochschulen, die Polizei, Gerichte, Justizvollzugsanstalten, die Kommunen, öffentliche Verkehrsbetriebe und Krankenhäuser. Hinzu kamen Stichproben im privaten Bereich, hier wurde die Videoüberwachung in Supermärkten und Kaufhäusern, in Einkaufspassagen, in Restaurants, Freizeitanlagen und Tankstellen, bei Ärzten, im Schienennahverkehr, in Industrie und privater Nachbarschaft unter die Lupe genommen.

Insgesamt wurden dabei 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.

Im Ergebnis wurden dabei mehr als 3.000 Kameras öffentlicher Stellen und mehr als 8.500 Kameras im privaten Bereich dokumentiert. Auf Basis der gut fundierten Schätzung, dass allenfalls jede zehnte Überwachungskamera sich in öffentlicher Hand befindet, ist daher für Rheinland-Pfalz von 30.000 bis 50.000 Überwachungskameras auszugehen.

Abgefragt wurden vom LfD zehn verschiedene Parameter der Videoüberwachung:

- überwachte Bereiche
- Kamerafunktionen (schwenkbar/zoombar/Audio/Bewegungsmelder/Attrappen)
- Monitoring oder Aufzeichnung
- Zeitraum der Videoüberwachung
- Gründe und Anlässe für die Videoüberwachung
- Kennzeichnung der Kamera
- Zugang zum Überwachungssystem
- Zugriff auf Speichermedien
- Dauer der Speicherung
- Einschätzung des Betreibers zum Erfolg der Videoüberwachung.

3.2.3 Ergebnisse der Umfrage

Die Ergebnisse dieser außergewöhnlich ertragreichen Umfrage können im Rahmen eines Tätigkeitsberichts nicht im Einzelnen vorgestellt werden. Deswegen bereitet der LfD für das Frühjahr 2010 eine umfangreiche Dokumentation der Umfrage vor.

An dieser Stelle sollen nur die wesentlichen Ergebnisse wiedergeben werden:

- Die häufigsten datenschutzrechtlichen Mängel bei der Videoüberwachung befinden sich im Bereich der Hinweispflichten (vgl. § 34 Abs. 2 LDSG und § 6b Abs. 2 BDSG). Häufig fehlen die 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.
- Als rechtlich problematisch hat sich der Einsatz von Videoüberwachungsattrappen durch die öffentliche Hand erwiesen. Zur Klärung der Zulässigkeit einer solchen „Schein-Videoüberwachung“ durch die öffentliche Hand regt der LfD eine Klarstellung im Landesdatenschutzgesetz an: Entweder sollte der Einsatz von Attrappen durch die öffentliche Hand generell verboten werden oder aber – unter Abwägung des Persönlichkeitsrechts der betroffenen Bürger sowie unter Beachtung des Rechtsstaatsprinzips – auf eine gesetzliche Grundlage gestellt werden.
- Regelmäßig fehlen Videoüberwachungskonzepte, welche vor Inbetriebnahme der Anlage verpflichtend zu erstellen sind (vgl. § 6b Abs. 1 Nr. 3, Abs. 3 BDSG; § 34 Abs. 3 LDSG). 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, so finden sich regelmäßig Verstöße gegen die Höchstspeicherdauer der Videoaufzeichnung. Eine Überschreitung der maximalen Grenze von 72 Stunden Speicherdauer führt regelmäßig zur Unverhältnismäßigkeit der Videoüberwachung.
- Eine Videoüberwachung von sog. „Tabubereichen“ ist immer rechtswidrig. Hierzu zählen Toilettenräume, Umkleidekabinen und Saunabereiche; Aufenthaltsräume, Kommunikationsstätten sowie die Gastronomie.
- Teil des Videoüberwachungskonzepts muss auch eine Zugriffsregelung sein, die verbindlich vorschreibt, aus welchen Anlässen welche Personen zum Zugriff auf die Speichermedien befugt sind. Um die Verletzung von Arbeitnehmerrechten zu verhindern, empfiehlt der LfD dringend, bei den Zugriffsregelungen die Betriebs- und Personalräte zu beteiligen.
- Die Zwecke der Videoüberwachung stimmen häufig nicht mit der Konzeption der Videoüberwachungsanlagen überein: Sicherheitsgewinne lassen sich regelmäßig nur durch sog. Monitoring, also durch die lückenlose Beobachtung von Livebildern durch eingriffsbereites Personal erzielen. Erfolgt die Videoüberwachung als reine Aufzeichnung, so sind hiermit keine Sicherheitsgewinne verbunden; allenfalls lassen sich (in einer begrenzten Zahl von Fällen) im Nachhinein Straftäter identifizieren. Hier gewinnt der LfD regelmäßig den Eindruck, dass an sich stimmige Videoüberwachungskonzepte aus Kostengründen soweit „minimiert“ werden, dass die Überwachungsmaßnahmen jede Erfolgschance einbüßen.
- Geraten Arbeitnehmer an ihrem Arbeitsplatz ständig oder häufig ins Blickfeld von Videoüberwachungsmaßnahmen, so können diese dadurch rechtswidrig werden, auch wenn sie gar nicht gegen die Arbeitnehmer gerichtet sind: Bereits die Möglichkeit einer Totalüberwachung durch den Arbeitgeber macht Videoüberwachung im Arbeitsverhältnis unzulässig. Hier sind die Arbeitnehmerrechte schon bei der Positionierung der Überwachungsanlagen zu berücksichtigen, zudem ist durch eine Betriebsvereinbarung die Nutzung der Videoüberwachungsanlagen zu Zwecken der Arbeitnehmerüberwachung auszuschließen.

Oft ist die Videoüberwachung sinnvoll, etwa in Parkhäusern, Supermärkten und wohl auch in Bahnhöfen. Allerdings breitet sie sich mittlerweile in rasantem Tempo und weitgehend unkontrolliert aus – auch in Bereichen, in denen man sich bisher unbeobachtet aufhalten konnte, wie etwa in Arztpraxen oder in der Gastronomie, im Schienennahverkehr und in der privaten Nachbarschaft.

Der LfD hat deshalb strengere gesetzliche Vorraussetzung für die Zulässigkeit der Videoüberwachung gefordert und unterbreitet hierzu dem Parlament entsprechende Vorschläge. Im staatlichen Bereich sollen den Behörden künftig Orientierungshilfen an die Hand gegeben werden, um eine rechtskonforme und zurückhaltende Anwendung der Videoüberwachung zu ermöglichen. Noch wichtiger ist es aber, dass die 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.

Die Beschwerden an den LfD richten sich nicht nur gegen Videoüberwachungsanlagen, die von Gewerbetreibenden, etwa im Einzelhandel, eingesetzt werden, sondern zunehmend auch gegen Videoüberwachungsanlagen, die von Privatpersonen betrieben werden. Dabei handelt es sich meist um Videokameras, die an Wohnhäusern angebracht und zumindest teilweise auf öffentliche Verkehrswege oder

Nachbargründstücke gerichtet sind. Ein Grund für die Zunahme derartiger Beschwerden dürfte darin liegen, dass die Videoüberwachung inzwischen zu einer „Jedermann-Technik“ geworden ist, die sich kostengünstig installieren und einfach betreiben lässt. Für die Aufsichtsbehörde bedeutet dies, dass durch die immer leichtere Verfügbarkeit dieser Technik die Zahl der Beschwerden aus dem Nachbarschaftsbereich spürbar zunimmt. Da der LfD jedoch ausschließlich für Videoüberwachungsanlagen zuständig ist, mit denen geschäftliche oder wirtschaftliche Zwecke verfolgt werden, müssen solche Fallgestaltungen an die Zivilgerichte überwiesen werden.

3.2.4 Webcam-Übertragungen

Immer häufiger nutzen öffentliche und private Stellen die Möglichkeit, mit Hilfe von webcams Liveaufnahmen ins Internet zu stellen. Damit sind besondere Probleme verbunden: Wie für alle ins Internet eingestellte Inhalte gilt generell, dass die Betreiber der webcams mit der Einspeisung der Bilder ins Netz unverzüglich die Kontrolle über die Inhalte und diese ihre Flüchtigkeit verlieren. Die Bildsequenzen können weltweit von Unbekannten nicht nur eingesehen, sondern auch gespeichert und reproduziert werden, dies ist mittlerweile selbst für Laien kein Problem mehr. Den Betroffenen ist es unmöglich zu erfahren, was mit diesen Aufnahmen geschieht. Gegen deren Missbrauch gibt es praktisch kein wirksames Mittel. Zahlreiche Beispiele auf einschlägigen Internetdiensten wie z. B. Youtube zeigen dies eindringlich. Durch Webcams ins Internet gestellte Videosequenzen beeinträchtigen die Betroffenen unabhängig vom Kontext der Aufzeichnung. Auch für die Betreiber von webcams können die Kameras zum unkalkulierbaren Risiko werden, z.B. wenn ein Betroffener seine persönlichkeitsrechtlichen Ansprüche zivilrechtlich geltend macht. Dies kann immer passieren, wenn Personen erkennbar sind, selbst wenn diese nur mit Zusatzwissen identifiziert werden können. Videoüberwachung per webcams ist daher nur in Ausnahmefällen gerechtfertigt. Die Veröffentlichung von per Webcam erstellten Personenaufnahmen im Internet ist in jedem Fall unzulässig. Beim Webcam-Einsatz ist daher vorrangig sicher zu stellen, dass einzelne Personen auf den Bildern nicht identifizierbar sind (s.a. 21. Tb. Tz. 18.1).

3.2.5 Schlussfolgerungen des LfD

Den Vorteilen der Videoüberwachung insbesondere bei der Diebstahlsvorbeugung und ihrem (beschränkten) Nutzen zur Aufklärung von Straftaten stehen 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 bloße Verlagerungseffekte auftreten, außerdem ist eine zweckmäßig durchgeführte Videoüberwachung technisch anspruchsvoll und äußerst kostspielig.

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 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 (§9 Abs. 5 LDSG, § 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 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 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 daher verhältnismäßig.
- Die Beweislast für die Zulässigkeit der Videoüberwachung liegt beim Betreiber!
- Die flächendeckende Videoüberwachung muss verhindert werden, da die Gefahr besteht, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.
- Mögliche Rechtsverletzungen können aus personellen Gründen nur unzureichend staatlich geahndet werden (Vollzugsdefizit). Effektiver Rechtsschutz der Betroffenen wird auch nicht durch die Zivilgerichte gewährt.

3.2.6 Nachtsichgeräte in Kinovorstellungen

Aufgrund von Pressemitteilungen aus anderen Bundesländern wurde der LfD darauf aufmerksam, dass bundesweit zahlreiche Kinobetreiber sich durch den oftmals heimlichen Einsatz von Nachtsichtgeräten gegen die Anfertigung von Raubkopien im Kinosaal schützen. Im Rahmen einer landesweiten Umfrage bei sämtlichen Kinobetreibern konnte der LfD ermitteln, dass etwa 20 Prozent aller Kinos diese Nachtsichtgeräte einsetzen. Solche optisch-elektronischen Überwachungen gem. § 6b BDSG weisen ein besonderes Gefährdungspotential auf, da sich die Kinobesucher häufig unbeobachtet fühlen und im abgedunkelten Kinosaal das Überwachungspersonal regelmäßig nicht erkennen können. Durch den Einsatz der Nachtsichtgeräte wird erheblich in schutzwürdige Interessen der Kinobesucher eingegriffen, da die Dunkelheit im Kino sowie die gemeinsame Blickrichtung sämtlicher Zuschauer den Eindruck von Privatheit und Intimität vermitteln.

Diese gravierende Problematik hat der LfD zum Anlass genommen, sich mit Vertretern der Filmindustrie, den Betreibern von Kinoketten sowie der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen an einen Tisch zu setzen und nach alternativen Schutzmaßnahmen zu suchen. Der LfD favorisiert hier insbesondere die offene Beobachtung des Publikums durch Kinopersonal ohne den Einsatz technischer Hilfsmittel sowie den Einsatz technischer Abwehrmaßnahmen zur Detektion von Kameraobjektiven ohne Beeinträchtigung der Persönlichkeitssphäre.

3.3 Soziale Online-Netzwerke

Soziale Netzwerke im Internet wie beispielsweise facebook, wer-kennt-wen, studiVZ, meinVZ, schülerVZ oder myspace ermöglichen in vielfältiger Weise eine Kommunikation und Vernetzung mit anderen Menschen im Internet. Diese Kommunikationsplattformen ermöglichen die Kontaktaufnahme mit Freunden, Bekannten und sonstigen Ansprechpartnern sowie einen Informations- und Meinungsaustausch über das Internet. Daneben gibt es auch geschäftliche Netzwerke, über die vorrangig berufliche Informationen ausgetauscht und beispielsweise neue Arbeitsplätze gesucht oder vermittelt werden. Soziale Netzwerke im Internet werden von Millionen von Menschen genutzt. So verfügt allein das soziale Netzwerk facebook weltweit über mehr als 200 Millionen Nutzer, darunter allein drei Millionen in Deutschland. Besonders große Netzwerke sind auch wer-kennt-wen mit 6,5 Millionen Mitgliedern sowie schülerVZ, meinVZ und studiVZ mit insgesamt 14 Millionen Mitgliedern.

Für das Jahr 2012 wird mit mehr als 22 Millionen Menschen in Deutschland gerechnet, die soziale Netzwerke im Internet nutzen. Die Nutzer von sozialen Netzwerken legen in diesem System regelmäßig ein persönliches Profil an, das sie den mit ihnen vernetzten Freunden und Bekannten oder auch der Allgemeinheit zur Einsicht oder zum Abruf über das Internet zur Verfügung stellen. In sozialen Netzwerken werden im Übrigen Nachrichten an andere Mitglieder versandt und von diesen empfangen sowie Foren zum Informations- und Meinungsaustausch eingerichtet. Die Finanzierung von sozialen Netzwerken erfolgt ganz überwiegend über Anzeigenerlöse, teilweise auch über Mitgliedsbeiträge. Darüber hinaus werden die in soziale Netzwerke eingestellten Informationen von den Diensteanbietern oder Dritten ausgewertet und für Werbezwecke kommerziell genutzt.

3.3.1 Datenschutzrisiken

Die Nutzer stellen regelmäßig eine Vielzahl von persönlichen Daten in das persönliche Profil ein, das im Rahmen des jeweiligen sozialen Netzwerks im Internet vorgehalten wird. Neben Angaben zum Wohnort, zum Alter und zum Beruf werden oftmals auch Fotos sowie sonstige Angaben über persönliche Interessen und Fähigkeiten oder auch zu persönlichen Ansichten und Erlebnissen in das Internet eingestellt. Die Veröffentlichung privater Informationen über die eigene Person in sozialen Netzwerken kann die Persönlichkeitsrechte der Betroffenen und deren Recht auf informationelle Selbstbestimmung insbesondere dann gefährden, wenn die im Internet abrufbaren Daten missbräuchlich für andere Zwecke genutzt werden.

Im August 2009 hat der LfD eine Broschüre mit Informationen und Tipps zum Schutz der Privatsphäre in sozialen Netzwerken im Internet herausgegeben. Dabei hat er folgende Risiken für Nutzer von sozialen Netzwerken im Internet aufgelistet:

- In das Internet eingestellte Informationen bleiben vielfach dauerhaft im Netz gespeichert, werden systematisch mit entsprechenden Programmen durchsucht und oftmals in andere Datenbestände kopiert, ohne dass Betroffene hiervon Kenntnis haben.
- In sozialen Netzwerke erstellte Profile und dort veröffentlichte Meinungsäußerungen, Einstellungen und Werturteile können entgegen dem Willen der Nutzer auch von zahlreichen Dritten gelesen werden wie beispielsweise Lehrern, Ausbildern oder Arbeitgebern.
- Die meisten Betreiber von sozialen Netzwerken erheben für deren Nutzung zwar keine Gebühren, zu ihrer Finanzierung sind sie aber auf Werbeeinnahmen angewiesen, die insbesondere auch aus der Vermarktung

der persönlichen Daten der Mitglieder der einzelnen sozialen Netzwerke erzielt werden.

3.3.2 Die Forderungen der obersten Aufsichtsbehörden

Bei ihrer Sitzung im April 2008 in Wiesbaden haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich deutlich gemacht, dass der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet eine zentrale Bedeutung zukomme. Im Einzelnen ist von den Datenschutzbehörden unter anderem gefordert worden, dass

- Anbieter sozialer Netzwerke die Nutzer umfassend über die Verarbeitung ihrer personenbezogenen Daten sowie ihre Wahl- und Gestaltungsmöglichkeiten unterrichten müssen,
- eine Verwendung von personenbezogenen Nutzungsdaten nach dem Telemediengesetz nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sei,
- es den Nutzern selbst überlassen bleiben müsse, welche Profil- und Nutzungsdaten für Zwecke einer Verwendung durch den Anbieter genutzt werden dürfen,
- Betroffenen nach dem Telemediengesetz ermöglicht werden müsse, sich in sozialen Netzwerken in anonymer Form oder unter einem Pseudonym bewegen zu können,
- von den Anbietern sozialer Netzwerke die notwendigen technischen und organisatorischen Maßnahmen getroffen werden müssten, um eine umfassende Datensicherheit und insbesondere zu gewährleisten, dass ein systematischer Export oder ein Herunterladen von Profildaten aus dem sozialen Netzwerk verhindert wird,
- datenschutzfreundliche Datenschutzstandardeinstellungen vorzunehmen seien, die die Privatsphäre der Nutzer möglichst umfassend schützen,
- die Auswertung der in sozialen Netzwerken gespeicherten personenbezogenen Daten mit Suchmaschinen nur mit ausdrücklicher Einwilligung der Betroffenen erfolgen dürfe, und
- die Nutzer in der Lage sein müssten, ihr Profil auf einfache Weise selbst löschen zu können und ggf. auch die Möglichkeit erhalten sollten, ein Verfallsdatum festlegen oder zumindest eine automatische Sperrung veranlassen zu können.

3.3.3 Forderungen des LfD

Mit den Gefährdungen der Persönlichkeitsrechte und der Privatsphäre von Betroffenen hat sich auch der LfD wiederholt befasst. Mit der bereits angesprochenen Informationsbroschüre zu sozialen Netzwerken, die im August 2009 veröffentlicht und allen rheinland-pfälzischen Schulen zugänglich gemacht wurde, wendet sich der LfD insbesondere an jugendliche Nutzer, aber auch an Eltern sowie an Lehrer mit dem Ziel, gemeinsam einen Beitrag zum Schutz der Privatsphäre für die Betroffenen zu leisten.

Zur Wahrung der Datenschutzrechte und der Privatsphäre empfiehlt der LfD unter anderem, dass die Nutzer von sozialen Netzwerken im Internet

- das ihren Interessen am ehesten entsprechende Netzwerk auswählen,
- persönliche Daten nach Möglichkeit nicht preisgeben und insbesondere Privatanschriften, Passwörter und Bankverbindungen nicht in ein öffentliches Netzwerk einstellen,
- Bilder, die in soziale Netzwerke eingestellt werden, sorgfältig auswählen und dabei darauf achten, dass auf einem Foto abgebildete weitere Personen hiermit einverstanden sind,
- die in den meisten sozialen Netzwerken bestehende Möglichkeit zur Änderung der Standardeinstellung nutzen und damit sicherstellen, dass der Name und das entsprechende Profil nicht weltweit über Suchmaschinen recherchierbar sind,
- für die einzelnen sozialen Netzwerke getrennte Profile anlegen und
- nach Beendigung der Mitgliedschaft in einem sozialen Netzwerk die Profildaten unverzüglich löschen.

Aus der Sicht des LfD kommt dem Schutz von Kindern und Jugendlichen in den sozialen Netzwerken eine besondere Bedeutung zu. Sie nutzen diese Netzwerke in einem erheblichen Umfang. Soweit Altersgrenzen durch die Anbieter festgelegt werden (bei schülerVZ 12 Jahre), werden diese nicht effizient kontrolliert; tatsächlich sind zahlreiche Kinder auch unter 12 Jahren in solchen Netzwerken aktiv, häufig ohne Kenntnis der Eltern. Im Privatrechtsverkehr dient die grundsätzlich vorgesehene Einbeziehung der Eltern in rechtsgeschäftliche Handlungen von Kindern und Jugendlichen dem Ziel des Minderjährigenschutzes (§§ 106 ff. BGB). Datenschutzrechtlich relevante Einwilligungen von Minderjährigen setzen deren Einsichtsfähigkeit voraus. Die Betreiber sozialer Netzwerke werden dieser Rechtslage aus der Sicht des LfD nicht gerecht. Die Mitwirkung der Eltern bei der Begründung von Nutzungsverhältnissen mit sozialen Netzwerken wird im Rahmen des Anmeldungsverfahrens häufig gar nicht angesprochen. Eine Information der Minderjährigen über die Gefahren der Nutzung solcher Netzwerke und die Möglichkeiten des Schutzes erfolgt nicht oder nicht altersgerecht. Es ist auch zu bemängeln, dass die Netzwerkbetreiber kein effizientes Altersverifikationssystem einsetzen. Für das Land Rheinland-Pfalz fördert der LfD Bemühungen, ein solches Altersverifikationssystem im

Zusammenwirken mit dem Betreiber des zentralen Einwohnerinformationssystem des Landes zu entwickeln.

Der LfD hat die Datenschutzaufsichtsbehörden der anderen Länder auf die Problematik des Minderjährigendatenschutzes in sozialen Netzwerken hingewiesen und Vorschläge zur gemeinsamen Beurteilung formuliert. Die Beratungen hierüber dauern noch an.

Die Tatsache, dass soziale Netzwerke technisch nicht genügend sicher sind, ist seit langem bekannt. So hat das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Darmstadt bereits am 23. September 2008 eine Studie zum Privatsphärenschutz von sieben Plattformen (myspace, facebook, studiVZ, wer-kennt-wen, lokalisten, XING und LinkedIn) veröffentlicht, in der unterschiedliche, zum Teil gravierende technische und strukturelle Mängel in Bezug auf die Datensicherheit festgestellt worden seien, die bislang keineswegs alle behoben worden sind. Allerdings ist auch zu konstatieren, dass bei Internet-Veröffentlichungen auf Plattformen, die der Kommunikation dienen, immer nur eine relativ, nie absolut und auf Dauer sichere Verarbeitung möglich sei. Auch dies muss den Nutzern durch Aufklärungsmaßnahmen vermittelt werden.

3.3.4 Sonstige Initiativen

Zu denen, die sich ebenfalls um Datenschutz in sozialen Netzwerken bemühen, gehört u.a. der Bundesverband der Verbraucherzentralen, der im Februar 2008 an die Betreiber von studiVZ und im Juli 2009 an eine Reihe weiterer Anbieter von sozialen Netzwerken Abmahnungen gerichtet und kritisiert hat, dass die Vertragsbedingungen einschließlich der vereinbarten Regelungen zum Datenschutz die Nutzer einseitig benachteiligen, da den Betreibern unverhältnismäßig weitgehende Rechte zur Verarbeitung personenbezogener Daten eingeräumt seien. Der Bundesverband der Verbraucherzentralen hat zwischenzeitlich bekannt gegeben, dass seinen Unterlassungsverlangen in Bezug auf verbraucherunfreundliche Regelungen in Allgemeinen Geschäftsbedingungen von myspace, facebook, studiVZ, wer-kennt-wen, lokalisten und XING Rechnung getragen wurde. Die Anbieter haben erklärt, die beanstandeten Geschäftsbedingungen künftig nicht mehr zu verwenden, in denen sie sich vor allem umfassende Datennutzungsrechte haben einräumen lassen.

Darüber hinaus hatten bereits im Februar 2009 mehrere große Betreiber von sozialen Netzwerken im Internet, darunter studiVZ, facebook und myspace gegenüber der EU-Kommission eine Selbstverpflichtungserklärung abgegeben, die auf eine umfassende Gewährleistung des Jugendschutzes abzielt. Die wichtigsten deutschen Netzwerke haben eine Selbstverpflichtung formuliert: Verhaltenskodex „Jugendschutz und Datenschutz in Social Communities“, unterzeichnet von den Netzbetreibern lokalisten, schülerVZ, studiVZ, meinVZ und werkennt-wen (Stand: 11. März 2009). Darin haben sich die Betreiber der sozialen Netzwerke verpflichtet, gezielte Suchanfragen nach Profilen Minderjähriger zukünftig zu unterbinden, den Profilzugriff nachhaltig einzuschränken und vorzusehen, dass den Nutzern altersgerechte Datenschutzeinstellungen vorgeschlagen werden.

Die Arbeitsgruppe Telekommunikation der Europäischen Datenschutzaufsichtsbehörden (Artikel 29-Gruppe) und die Internationale Konferenz der Datenschutzbeauftragten haben sich zum Datenschutz in sozialen Netzwerkdiensten – weitgehend inhaltsgleich – geäußert:

Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum“ – vom 3./4. März 2008, Rom (Italien) (im Internet abrufbar unter http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group).

Über die Umsetzung der im Februar 2009 zwischen der EU-Kommission und den Betreibern der sozialen Netzwerke im Internet vereinbarten Grundsätze zur Verbesserung des Jugendschutzes soll nach 18 Monaten, das heißt Ende 2010, erneut beraten und ein etwaiger Anpassungsbedarf geprüft werden.

Zusammenfassung und Ausblick

In den sozialen Netzwerken im Internet geben Millionen von Menschen jeden Tag eine Vielzahl von persönlichen Daten preis, ohne deren Nutzung und weitere Verwendung umfassend kontrollieren zu können. Insoweit können soziale Netzwerke im Internet die Rechte der Nutzer und insbesondere auch ihr Recht, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen, nachhaltig gefährden. Aus diesem Grund ist es notwendig, dass für die sozialen Netzwerke im Internet umfassende Sicherheitskonzepte entwickelt werden, die sowohl den Erfordernissen der Datensicherheit als auch dem Schutz der Persönlichkeitsrechte und der Privatsphäre der Betroffenen umfassend Rechnung tragen.
Der technische Datenschutz ist durch die Anbieter zu verbessern; die Nutzer müssen in die Lage versetzt werden, Zugriffsschranken leicht und unkompliziert einrichten zu können (als Maßnahme des „Selbstdatenschutzes“); die Angebote sind insgesamt datenschutzfreundlich auszugestalten; die Anbieter müssen – soweit Selbstverpflichtungen nicht greifen – gesetzlich zur Beachtung von Mindeststandards verpflichtet werden.

3.4 Vernetzter Datenschutz

3.4.1 Konferenz der Datenschutzbeauftragten und Düsseldorfer Kreis

Seit über 30 Jahren kommen die Datenschutzbeauftragten des Bundes und der Länder zu gemeinsamen Konferenzen zusammen, zweimal im Jahr unter wechselndem Vorsitz, um aktuelle datenschutzrechtliche Fragen zu erörtern und die oft von Arbeitskreisen vorbereiteten Arbeitsergebnisse in Beschlüssen und Entschließungen zusammenzufassen. Die Konferenz und ihre Gremien bilden eine Plattform für den Austausch datenschutzrelevanter Informationen und ermöglichen eine gewisse Arbeitsteilung, ohne die die Querschnittsmaterie „Datenschutz“ nicht sinnvoll und effektiv zu bewältigen wäre.

Da nicht alle Datenschutzbeauftragte auch für den nicht-öffentlichen Bereich zuständig sind, beschränkt sich die Konferenz in der Regel auf Fragen des staatlichen Datenschutzes. Der Datenschutz im nicht-öffentlichen Bereich wird vom sog. Düsseldorfer Kreis behandelt. Dies ist der Zusammenschluss der Aufsichtsbehörden, die den Datenschutz im nicht-öffentlichen Bereich zu überwachen haben. Er hat eine ähnlich lange Tradition wie die Konferenz der Datenschutzbeauftragten und wird – wie diese – von einer Reihe von ständigen Arbeitsgruppen unterstützt.

Der LfD ist mit seinen Mitarbeitern in den meisten Arbeitskreisen und Arbeitsgruppen vertreten, zum Teil tagen diese unter rheinland-pfälzischer Federführung. Die damit einhergehende Arbeitsbelastung ist gerade für eine kleine Dienststelle wie die des rheinland-pfälzischen LfD groß. Trotzdem überwiegen die Vorteile, wobei allerdings eine stärkere Ausrichtung auf landesspezifische Themenstellungen anzustreben ist.

3.4.2 Behördliche Datenschutzbeauftragte

Bereits im letzten Tätigkeitsbericht war darauf hingewiesen worden, dass der LfD damit begonnen habe, die große Zahl der behördlichen Datenschutzbeauftragten zu einem Netzwerk zusammenzufassen, um ihnen eine effektivere Arbeit in ihrem Verantwortungsbereich zu ermöglichen (s.a. 21. Tb., Tz. 8.1 und Tz. 25). Dies ist im Berichtszeitraum auch geschehen.

In den beiden zurückliegenden Jahren fanden jeweils Sitzungen mit den Datenschutzbeauftragten der obersten Landesbehörden und Tagungen mit den Datenschutzbeauftragten der Kommunen statt. Die Treffen mit den kommunalen Datenschutzbeauftragten werden auch von den kommunalen Spitzenverbänden gefördert und begleitet. In einem Kreis von jeweils rund 100 Personen konnten so die gegenseitigen Kontakte ausgebaut und praxisrelevante Datenschutzfragen erörtert werden.

Gegenwärtig laufen die Vorbereitungen für entsprechende Treffen mit den Datenschutzbeauftragten der Justiz und den Datenschutzbeauftragten der Hochschulen. Auch diese Treffen sollen verstetigt werden.

Mit den schulischen Datenschutzbeauftragten steht der LfD ohnehin in einem regelmäßigen Kontakt. Dieser wird über eine E-Mail-Liste aufrechterhalten, in der die Namen von 1.500 schulischen Datenschutzbeauftragten verzeichnet sind. Über diese – mit Unterstützung des Bildungsministeriums erstellte – Verteilerliste ist es möglich, die schulischen Datenschutzbeauftragten in konkrete Projekte einzubinden – etwa die Bestandsaufnahme der Videoüberwachung in den Schulen –, sie zu Informationsveranstaltungen des LfD einzuladen und mit notwendigem Informationsmaterial zu versorgen.

Die Pflege dieser Netzwerke führt im Übrigen – ganz unabhängig von Tagungen und Veranstaltungen – zu einem regen Meinungsaustausch in der datenschutzrechtlichen Alltagsarbeit. Dieser könnte noch intensiver sein, wenn den behördlichen Datenschutzbeauftragten für die Wahrnehmung ihres verantwortungsvollen Amtes mehr Zeit eingeräumt und mehr Aufmerksamkeit entgegengebracht würde. Die behördlichen Datenschutzbeauftragten sind die Datenschutzfachkräfte vor Ort. Von ihrem Einsatz hängt das Datenschutzniveau im Land maßgeblich ab. Dass es in den zurückliegenden Jahren stetig gewachsen ist, ist auch ihr Verdienst.

Allerdings ist dies keine Selbstverständlichkeit. Gerade die zunehmende Entwicklung der Informations- und Kommunikationstechnologien macht es zwingend notwendig, die Aus- und Fortbildung der behördlichen Datenschutzbeauftragten zu intensivieren. Das sollte auch im Landesdatenschutzgesetz ausdrücklich vorgeschrieben werden (s.a. Tz. 2.3.2).

3.4.3 Betriebliche Datenschutzbeauftragte

So wie nach dem Landesdatenschutzgesetz die Landesbehörden behördliche Datenschutzbeauftragte einzusetzen haben, sind nach dem Bundesdatenschutzgesetz in den Betrieben grundsätzlich betriebliche Datenschutzbeauftragte zu bestellen. Dies geschieht aber offenbar nur zum Teil. Schätzungen zufolge dürften allenfalls 50 Prozent der Betriebe, die einen Datenschutzbeauftragten zu bestellen haben, über einen solchen verfügen.

Der Aufbau eines Netzwerkes ist in diesem Bereich ungleich schwieriger als im staatlichen Bereich. Das ist

darauf zurückzuführen, dass die betrieblichen Datenschutzbeauftragten dem LfD in der Regel nicht bekannt sind und weil die große Zahl der in Betracht kommenden Personen eine Netzwerkarbeit kaum möglicht macht. Immerhin hatte der LfD die sog. Erfahrungsaustauschkreise, in denen sich betriebliche Datenschutzbeauftragte selbst organisiert haben, zu einem gemeinsamen Treffen nach Mainz eingeladen und auch mit ihnen eine regelmäßige Zusammenarbeit vereinbart.

Darüber hinaus gibt es intensive Kontakte mit betrieblichen Datenschutzbeauftragten der großen rheinland-pfälzischen Unternehmen, insbesondere mit den betrieblichen Datenschutzbeauftragten der BASF, von Boehringer Ingelheim, und der Debeka. Die BASF organisiert regelmäßige Jahrestreffen der betrieblichen Datenschutzbeauftragten der BASF Gruppengesellschaften, zu denen auch der LfD eingeladen wird. Diese ganztägigen Veranstaltungen sind Ausdruck einer erfreulichen Datenschutzkultur und geben dem LfD im Übrigen Gelegenheit, für Datenschutz und Datensicherheit zu werben. Zugleich sensibilisieren sie ihn aber auch für die besonderen Belange der Wirtschaft. Deshalb liegt der Ausbau dieser Kontakte ganz im Interesse des LfD.

3.4.4 Wissenschaftsrunde

Im September 2009 traf sich erstmals beim LfD die von ihm ins Leben gerufene „Wissenschaftsrunde“. Ziel dieses Kreises ist es, den LfD in seiner Arbeit zu begleiten und mit ihm aktuelle (verfassungs)rechtliche und technische Fragestellungen zum Datenschutzrecht kontinuierlich zu erörtern. Hierzu hat der LfD einen Kreis junger Rechtswissenschaftler – Professoren, Habilitanden und Richter – versammelt, die ihn bei mehreren Treffen im Jahr durch Anregungen, Stellungnahmen und Kritik der Datenschutzpraxis unterstützen. Bei den ersten Treffen stehen die europäische Rahmensetzung für das nationale Datenschutzrecht sowie aktuelle Modernisierungsansätze für das Bundes- bzw. Landesdatenschutzgesetz im Mittelpunkt der Diskussion.

3.5 Öffentlichkeitsarbeit

Der LfD hat nach dem Landesdatenschutzgesetz in erster Linie eine Kontrollaufgabe. Er hat – wie sich aus § 29 Abs. 1 LDSG ergibt – aber auch die Aufgabe, die Bürger zu beraten. Dies geschieht im Zusammenhang mit Eingaben, aber auch dann, wenn die Öffentlichkeit über allgemeine Datenschutzentwicklungen und konkrete Datenschutzvorfälle informiert wird. Beides hat im Berichtszeitraum zugenommen: Die Zahl der Eingaben, aber auch die Maßnahmen der Öffentlichkeitsarbeit.

Der LfD bemisst der Öffentlichkeitsarbeit grundsätzliche Bedeutung zu. Sie erwächst letztlich aus dem im Demokratieprinzip enthaltenen Grundsatz der Transparenz und Publizität staatlichen Handelns. Ganz wesentlich zielt sie darauf, die Bürger zum Selbstdatenschutz zu bewegen. Zugleich trägt sie zu einer lebendigen Datenschutzkultur bei, die unverzichtbare Voraussetzungen für einen effektiven Datenschutz ist.

3.5.1 Pressearbeit

Das gestiegene Interesse am Datenschutz kam im Berichtszeitraum auch darin zum Ausdruck, dass die Anfragen der Medien, zu aktuellen Datenschutzfragen Stellung zu nehmen, signifikant zugenommen haben und zwar unabhängig davon, ob es sich um Datenschutzangelegenheiten aus Rheinland-Pfalz oder um bundes- oder europarechtliche Datenschutzprobleme handelte. Der LfD gilt als unabhängiger Sachverständiger für den Datenschutz, auch wenn es um Angelegenheiten geht, für die seine Dienststelle nicht zuständig ist. Der LfD seinerseits hat auf die wachsende mediale Nachfrage mit Pressekonferenzen und einer großen Zahl von Presseerklärungen reagiert. Im Berichtszeitraum wurden mehr Presseerklärungen verfasst als in den zehn Jahren zuvor.

3.5.2 Homepage

Die Presseerklärungen sind Teil der von Mitarbeitern der Dienststelle neu gestalteten Homepage des LfD (http://www.datenschutz.rlp.de/), in der aktuelle Informationen ebenso abgerufen werden können wie Handreichungen und Orientierungshilfen zu grundsätzlichen Datenschutzfragen. Im Übrigen enthält die Homepage eine eigene Jugendseite mit datenschutzrelevanten Informationen für Kinder und Jugendliche (s.a. Tz. 3.1.6). Die neue Homepage des LfD erfreut sich offenbar großer Beliebtheit. In der Liste der meistbesuchten Datenschutzwebseiten nimmt sie regelmäßig einen Spitzenplatz ein.

3.5.3 Informationsveranstaltungen

Der LfD ist aber nicht nur in der virtuellen Öffentlichkeit gut platziert. Mit besonderem Nachdruck hat er eine ganze Reihe von öffentlichen Informationsveranstaltungen durchgeführt. Die Besucherzahlen zeigen, dass diese Veranstaltungen – und damit das Datenschutzthema – auf großes Interesse stoßen. Mit jeweils über 300 Besuchern waren vor allem die Veranstaltungen, die zum Europäischen Datenschutztag durchgeführt wurden, besonders gut besucht. Ein großer Teil der Veranstaltungen wurde in Kooperation mit anderen Einrichtungen durchgeführt, was nicht nur in finanzieller Hinsicht von Vorteil war, sondern auch dem o.g. Netzwerkgedanken (s.a. Tz. 3.4) Rechnung trug.

Folgende Veranstaltungen wurden im Berichtszeitraum durchgeführt:

3. Dezember 2007: „Glücklich ist, wer vergisst …“

Gemeinsam mit der Friedrich-Ebert-Stiftung veranstaltete der LfD ein Symposium über die Bedeutung des Vergessens und das ewige Online-Gedächtnis des Internet, zu dem ca. 160 Gäste erschienen waren, um mit dem Gedächtnisforscher Prof. Markowitsch von der Universität Bielefeld und dem Informatiker Prof. Mayer-Schönberger von der Harvard Universität zu diskutieren.

28. Januar 2008: „Denn sie wissen nicht, was sie tun!“

Etwa 300 Lehrer, Eltern und Schüler versammelten sich in der Mainzer Akademie der Wissenschaften und der Literatur, um anlässlich des 2. Europäischen Datenschutztages mehr über den Datenschutz in der Online-Generation zu erfahren. Die Veranstaltung wurde gemeinsam mit dem Ministerium für Bildung, Wissenschaft, Jugend und Kultur durchgeführt.

23. April 2008: „Schutz der Privatheit – Informationsgesellschaft ohne Tabu?“

In der Mainzer Akademie der Wissenschaften und der Literatur diskutierte Justizminister Bamberger gemeinsam mit dem LfD und weiteren Experten über den Schutz der Privatsphäre. Auf dem Podium referierten und diskutierten die Richterin am Bundesverfassungsgericht Dr. Christine Hohmann-Dennhardt, die Philosophiedozentin Prof. Dr. Beate Rössler von der Universität Amsterdam, der Medienwissenschaftler Dr. Bernd Flessner von der Universität Erlangen-Nürnberg und Andreas Bogk vom Chaos Computer Club. Wiederum waren rund 300 Gäste erschienen.

6. Mai 2008: „Schutz der Privatheit – Informationsgesellschaft ohne Tabu?“

Auch in der Landesvertretung in Berlin thematisierten der LfD und der Justizminister bei einer gemeinsamen Podiumsveranstaltung die Gefährdungen der Privatsphäre durch Staat und Wirtschaft. Auch hier war die Resonanz mit über 200 Gästen groß.

25. August 2008: Verbraucherdialog zum Thema „RFID“

Auf Einladung von Verbraucherschutzministerin Margit Conrad und des LfD diskutierten Experten aus Unternehmen, Branchen- und Verbraucherverbänden, der Wissenschaft sowie verschiedener rheinland-pfälzischer Ministerien über die Auswirkungen von RFID auf die Verbraucher.

3. November 2008: „Vernachlässigtes Kapital – Datenschutz in der Privatwirtschaft“

Auf Einladung des LfD waren über 200 Gäste aus der Wirtschaft, der Landesverwaltung und der Justiz in den Plenarsaal des rheinland-pfälzischen Landtags gekommen, um sich über die aktuellen Probleme des Datenschutzes in der Privatwirtschaft zu informieren. Nach einem einführenden Referat der seinerzeitigen Bundesjustizministerin Brigitte Zypries diskutierten auf dem Podium unter Leitung von Bernhard Töpper (ZDF) u.a. Rainer Neumann, Vorstandsvorsitzender der Schufa, Prof. August-Wilhelm Scheer, Präsident des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (BITKOM), Günter Wallraff und die Staatsministerin für Umwelt, Forsten und Verbraucherschutz, Frau Margit Conrad.

1. Dezember 2008: Öffentliche Verleihung des Wissenschaftspreises

Im Landtagsgebäude wurde erstmals der Wissenschaftspreis des LfD an junge Wissenschaftler des Landes verliehen. Die Preisrede hielt in Anwesenheit von rund 100 Gästen Frau Staatsministerin Margit Conrad.

15. Dezember 2008: „25 Jahre moderner Datenschutz“

Auf Anregung des LfD und in Kooperation mit seiner Dienststelle fand darüber hinaus am 15. Dezember 2008 in Karlsruhe am 25. Jahrestag der Volkszählungsentscheidung eine Veranstaltung zum Thema „25 Jahre moderner Datenschutz“ statt. Die Festrede hielt der Präsident des Bundesverfassungsgerichts Prof. Hans-Jürgen Papier.

28. Januar 2009: „Ach wie gut, dass jeder weiß …“

In einem gemeinsamen Symposium von ZDF und LfD ging es anlässlich des 3. Europäischen Datenschutztags um den „digitalen Exhibitionismus“ im Internet. Hauptreferenten waren Andreas Poller vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Darmstadt, Dr. Jan Schmidt vom Hans-Bredow-Institut für Medienforschung und Prof. Dr. Alexander Roßnagel, Vizepräsident der Universität Kassel. Wieder waren weit über 300 Besucher anwesend.

18. Mai 2009: „Nackt im Netz? – Datenouting in schülerVZ, wer-kennt-wen und Co“

Videopräsentationen und angeleitete Internet-Recherchen im Landtagsgebäude erreichten anlässlich des Tags der offenen Tür im Rahmen des Verfassungsfestes des Landes eine Vielzahl von interessierten Besuchern.

8. Juli 2009: „Datenschutz ist Verbraucherschutz“

Rund 200 Gäste fanden sich im Landesmuseum in Mainz auf Einladung von Verbraucherschutzministerin Margit Conrad und des LfD ein. Datenschutz beim Adresshandel, beim Scoring, bei Kundenkarten und im Internet sowie das Vertrauen zwischen Verbrauchern und Unternehmern waren die Themen der ganztätigen Veranstaltung. Renate Schmidt, Mitglied und frühere Vizepräsidentin des Deutschen Bundestags, schilderte außerdem ihre Erfahrungen als Ombudsfrau für den Datenschutz bei Vodafone.

21. September 2009: Vorstellung des LDSG-Kommentars

Im Juli 2009 war die von Mitarbeitern des LfD erstellte aktualisierte Fassung des Kommentars zum Landesdatenschutzgesetz erschienen. Gemeinsam mit dem Verlag hatte der LfD die Neuauflage zum Anlass genommen, den Kommentar im Rahmen einer Veranstaltung der interessierten Öffentlichkeit vorzustellen. In Anwesenheit der Spitzen der rheinland-pfälzischen Justiz hielt Justizminister Dr. Bamberger das Eingangsreferat zum Thema „Persönlichkeitsrechte im Internetzeitalter“. Der hessische Landesbeauftragte für den Datenschutz, Prof. Dr. Michael Ronellenfitsch, würdigte den Kommentar.

Insgesamt waren über 2.300 Besucher zu diesen Veranstaltungen gekommen, über die in der Regel auch in den Medien berichtet wurde.

3.5.4 Publikationen

Faltblatt „Datenschutz in Rheinland-Pfalz“

Das Faltblatt soll den Bürgern Grundinformationen zum Datenschutz geben. Mit den Fragestellungen

- Worum geht es bei dem Datenschutz?
- Wer schützt ihre Daten?
- Welche Datenschutzrechte haben Sie?
- Wer ist Ansprechpartner in Rheinland-Pfalz?
- Was können wir für Sie tun?

soll die Broschüre dazu beitragen, dass Bürger sorgsam mit ihren Daten umgehen und darauf achten, was mit ihnen geschieht.

Broschüre „Der betriebliche Datenschutzbeauftragte“

Mit der Übertragung der Zuständigkeit für den privaten Datenschutz will der LfD auch den Unternehmen als Gesprächspartner und Ratgeber zur Verfügung stehen. Als Bindeglied zwischen den Unternehmen und dem LfD sind dabei die betrieblichen Datenschutzbeauftragten von besonderer Bedeutung. Über ihre Aufgabe und ihre Stellung unterrichtet die Broschüre „Der betriebliche Datenschutzbeauftragte“. Sie wendet sich an die Unternehmensleitungen, an die betrieblichen Datenschutzbeauftragten selbst, aber auch an alle, die sich über die Funktion des betrieblichen Datenschutzbeauftragten informieren wollen.

Broschüre „Die schöne neue Welt von SchülerVZ, WKW und Co“

Diese Broschüre gibt Tipps und Hinweise zum verantwortungsvollen Umgang mit den eigenen Daten und dem respektvollem Umgang mit Daten anderer in den sozialen Netzwerken. Sie ist in einer Auflage von 20.000 Exemplaren gedruckt worden und steht allen Schulen des Landes zur Verfügung.

4. Medien und Telekommunikation

4.1 Google Street View

Google Incorporated ist das weltweit führende im Internet tätige Unternehmen mit Sitz in Kalifornien/USA, dessen Suchmaschine Eingang in die Umgangssprache gefunden hat; weitere Schwerpunkte liegen in umfangreichen Service-Angeboten für Nutzer des World Wide Web. Zu diesen Angeboten gehört das Bereithalten einer kartographischen Darstellung der Erdoberfläche, insbesondere unter Einbeziehung der Pläne von Städten und Gemeinden (Google Maps). In den USA und in anderen Ländern (z.B. England und Frankreich) wurde dieses Angebot um eine Möglichkeit erweitert, von den Straßenplänen auf fotografische Straßenansichten zu springen. Diese Erweiterung nennt Google „Street View“. Im Herbst 2008 wurde bekannt, dass Google plane, diese Funktion auch für deutsche Städte und Gemeinden anzubieten. Seit dieser Zeit fahren Kamerawagen von Google durch deutsche Städte und Dörfer und fotografieren von einem zwei Meter hohen Mast aus die sich von dort zeigenden Häuser unter Einschluss parkender Fahrzeuge und sich im Straßenraum aufhaltender Passanten.

In diesem Zusammenhang haben sich zahlreiche Datenschutzfragen gestellt. Viele Menschen waren und sind der Ansicht, weder sie selbst noch die von ihnen bewohnten (bzw. die ihnen gehörenden) Häuser dürften ohne ihre Einwilligung fotografiert und ins Internet gestellt werden. Die sich hier stellenden Fragen sind kontrovers beurteilt worden.

4.1.1 Zuständigkeitsfragen

Zunächst ist von Bedeutung, welche Datenschutzaufsichtsbehörde sich um die Aktivitäten dieses US-amerikanischen Unternehmens auf deutschem Boden zu kümmern hat. Nach den Regelungen des Bundesdatenschutzgesetzes (§ 1 Abs. 5) findet dieses Gesetz Anwendung, sofern eine datenverarbeitende Stelle, die außerhalb der Europäischen Union belegen ist, personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt. Die deutsche Aufsichtsbehörde kontrolliert in diesen Fällen die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Da die Datenerhebung durch Google überall in Deutschland erfolgt ist, sind 16 Datenschutzbehörden zuständig. Um die Verhandlungen mit Google zu erleichtern, haben die deutschen Datenschutzaufsichtsbehörden vereinbart, wegen des Hamburger Sitzes von Google Deutschland die Verhandlungsführung auf den hamburgischen Datenschutzbeauftragten zu übertragen.

4.1.2 Materielle Rechtsfragen

Der schleswig-holsteinische Datenschutzbeauftragte, der sich als Erster der Angelegenheit angenommen hatte, kam zunächst in seinem Gutachten vom 30. September 2008 zu dem Ergebnis, dass jedenfalls die Internet-Veröffentlichung solcher Bilder ohne Einwilligung unzulässig sei (s. http://www.datenschutzzentrum.de/geodaten/20080930-googlestreetview-bewertung.htm). Es wird aber auch die Auffassung vertreten, eine Abwägung des Informationsfreiheitsrechtes mit den schutzwürdigen Belangen der Bewohner ergebe, dass die öffentlichen Straßenansichten auch im Internet gezeigt werden dürften. Erforderlich sei eine ausreichende Anonymisierung von abgebildeten Personen und Kfz-Kennzeichen. Beispielsweise vertritt der wissenschaftliche Dienst des schleswig-holsteinischen Landtags diese Ansicht (Gutachten vom 4. Februar 2009, http://www.landtag.ltsh.de/infothek/wahl16/umdrucke/3900/umdruck-16-3924.pdf).

4.1.3 Der gemeinsame Standpunkt der deutschen Datenschutzaufsichtsbehörden

Das Gremium der deutschen Datenschutzaufsichtsbehörden (der „Düsseldorfer Kreis“) hat in Kenntnis dieser unterschiedlichen Auffassungen am 14. November 2008 unter der Überschrift „Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet“ folgenden Beschluss gefasst:

„Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die

Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen."

Damit hat dieses Gremium die grundsätzliche Zulässigkeit solcher Internet-Veröffentlichungen akzeptiert, sie aber unter den Vorbehalt begleitender Datenschutzmaßnahmen gestellt.

4.1.4 Stand der Vereinbarungen mit „Google"

Auf dieser Grundlage hat der hamburgische Landesdatenschutzbeauftragte Vereinbarungen mit Google getroffen. Google hat verbindlich zugesichert,

- eine Technologie zur Verschleierung von Gesichtern vor der Veröffentlichung von derartigen Aufnahmen einzusetzen;
- Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten und derartige Widersprüche zu bearbeiten;
- dass Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern in einer einfachen Form berücksichtigt werden mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs;
- die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben;
- dass die Widerspruchsmöglichkeit auch nach der Veröffentlichung noch besteht;
- die Löschung/Unkenntlichmachung der Rohdaten so schnell wie möglich vorzunehmen;
- die Löschung oder Unkenntlichmachung der Rohdaten von Personen, Kfz und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind. Die Löschung oder Unkenntlichmachung dieser Daten in den Rohdaten wird bereits vor der Veröffentlichung vorgenommen, wenn der Widerspruch bis zu einem Monat vor Veröffentlichung der Bilder bei Google eingeht. Später oder auch nach Veröffentlichung eingehende Widersprüche führen zu einer Löschung in den Rohdaten binnen zwei Monaten;
- eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen für Google Street View vorzulegen. Insbesondere gehört hierzu auch eine deutliche Beschreibung des Umgangs mit den Widersprechendendaten von der Entgegennahme des Widerspruchs bis zur endgültigen Löschung bzw. Unkenntlichmachung.

Widerspruch kann eingelegt werden im Internet unter http://maps.google.de/intl/de/help/maps/streetview/faq.html oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg. Der Link mit dem Text: „FAQ Street View (inkl. Widerspruchsmöglichkeiten)" ist nunmehr direkt auf der ersten Seite der Hilfeseiten für Google Maps Deutschland erreichbar. Diese Hilfeseiten erreicht jeder Nutzer direkt aus dem Produkt Google Maps Deutschland, wenn er oben rechts den Link „Hilfe" anklickt.

4.1.5 Aktivitäten des LfD

Der LfD hat sich von Anfang an um eine intensive Information der Bevölkerung bemüht. In Presseerklärungen und in seinem Internet-Angebot hat er auf das Vorhaben und die Möglichkeiten der Bewohner, sich dagegen zu wehren, hingewiesen (s. das Muster eines Widerspruchsschreibens unter http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2009061701). Eine große Zahl von Bürgern hat auch die Möglichkeit genutzt, sich dieses Musterschreiben per Post zusenden zu lassen. Dabei wurde deutlich, dass die Datenschutzanstrengungen sich nicht nur auf die Bürger beschränken dürfen, die über einen Internet-Zugang verfügen.

In folgenden Fragen hat der LfD sich an den hamburgischen Datenschutzbeauftragten gewandt und um Klärung bzw. Unterstützung gebeten:

- Google hat auf seiner Website nicht immer zeitnah und korrekt darüber informiert, wann und wo seine Kamerawagen unterwegs sind. Dies ist erst auf dem Wege einer Intervention über den hamburgischen Datenschutzbeauftragten verbessert worden, kann aber noch nicht als zufriedenstellend bezeichnet werden.
- Fraglich ist, ob Körperschaften (beispielsweise Gemeinden) bezüglich ihrer eigenen Gebäude widerspruchsbefugt sind. Dies hat der hamburgische Datenschutzbeauftragte unter Hinweis auf den Charakter der Vereinbarung als allein dem Schutz natürlicher Personen dienend verneint.
- In den Rückmeldungen auf Widersprüche kündigt Google an, dass eine Löschung von Bildern erst aufgrund weiterer Aktivitäten der Widersprechenden – deren Art und Umfang noch unklar ist – erfolgen soll. Dies hat der LfD problematisiert; er hält die Forderung

nach solchen weiteren Handlungen der Widersprechenden nur dann für zulässig, wenn sich aus den Widersprüchen selbst Unklarheiten bezüglich des gemeinten Objekts (der betroffenen Liegenschaft) ergeben. Der hamburgische Kollege hat darauf hingewiesen, dass zunächst abgewartet werden solle, welche Anforderungen Google konkret erheben würde.

4.1.6 Aktivitäten von Landtag und Landesregierung

Der Landtag hat sich in seiner Sitzung vom 25. Juni 2009 mit Google Street View befasst; auch das Kabinett hat sich dieser Thematik angenommen. Im August 2009 hat die Landesregierung beschlossen, ein externes Gutachten in Auftrag zu geben. Es soll untersuchen, wie sich die Zulässigkeit des Vorgehens von Google Street View nach geltendem Recht beurteilt, insbesondere unter Berücksichtigung datenschutzrechtlicher Bestimmungen, des Rechts am eigenen Bild, des allgemeinen Persönlichkeitsrechts und des Schutzes der Privatsphäre. Mit der Erstellung des Gutachtens sind Professor Thomas Dreier und Professorin Indra Spiecker vom Institut für Informations- und Wirtschaftsrecht der Universität Karlsruhe beauftragt worden. Der Landesjustizminister unterstrich anlässlich der öffentlichen Bekanntgabe dieses Vorhabens, dass die vollständige Erfassung des Wohnumfeldes von Bürgern und die weltweite Verbreitung über das Internet von vielen als persönliche Beeinträchtigung und als Einschränkung des Rechts auf informationelle Selbstbestimmung empfunden werde. Deshalb müssten die Möglichkeiten einer weiteren Stärkung der Rechte der Betroffenen geprüft werden. Die Privatsphäre der Bürger müsse auch von Internet-Diensten respektiert werden. Der LfD teilt diese Auffassung und ermutigt die Landesregierung, sich um eine Novellierung der derzeit unzureichenden und nicht genügend klaren Rechtsnormen zu bemühen.

4.1.7 Fazit

Der LfD vertritt die Auffassung, dass die bisher mit Google getroffenen Absprachen nur einen ersten Schritt in der Auseinandersetzung mit diesem Projekt darstellen dürfen. Dabei kann es aber nicht sein Bewenden haben. Weitere Schritte müssen hinzukommen:

- Die datenschutzrechtlichen Sicherungen müssen weiter ausgebaut werden. Notwendig ist außerdem, die Einhaltung der bisher getroffenen Absprachen lückenlos zu kontrollieren. Hierzu werden die Datenschutzbeauftragten ihren Teil beitragen.
- Längst überfällig ist es, die einschlägigen Rechtsgrundlagen vor allem im Bundesdatenschutzgesetz, die noch aus dem vergangenen Jahrhundert stammen, an die neue Internet-Zeit anzupassen, um auch Internetdienste wie Google Street View rechtlich besser behandeln und bewerten und gegebenenfalls auch untersagen zu können.
- Hinzukommen müssen internationale Vereinbarungen, die sicherstellen, dass die u.a. in den deutschen Ländern aufgenommenen Städte-Bilder auch dann einem hinreichenden Datenschutz und einer entsprechender Kontrolle unterliegen, wenn sie – wie im Falle von Google – in den USA verarbeitet werden.

Google Street View ist nicht nur ein Datenschutzproblem. Es ist vielmehr primär ein Menetekel für jene „schöne, neue Welt“, in der die Menschen und ihre private Umgebung aufgrund der technischen Entwicklung lückenlos erfasst und kontrolliert werden können. Staat und Gesellschaft müssen sich mit diesen Entwicklungen beschäftigen. Es bedarf einer breiten gesellschaftlichen Diskussion darüber, ob Vorgänge, die wie Google Street View zu einer zunehmenden Veröffentlichung von Privatheit und privatem Umfeld führen, akzeptiert werden sollen und, wenn ja, in welchem Umfang und unter welchen Bedingungen dies künftig erlaubt sein soll.

Der LfD begrüßt, dass sich der Landtag und die Landesregierung dieser Aufgabe angenommen und dieses Thema zum Gegenstand ihrer Arbeit gemacht haben.

4.2 Google Analytics

Sehr viele Betreiber eines Internet-Angebots setzen Instrumente ein, um die Reichweite und Effizienz ihrer Web-Präsenz genauer in Erfahrung zu bringen. Solche Internet-Analysetools kommen häufig nicht ohne personenbeziehbare Daten (etwa die IP-Adresse von Nutzern) aus und sind deshalb aus Datenschutzsicht kritisch zu betrachten. Das weit verbreitete Tool Google Analytics steht dabei besonders in der Diskussion.

Dabei handelt es sich um einen kostenlosen Dienst, der der Analyse von Zugriffen auf Webseiten dient. Es werden Funktionen geboten wie Darstellung der Herkunft der Besucher, Verweildauer und Suchbegriffe in Suchmaschinen. Google kann unter bestimmten Voraussetzungen mit Google Analytics ein umfassendes Nutzerprofil von Webseiten-Besuchern anlegen. Es ist ungeklärt, ob die bei Google eingegangenen Daten dort (intern) weiterverarbeitet werden oder nicht. Google könnte mit den durch Analytics erhaltenen Daten beispielsweise den Suchalgorithmus anpassen. Bei Websurfern, die ein Konto bei Google besitzen (und somit das „Google-Cookie“ in ihrem Browser gespeichert haben), wäre Google technisch in der Lage, die gesammelten Datenspuren mit einem

Nutzerkonto zu verknüpfen und genau nachzuvollziehen, wer sich wann auf welcher Webseite aufgehalten hat, wenn diese Webseiten Google Analytics einsetzen. Darüber hinaus wäre es auch denkbar, dass exakte Informationen darüber gespeichert werden, welche Produkte wie oft, wann und zu welchem Preis in einem Onlineshop verkauft werden.

§ 12 Abs. 1 TMG lässt eine Verarbeitung von personenbezogenen Daten nur zu, wenn der Benutzer vorher zugestimmt hat oder eine gesetzliche Ermächtigung vorliegt. Durch den Einsatz eines Tools wie Google Analytics wird aber derzeit noch grundsätzlich die vollständige IP-Adresse (ein benutzerbezogenes Datum) des Seitenbesuchers an einen Dritten (Google) übermittelt. Der Aufrufende erfährt grundsätzlich nichts über die Interaktion mit Google Analytics. Eine Einwilligung müsste bewusst und freiwillig erfolgen (§ 13 Abs. 2 TMG). Die Nutzung der Webseite dürfte nicht von der Erteilung einer Zustimmung abhängig gemacht werden (§ 12 Abs. 3 TMG).

Der Datenschutzbeauftragte in Schleswig-Holstein äußerte sich in seinem 31. Tätigkeitsbericht vom 31. März 2009 zu Google-Analytics (S. 135):

„Derzeit ist die Nutzung des kostenlosen Google Analytics Services durch Webseitenanbieter unzulässig. Google muss dessen Konfiguration so ändern, dass die Betroffenen ihr Recht auf Widerspruch, Information und Auskunft sowie Löschung der Daten wirksam wahrnehmen können. Für den rechtswidrigen Einsatz des Dienstes haften die Webseitenbetreiber."

Die Erörterungen der Datenschutzaufsichtsbehörden zu Google Analytics dauern derzeit an. Unabhängig davon ist aus der Sicht des Datenschutzes in jedem Fall zu fordern, dass Webseiten-Anbieter, die Google Analytics einsetzen, darauf deutlich (etwa in ihrer Datenschutzerklärung) hinweisen. Dies würde dem Besucher der Webseiten ermöglichen, Vorkehrungen gegen den nicht auszuschließenden Datenmissbrauch durch Google zu treffen. Er könnte beispielsweise die Erfassung von Datenspuren durch Google Analytics dadurch verhindern, dass er das Laden und Ausführen des Google-Analytics-Scripts unterbindet. Dies geschieht beispielsweise durch das Blockieren von JavaScript (zum Beispiel durch die Firefox-Erweiterung NoScript oder durch Werbeblocker). Auch möglich ist, den Zugriff auf die Google-Analytics-Domain google-analytics.com insgesamt zu sperren (zum Beispiel durch Werbeblocker oder durch die Verwendung der hosts-Dateien).

Vor diesem Hintergrund hat der LfD eine Umfrage zum Einsatz dieses Tools in der Landesregierung und ihrem unmittelbar nachgeordneten Bereich durchgeführt. Es hat sich ergeben, dass Google Analytics nur durch wenige Stellen eingesetzt wird, mit denen eine Diskussion darüber geführt wird, welche datenschutzgerechten Alternativen einsetzbar sind.

In der Privatwirtschaft ist dieses Tool allerdings weit verbreitet; dort stellen sich rechtlich die gleichen Fragen. Es wird weitere vielfältige Aufklärungs- und Kontrollmaßnahmen erfordern, um hier Fortschritte zu erreichen.

Die für den privaten Bereich zuständigen Datenschutzaufsichtsbehörden (der „Düsseldorfer Kreis") haben sich auf eine Entschließung geeinigt, in der die wesentlichen datenschutzrechtlichen Anforderungen an „Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten" dargestellt worden sind (im Internet-Angebot des LfD abrufbar unter http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20091127_inetreichweite).

4.3 Bewertungsplattformen

Der Bundesgerichtshof hat entschieden (mit Urteil vom 23. Juni 2009, Az. VI ZR 196/08; im Internet-Angebot des LfD: http://www.datenschutz.rlp.de/de/gerichtsentscheidungen.php?submenu=bund), dass die Bewertung von Lehrern durch Schüler in dem Bewertungsportal „spickmich.de" trotz der fehlenden Einwilligung der betroffenen Lehrer mit dem informationellen Selbstbestimmungsrecht vereinbar ist und nicht gegen Datenschutzvorschriften verstößt. Die Meinungsfreiheit der Schüler wiege schwerer, zumal die klagende Lehrerin nicht in ihrer Privatsphäre, sondern nur in ihrer beruflichen Tätigkeit betroffen sei und keine konkrete Beeinträchtigung geltend gemacht habe.

Der LfD stimmt dieser Entscheidung im Ergebnis zwar zu. Er betont aber, dass er der anonymen Bewertung von Lehrern in öffentlichen Internet-Plattformen nichts abgewinnen kann. Auch wenn etwas erlaubt ist, muss man nicht jeden Spaß, jeden Unsinn und jede Mode mitmachen.

Maßgeblich ist für ihn deshalb nicht, ob die Lehrerbewertung erlaubt ist, sondern ob sie auf faire Art und Weise durchgeführt wird. Dies gilt für andere Bewertungsplattformen im Internet in gleicher Weise. Daran bestehen häufig Zweifel.

Zunächst sieht das Bundesdatenschutzgesetz in solchen Fällen zwingend vor, dass die Betroffenen darüber unterrichtet werden, wenn sie betreffende Daten in das Internet eingestellt werden. Außerdem sind Vorkehrungen zu treffen, die eine faire Beurteilung der Betroffenen sicherstellen oder zumindest fördern. So sind erkennbare Mani-

pulationen, die von wenigen Personen mit Schädigungsabsicht erfolgen, auszuschließen. Schließlich müssen die Betroffenen auch Gelegenheit erhalten, sich über die Bewertungsgrundlagen zu unterrichten und auch ihre Sicht der Dinge auf der Bewertungsplattform darzustellen.

All dies ist beispielsweise bei „spickmich.de“ zurzeit nicht der Fall. Solange aber entsprechende Vorkehrungen nicht getroffen sind, rät der LfD jedem Schüler zur Zurückhaltung. Ziel des Datenschutzes ist es auch, den fairen Umgang miteinander zu fördern. Dieser faire Umgang ist gerade im Verhältnis zwischen Lehrer und Schüler notwendig. Bei „spickmich.de“ ist er zurzeit aber nicht gewährleistet.

Die Datenschutzbeauftragten sind derzeit damit befasst, allgemeine Kriterien für eine datenschutzgerechte Veröffentlichung von Bewertungsdaten zu erstellen; angesichts der Vielgestaltigkeit der hier zu betrachtenden Phänomene ist diese Aufgabe schwierig.

4.4 Veröffentlichungen im Internet

4.4.1 Jubiläumsdaten aus dem Melderegister

Zeitungen veröffentlichen in ihrem Internet-Angebot häufig auch Jubiläumsdaten, die sie von den Meldebehörden auf der Basis des Meldegesetzes erhalten haben. Es stellt sich die Frage, ob für solche Internet-Veröffentlichungen eine ausreichende Rechtsgrundlage existiert und ob ggf. das Melderecht in dem Sinne zu ändern ist, dass Internet-Veröffentlichungen von Jubiläumsdaten nur auf der Basis ausdrücklicher Einwilligungen erfolgen dürfen.

Diese Frage betrifft letztlich die Bewertung, ob der Gesetzgeber dann, wenn er Veröffentlichungen in Printmedien vorschreibt oder zulässt, er gleichzeitig die Internet-Veröffentlichung erlaubt hat. Da die entsprechende meldegesetzliche Grundlage aus Vor-Internet-Zeiten stammt, ist dies zumindest zweifelhaft. Vergleichbare Fragen dürften sich aber für viele unterschiedliche Rechtsgrundlagen stellen, die die Veröffentlichung von Daten regeln.

Auch im Zusammenhang mit Veröffentlichungen von Zwangsversteigerungsdaten wurde diese Problematik bereits erörtert.

Aus der Sicht des LfD setzen Internet-Veröffentlichungen von Daten – mindestens im staatlichen Bereich – eine Rechtsgrundlage voraus, die diese Veröffentlichungsform bewusst einbezieht. Eine allgemeine Stellungnahme der Datenschutzbeauftragten und -aufsichtsbehörden dazu ist wünschenswert. Mit dieser Zielrichtung führt der LfD derzeit die Diskussion mit seinen Kollegen.

4.4.2 Zeitungsartikel im Internet

Häufig stellt sich die Frage, ob Zeitungs- oder Zeitschriftenveröffentlichungen ohne weitere Voraussetzungen durch die Presse selbst oder durch Dritte im Internet präsentiert werden dürfen. Der LfD ist in den unterschiedlichsten Zusammenhängen mit dieser Frage konfrontiert worden. Er geht bei seiner Beurteilung von folgenden Überlegungen aus:

Websites im Internet, die im allgemeinen Zugriff stehen, sind als Telemedien im Sinne des Telemediengesetzes anzusehen (§ 1 Abs. 1 TMG). Für die Verarbeitung von Inhaltsdaten durch Telemedien gelten danach keine speziellen Regelungen; anzuwenden sind vielmehr die allgemeinen datenschutzrechtlichen Gesetze, die für den Betreiber des in Rede stehenden Telemediums gelten und die die Veröffentlichung von Daten normieren.

Danach ist also nach folgenden Kategorien zu unterscheiden:

- Presseähnliche Telemedien sind wie Presseorgane selbst zu behandeln (§ 12 LMG); eine staatliche Aufsicht durch die Landesdatenschutzbeauftragten kommt bezüglich der sog. „Inhaltsdaten“, also der in Artikeln veröffentlichten Informationen, nicht in Betracht. Schutz gewährt insoweit das allgemeine Zivilrecht (z.B. durch § 823 BGB; das allgemeine Persönlichkeitsrecht wird als absolutes Recht, das gegenüber jedermann gilt, angesehen). Durchgesetzt werden muss dieses Recht dann aber vor den Zivilgerichten. Außerdem ist die Wahrnehmung des presserechtlichen Gegendarstellungsanspruchs auch gegenüber solchen Telemedien (§ 11 LMG) möglich.
- Für öffentliche Stellen des Landes, etwa staatliche Archive, die in ihrem Internet-Angebot Zeitungsartikel veröffentlichen, gelten die §§ 5, 12 ff., 16 LDSG. Eine wirksame Einwilligung der Betroffenen würde danach in jedem Fall ausreichen. Wenn eine solche nicht vorliegt, ist zu prüfen, ob eine Rechtsgrundlage eine solche Veröffentlichung ausdrücklich erlauben würde (§ 5 Abs. 1 LDSG i.V.m. einer entsprechenden Rechtsnorm, z.B. § 16 LDSG). Die allgemeine Aufgabe, Zeitungsartikel zu dokumentieren, reicht aber zur Rechtfertigung der Internet-Veröffentlichung personenbezogener Daten nicht aus. Nach § 16 Abs. 1 Nr. 1 LDSG ist zwar die Übermittlung personenbezogener Daten an nichtöffentliche Stellen (darunter würde auch die Veröffentlichung im Internet fallen) zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der über-

mittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 12 Abs. 4 oder § 13 Abs. 2 Nr. 3 LDSG zulassen würden. Diese Voraussetzungen dürften in der Praxis aber nur selten eine Internet-Veröffentlichung rechtfertigen. Dies betrifft auch die Veröffentlichungen durch staatliche Archive oder Bibliotheken im Internet.

- Für private Anbieter von Telemedien, die kein presseähnliches Telemedium betreiben, sind §§ 5, 28, 29 BDSG zugrunde zu legen, die ebenfalls besondere Voraussetzungen für eine Veröffentlichung erfordern. Ergänzend ist die Rechtsprechung zur Verletzung von Persönlichkeitsrechten durch Internet-Nachweise des Inhalts von Zeitungsartikeln zu berücksichtigen (Ansprüche aus § 823 Abs.1 bzw. Abs. 2 BGB , ggf. i.V.m. Unterlassungsansprüchen gem. § 1004 BGB). Die bislang ergangenen Entscheidungen betreffen Internetveröffentlichungen über Straftaten Betroffener und berücksichtigen das Resozialisierungsinteresse der Betroffenen in besonderer Weise (z.B. LG Hamburg vom 16. November 2007, Az. 324 O 250/07 unter Berufung auf BVerfGE 35, S. 202 ff., 233 ff. – Lebach I, m.w.N.; BVerfG, Beschluss vom 25. November 1999, NJW 2000, S. 1859 ff., 1860 f. – Lebach II).

Es stellen sich aber in diesem Zusammenhang durchaus gewichtige Fragen, die noch ungeklärt sind:

- Wann ist von einem „presseähnlichen Telemedium“ zu sprechen? Wo liegen die Grenzen? Was gilt in Bezug auf Vereinsnachrichten, Firmeninformationen für die Mitarbeiter u.ä.? Sind Blogs und Forenbeiträge wie Leserbriefe in Zeitungen privilegiert? Wenn nein, wann beginnt diese Gleichsetzung?
- Zugunsten von Zeitungsverlagen greift in diesem Zusammenhang auch bezogen auf die Archivierung alter Presseartikel das Grundrecht auf Pressefreiheit ein, das durch das sog. „Presseprivileg“ des Bundesdatenschutzgesetzes und der Landesmediengesetze (§ 41 BDSG, § 12 LMG) gesetzlich verankert ist. Dadurch sind den Datenschutzbeauftragten aufsichtsbehördliche Maßnahmen in diesem Zusammenhang untersagt. Den Betroffenen bleibt die Anrufung der Selbstkontrollorgane der Presse, also des Presserates (im Internet erreichbar unter http://www.redaktionsdatenschutz.de/). Es stellt sich aber die Frage, ob es wirklich angemessen ist, die lange zurückgehende Speicherung und Veröffentlichung von Presseartikeln durch die Presse selbst in gleicher Weise zu privilegieren wie die aktuellen Ausgaben solcher Medien.

Der LfD wird sich auch durch seine Beteiligung an den entsprechenden Diskussionen auf der Ebene des Bundes um eine Klärung dieser Fragen bemühen.

4.4.3 Bereitstellung von archivierten Blog-Beiträgen

Ein in Rheinland-Pfalz ansässiger Anbieter betreibt zwei Webseiten. Er hat aus dem Usenet zahlreiche Gruppen ausgewählt und die dort veröffentlichten Nachrichten systematisch nach Newsgruppen geordnet und innerhalb dieser Gruppen chronologisch für jedermann zum Abruf bereit gestellt. Regelmäßig sind die Namen und Mail-Adressen der Nachrichtenverfasser kenntlich. Eine regelmäßige Löschung ist nicht vorgesehen. Die Beiträge werden von Google-Recherchen erfasst und angezeigt; das Suchen mit dem Namen des Urhebers der Nachrichten ist damit möglich geworden.

Bei diesen Mediendiensten handelt es sich nicht um Presse bzw. um ein presseähnliches Medium im Internet, für die die Pressefreiheit sowie das Landesmediengesetz anwendbar wären. Rechtlich handelt es sich vielmehr um ein Angebot gem. § 29 BDSG (geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung). Danach ist das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt. Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (§ 28 Abs. 1 Satz 2 BDSG).

Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein solches schutzwürdiges Interesse ist besonders dann anzunehmen, wenn sich die Daten beziehen auf strafbare Handlungen, auf Ordnungswidrigkeiten sowie bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse (§ 28 Abs. 3 Satz 2).

Vor diesem Hintergrund sieht der LfD keine rechtliche Verpflichtung des Anbieters dieser Webseiten, bei Widersprüchen von Usenet-Autoren deren Namen und E-Mail-Adresse zu löschen, wenn diese keine besonderen Gesichtspunkte für die Schutzbedürftigkeit dieser Angaben im konkreten Zusammenhang anführen. Allerdings wird vertreten, jeder Wunsch, auch der nicht begründete,

verursache die Löschungspflicht; dies gebiete der Gedanke des informationellen Selbstbestimmungsrechts. Dem kann bei Daten, die zulässigerweise veröffentlicht worden sind, nicht gefolgt werden: der Urheber hat sich an einer öffentlichen Diskussion mit Namen beteiligt. Damit hat er ein Faktum gesetzt, dessen Dokumentation zunächst legitim ist. Dieses Dokumentationsinteresse umfasst grundsätzlich die bereits veröffentlichten Identitätsdaten. Ein Anspruch auf deren Löschung muss das Dokumentationsinteresse überwiegen. Sicher sind keine hohen Anforderungen an die Begründung von solchen Löschungsbegehren zu stellen. Mehr als der bloße Willen muss allerdings vorgetragen werden.

Dieses Ergebnis wird auch durch eine Einbeziehung der Regelung des § 35 Abs. 5 BDSG in die Betrachtung gestützt. Nach dieser Vorschrift besteht für Jedermann ein Widerspruchsrecht: Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt.

Auch danach ist also ein Widerspruch nur zu berücksichtigen, wenn ein schutzwürdiges Interesse besteht, das über das allgemeine und nicht begründungsbedürftige Grundrecht auf informationelle Selbstbestimmung hinausgeht.

Aus den Nutzungsbedingungen bzw. Nutzungsusancen des Usenet ergibt sich noch folgender zusätzlicher Gesichtspunkt, der das vorgenannte Ergebnis weiter stützt: Es existiert im Usenet ein Mechanismus (s.a. http://de.wikipedia.org/wiki/X-No-Archive), welcher bei dem Absenden einer Nachricht deren Archivierung untersagt. Jeder Newsgroup-Beiträger kann diese Möglichkeit nutzen. Weiter ist allerdings darauf hinzuweisen, dass aus § 35 Abs. 2 Satz 2 Nr. 4 BDSG eine Löschungsverpflichtung resultieren könnte. Diese gesetzliche Löschungspflicht gilt unabhängig vom Antrag eines Betroffenen. Danach sind personenbezogene Daten zu löschen, wenn sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist. Die Erforderlichkeit ist am Speicherungszweck zu messen. Angesichts der Schnelllebigkeit des Internet dürfte also diese Löschungspflicht auch für Dateien bestehen, die aus einem bloßen Dokumentationsinteresse heraus angeboten werden.

Unabhängig davon wäre es aus datenschutzrechtlicher Sicht zu begrüßen, wenn in den – sicherlich nicht sehr zahlreichen – Fällen, in denen ein Betroffener Widerspruch einlegt, eine Anonymisierung des fraglichen Newsgroup-Beitrages auch ohne Rechtspflicht erfolgen würde. Dies würde zur Akzeptanz des Angebots beitragen, ohne seinen Nutzwert unzumutbar einzuschränken. Es bleibt allerdings dem Webseiten-Betreiber überlassen, ob er dieser Anregung folgt.

5. Wirtschaft

5.1 Datenschutz in der Privatwirtschaft

Die Vielzahl der Datenschutzskandale der vergangenen zwei Jahre – Deutsche Telekom, Deutsche Bahn und Lidl stehen (leider) nur stellvertretend hierfür – haben zu der Einsicht geführt, dass das Grundrecht auf informationelle Selbstbestimmung heute vorrangig nicht (mehr) nur durch staatliche Aktivitäten, sondern besonders durch privatwirtschaftliche Akteure gefährdet wird. Diese Verlagerung des Gefährdungspotentials bestätigt auch der Präsident des Bundesverfassungsgerichts, Prof. Dr. Papier, der vor den Gefahren eines „Super-GAUs des Datenschutzes“ in der Privatwirtschaft eindringlich warnt.

Die Entwicklung der Eingaben von Bürgern an den LfD gibt dieser Einschätzung Recht: Bewegte sich die Zahl der Eingaben an die Aufsichts- und Dienstleistungsdirektion im Jahre 2008 noch im zweistelligen Bereich, so gingen beim LfD seit Aufnahme seiner Tätigkeit im privatwirtschaftlichen Bereich bereits im ersten Jahr mehr als 1.000 Eingaben ein, in mehr als 300 Fällen führten diese Eingaben zu weitergehenden Ermittlungen und umfangreichen Stellungnahmen des LfD. Schwerpunkte der Eingaben sind dabei die Bereiche Arbeitnehmerdatenschutz, Videoüberwachung, Internetnutzung, Adresshandel sowie Fragen zur Tätigkeit der betrieblichen Datenschutzbeauftragten.

Schätzungsweise über 200.000 private geschäftsmäßig tätige Datenverarbeiter sind in Rheinland-Pfalz ansässig. Eine lückenlose flächendeckende Überwachung und Kontrolle ist angesichts der zur Verfügung stehenden personellen und sächlichen Ausstattung des LfD – auch nach der Aufstockung im Jahre 2009 – unmöglich. Auch helfen gesetzgeberische Maßnahmen alleine nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht unterbunden werden können. Die Datenschutzaufsichtsbehörden müssen daher auch zukünftig organisatorisch, personell und finanziell in die Lage versetzt werden, ihren Beratungs- und Kontrollaufgaben unabhängig und wirkungsvoll nachkommen zu können.

Generell ist 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 Informationen entstehen bei immer mehr privaten Unternehmen und keineswegs nur bei 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. Hinzu kommen die neuen Gefahren im Internet, insbesondere durch das Web 2.0, durch eine lückenlose Erfassung des Nutzungsverhaltens, durch Identitätsdiebstähle, Phishing oder virtuellen Exhibitionismus.

In dieser Situation kann die Kontroll- und Aufsichtstätigkeit der staatlichen Aufsichtsbehörde nur „Grundbedarfe“ abdecken, mehr als die stichprobenartige Untersuchung datenschutzrechtlicher Problemfelder in wenigen Schwerpunktgebieten sind weder personell noch finanziell möglich. Umso wichtiger war es für den LfD, von Anfang an Netzwerke zu bilden, die Beratungsleistungen auszubauen und durch zahlreiche Vorträge zum Thema Datenschutz Multiplikatoren zu erreichen (s.a. Tz. 3.4).

Eine herausgehobene Stellung spielen dabei naturgemäß die betrieblichen Datenschutzbeauftragten, die als „Außenstellen“ des Datenschutzes für ein möglichst hohes Niveau des Datenschutzes in den Betrieben verantwortlich sind. Aus diesem Grunde hat der LfD die Kontakte zu den „Erfahrungsaustausch-Kreisen“ der betrieblichen Datenschutzbeauftragten (Erfa-Kreise) intensiviert (s.a. Tz. 3.4.3) und durch eigene Informationsveranstaltungen in Mainz die Netzwerkbildung in diesem Bereich gefördert. Auf dieser „Fachebene“ spielte der Meinungsaustausch über die zahlreichen Novellierungen des Bundesdatenschutzgesetzes zum 1. September 2009 eine ebenso wichtige Rolle wie die Berichte der betrieblichen Datenschutzbeauftragten aus ihren Unternehmen.

Zugleich wurde der Kontakt zu den institutionellen Ansprechpartnern ausgeweitet und vertieft: Die Industrie- und Handelskammern, die Handwerkskammern, aber auch die Kammern der freien Berufe (Ärztekammern, Rechtsanwaltskammern, Notarkammern) sind „natürliche Verbündete“ des LfD, mit ihnen wurden seit Anfang des Jahres 2009 zahlreiche Gespräche über Kooperationsmöglichkeiten geführt. Erste Früchte dieser Koordinierung sind zum Beispiel Fachvorträge bei der Rechtsanwaltskammer Koblenz oder bei der Industrie- und Handelskammer Trier, die sich eines hohen Interesses bei den Kammermitgliedern erfreuten.

Wichtiger Kooperationspartner der Datenschützer sind auch die Verbraucherschützer. Häufig arbeiten sie, wenn auch mit unterschiedlichen Ansätzen, an denselben Problemen, etwa an der Bekämpfung von betrügerischen Vertragsabschlüssen im Internet oder dem Schutz Minderjähriger in sozialen Netzwerken. Aus diesem Grund sind der LfD und die Verbraucherschutzzentrale Rheinland-Pfalz entschlossen, auf den gemeinsamen Tätigkeitsfeldern die Kräfte zu bündeln. So informiert die Verbraucherschutzzentrale bereits in Absprache mit dem LfD

die Verbraucher über ihre Möglichkeiten, datenschutzrechtliche Auskunfts- und Löschungsansprüche gegenüber gewerblichen Anbietern durchzusetzen, umgekehrt kann der LfD bei der Klärung der Rechtmäßigkeit von Vertragsanbahnungen (sog. cold calls) und bei der Ermittlung der für Werbemaßnahmen verantwortlichen Stellen wichtige Unterstützung leisten. Für das Jahr 2010 ist eine Intensivierung dieser Zusammenarbeit bereits eingeplant.

Neben der absolut notwendigen aufsichtbehördlichen Tätigkeit wird der LfD auch zukünftig das Schwergewicht seiner Bemühungen auf Kooperation und Beratung im Bereich der Privatwirtschaft legen. Entscheidend für das Niveau des Datenschutzes in den Unternehmen ist weniger die gesetzgeberische und aufsichtbehördliche Tätigkeit des Staates, sondern vielmehr das Engagement und die Durchsetzungsfähigkeit der betrieblichen Datenschutzbeauftragten.

5.2 Aufsichtsbehördliche Rechte des LfD

Gemäß § 24 Abs. 1 Satz 2 LDSG ist der LfD auch Aufsichtbehörde nach dem Bundesdatenschutzgesetz für die Datenverarbeitung nicht-öffentlicher Stellen. Mit dieser aufsichtsbehördlichen Tätigkeit sind in erster Linie Kontrollaufgaben verbunden (vgl. § 38 Abs. 1 Satz 1 BDSG). Die Aufsichtsbehörde kontrolliert die Ausführung des Bundesdatenschutzgesetzes sowie andere Vorschriften über den Datenschutz. Sie berät und unterstützt aber auch die betrieblichen Datenschutzbeauftragten und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse (§ 38 Abs. 1 Satz 2 BDSG). Ferner leistet die Aufsichtsbehörde anderen Mitgliedstaaten der Europäischen Union auf Ersuchen Amtshilfe.

Zur Erfüllung ihrer Aufgaben ist die Aufsichtsbehörde mit weit reichenden gesetzlichen Befugnissen ausgestattet: So hat die Aufsichtsbehörde ein umfassendes Auskunftsrecht gegen die Leitung von Privatunternehmen (§ 38 Abs. 3 BDSG). Verstöße gegen diese umfassende Auskunftspflicht können zudem als Ordnungswidrigkeit verfolgt und mit einem Bußgeld von bis zu 50.000 Euro geahndet werden (§ 43 Abs. 1 Nr. 10, Abs. 3 BDSG). Darüber hinaus hat die Aufsichtsbehörde zur Stärkung ihrer Position ein Betretungsrecht: Die Mitarbeiter der Aufsichtsbehörde sind befugt, zur Erfüllung ihrer Aufgaben während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der kontrollierten Stellen zu betreten und dort Prüfungen und Besichtigungen vornehmen (§ 38 Abs. 4 Satz 1 BDSG). Dabei können sie auch geschäftliche Unterlagen sowie die verwendeten Datenverarbeitungsprogramme einsehen (§ 38 Abs. 4 Satz 2 BDSG).

Eine weitere Verstärkung hat die Position der Aufsichtsbehörden mit der Novellierung des Bundesdatenschutzgesetzes zum 1. September 2009 erfahren. Erstmals verfügt die Aufsichtsbehörde nunmehr über ein eigenständiges Anordnungsrecht zur Behebung festgestellter Verstöße gegen Datenschutzvorschriften (§ 38 Abs. 5 Satz 1 BDSG). Darüber hinaus ist sie befugt, bei festgestellten schwerwiegenden Verstößen oder Mängeln bestimmte Arten der Datenverarbeitung zu untersagen und diese Untersagung mit Zwangsmitteln (Verhängung eines Zwangsgeldes) durchzusetzen.

Mit diesem erheblich ausgeweitetem Arsenal an Informations- und Zwangsmitteln ist die Aufsichtsbehörde inzwischen grundsätzlich in die Lage versetzt, Verstöße gegen datenschutzrechtliche Bestimmungen aufzudecken, zu beseitigen und zu sanktionieren. Hiervon hat die Aufsichtsbehörde auch bereits im ersten Jahr ihrer Verankerung beim LfD umfangreich Gebrauch gemacht. Neben zahlreichen Ortsterminen unter Inanspruchnahme des Betretungs- und Einsichtsrechts der Aufsichtsbehörde hat sie ihre Informationsrechte intensiv genutzt und zunächst verweigerte Auskünfte durch die Androhung von Zwangsgeldfestsetzungen erhalten können. Darüber hinaus sind mehrere Ordnungswidrigkeitenverfahren eingeleitet und zum Teil mit erheblichen Bußgeldern in vierstelliger Höhe bereits rechtskräftig abgeschlossen worden. Besonders zu betonen ist dabei, dass die Aufsichtsbehörde zur Einleitung von Ordnungswidrigkeitenverfahren nur dann schreitet, wenn festgestellte Datenschutzverstöße gemeinsam mit der verantwortlichen Stelle nicht geklärt und nicht freiwillig beseitigt werden konnten. Bislang wurde keiner der erlassenen Verwaltungsakte und keiner der verhängten Bußgeldbescheide im Gerichtsverfahren aufgehoben; zukünftig ist bei der zu erwartenden Anzahl von Ordnungswidrigkeitenverfahren allerdings verstärkt mit Rechtsstreitigkeiten auf diesem Gebiet zu rechnen. Ob die personelle Ausstattung der Aufsichtsbehörde hierfür ausreichen wird, kann noch nicht prognostiziert werden.

5.3 Betriebsrätliches Schnellinformationssystem

Im Zeitraum vom 1. Januar 2009 bis zum 31. Dezember 2009 wurden im Rahmen eines sog. betriebsrätlichen Schnellinformationssystems die Betriebsräte bestimmter Unternehmen auf der Grundlage eines einheitlichen Fragebogens wöchentlich nach der wirtschaftlichen Situation ihres Unternehmens befragt. Grundlage der Erhebung war ein Stammdatenblatt, in welchem der Betriebsrat die Anschrift seines Betriebs, dessen Geschäftsführer bzw. Vorstand, den Betriebsratsvorsitzenden, seine Stellvertreter und sonstige

Ansprechpartner aufführte. Außerdem fanden sich dort Angaben zum Jahrsumsatz und -ergebnis des letzten Geschäftsjahres, darüber hinaus wurden Angaben zum Einsatz von Leiharbeitern und befristeten Arbeitnehmern, zum Stand der Arbeitszeitkonten, von Überstunden und zur Arbeitszeitverkürzung abgefragt. Im Rahmen der wöchentlichen Befragung der Betriebsräte wurde nach der Entwicklung der Auftragssituation im Betrieb, nach der Einschätzung der künftigen Auftragsentwicklung, nach aufgetretenen Finanzierungsproblemen, nach der Reduktion von Investitionsvolumina sowie nach In- und Outsourcing-Maßnahmen gefragt. Das Projekt wurde mit Mitteln aus dem Landeshaushalt gefördert und von einer GmbH durchgeführt.

Die rechtliche Bewertung dieses betriebsrätlichen Schnellinformationssystems führte zum Streit. Dabei ging es vor allem auch um datenschutzrechtliche Bewertungen. Als wichtiger neuer Aspekt ist die Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht von Unternehmen zu berücksichtigen. Demnach sind nicht nur personenbezogene Daten, sondern auch unternehmerische Daten von der Verfassung mit einem besonderen Schutz versehen. Gesetzgeberische Schlussfolgerungen sind auch aus dieser Rechtsprechung des Bundesverfassungsgerichts bislang noch nicht gezogen worden. Auch die parlamentarische Debatte zum betriebsrätlichen Schnellinformationssystem hat im Berichtszeitraum noch nicht ihr Ende gefunden.

5.4 Datenklau

Im Jahr 2008 gehörte „Datenklau“ zu den „Worten des Jahres“ (es stand an dritter Stelle hinter „Finanzkrise“ und „verzockt“). Anlass für die öffentliche Aufmerksamkeit diesem Phänomen gegenüber boten insbesondere die Skandale um die Telekom: Im Jahr 2006 kam es bei der damaligen T-Mobile GmbH, einer Tochtergesellschaft der Deutschen Telekom, zum Abfluss von rund 17 Millionen Kundendatensätzen mit Mobiltelefonnummer, Name, Vorname, Anschrift, Geburtsdatum und teilweise der E-Mail-Adresse. Nachdem in der Presse Hinweise auftauchten, dass ein rheinland-pfälzisches Internet-Unternehmen über diese Daten verfüge, hat der LfD in der Angelegenheit örtliche Feststellungen getroffen. Diese ergaben, dass das Unternehmen tatsächlich im Besitz der Kundendaten war.

Der Inhaber wies darauf hin, dass er, nachdem ihm die Daten via Internet von einem Datenhändler zur Verfügung gestellt worden waren, die Deutsche Telekom unterrichtet habe. In der Folgezeit wurde jedoch nicht um die Löschung der Daten ersucht, vielmehr sei darum gebeten worden, die Informationen zunächst für weitere Ermittlungen vorzuhalten. Danach ergingen keine weiteren Anweisungen. Weshalb die Daten über zweieinhalb Jahre im Besitz des Unternehmens blieben, obwohl die verantwortliche Stelle informiert war, war für den LfD nicht nachvollziehbar. In Abstimmung mit der zuständigen Staatsanwaltschaft wurde das zu Beweissicherungszwecken Nötige veranlasst und die bei dem Unternehmen vorhandenen Daten gelöscht.

Seit dieser Zeit haben sich die Meldungen über Datendiebstähle in den unterschiedlichsten Bereichen, über unzulässigen Handel mit Adress- und Bankverbindungsdaten sowie unzulässige Datennutzungen insbesondere durch Callcenter gehäuft. Nach einem Bericht der Zeitung "Die Wirtschaftswoche" vom Oktober 2008 waren dieser 21 Millionen Datensätze mit Angaben zur jeweiligen Person, deren Bankverbindung sowie teilweise den Vermögensverhältnissen zum Kauf angeboten worden. Laut Wirtschaftswoche führten erste Spuren fast durchgängig zu Call-Centern, die als Dienstleister für Unternehmen tätig würden.

In letzter Zeit ist der Begriff verbunden worden mit dem Herunterladen von Nutzerprofildaten aus sozialen Netzwerken und dem Verkauf von Steuersünderdaten aus Liechtenstein und der Schweiz.

Aus Sicht des LfD zeigen solche Vorgänge, dass der Schutz von Unternehmensdatenbanken vielfach unzureichend ist. Im Rahmen der Auslagerung von Aufgaben der Kundenbetreuung und -aquise in Call-Center werden häufig Zugänge zu unternehmenseigenen Kundendaten eingerichtet, ohne dass eine angemessene Absicherung erfolgt. Die Datensätze können offenbar aus den Unternehmensdatenbanken abgezogen werden, ohne dass dies durch entsprechende Sicherheitsvorkehrungen verhindert bzw. erkannt wurde. Die Fälle zeigen, dass illegal erworbene Informationen eine gut bezahlte Ware sind. Der LfD fordert daher von den Unternehmen, die Absicherung ihrer Kundendaten zu verbessern. Gegenüber Innentätern und missbräuchlich handelnden Auftragnehmern ist gutgläubiges Vertrauen unangebracht.

Es muss geprüft werden, ob die vorhandenen Strafbestimmungen ausreichen. Diese stellen in erster Linie unbefugte Zugriffe auf Daten unter Strafe, unter Umständen jedoch nicht die missbräuchliche Verwendung von Daten, auf die im Rahmen eingeräumter Berechtigungen zugegriffen werden konnte.

Im Übrigen weisen solche Vorgänge auf Strukturen bei Datenflüssen hin, die von den Aufsichtsbehörden nur

bedingt zu kontrollieren sind. Bei ca. 5.000 Call-Centern bundesweit, davon etwa 60 in Rheinland-Pfalz, ist mit der derzeitigen Personalausstattung eine umfassende Kontrolle nicht möglich. Es kommt darauf an, dem illegalen Datenhandel mit rechtlichen und technischen Maßnahmen zu begegnen.

Vor diesem Hintergrund hat der LfD am 3. November 2008 unter dem Titel "Vernachlässigtes Kapital – Datenschutz in der Privatwirtschaft" zu einer Veranstaltung in den Plenarsaal des rheinland-pfälzischen Landtags eingeladen. Unter den ca. 200 Gästen aus den Bereichen der Wirtschaft, der Landesregierung und der Justiz befanden sich Bundes- und Landtagsabgeordnete, der Präsident des Verfassungsgerichtshofs, die Präsidenten der Oberlandesgerichte und der obersten Fachgerichte des Landes, der Präsident des Rechnungshofs, zahlreiche Abteilungsleiter aus den Ressorts, betriebliche und behördliche Datenschutzbeauftragte sowie auch jugendliche Zuhörer.

In seiner Begrüßung hob der LfD hervor, dass neben allen Anstrengungen des Gesetzgebers, der Kontrollbehörden und der privaten Wirtschaft selbst vor allem auch die Bürger gefordert seien, im Sinne eines "Selbstdatenschutzes" mit eigenen Daten überlegt umzugehen und auch auf technische Sicherungsmaßnahmen zu achten. In ihrem Einführungsvortrag stellte die Bundesministerin der Justiz Brigitte Zypries dar, welche Überlegungen für die Bundesregierung derzeit maßgeblich sind, um das Bundesdatenschutzgesetz sachgerecht zu novellieren.

Prof. Dr. Dr. h.c. mult. August-Wilhelm Scheer, Präsident des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (BITKOM), wies vor allem auf die Folgen der Globalisierung in der IT-Welt hin. Selbst europäische Regelungen griffen zu kurz. Die DV-Welt werde von Global Playern bestimmt, die ihren Sitz außerhalb Europas hätten. Für Deutschland sah er weniger ein Defizit bei den vorhandenen Regelungen, als vor allem im Vollzug: Alle bekannt gewordenen Datenschutzskandale der letzten Zeit würden auf Gesetzesverletzungen beruhen. Es komme darauf an, diese durch wirkungsvollere Kontrollen zu verhindern.

Seine Erfahrungen als Call-Center-Mitarbeiter schilderte Günter Wallraff. Nach seiner Kenntnis arbeiteten 80 Prozent der werbenden Callcenter (die unverlangte Anrufe tätigen) illegal und nutzten Datenbestände aus dubiosen Quellen. Er plädierte nachdrücklich dafür, in diesem Bereich effektiv, besonders durch verdeckte Ermittlungen, illegale Machenschaften aufzuklären und die Verantwortlichen zu bestrafen.

Margit Conrad, Staatsministerin für Umwelt, Forsten und Verbraucherschutz, sah – in Übereinstimmung mit der Bundesjustizministerin – deutlichen Handlungsbedarf für den Gesetzgeber. Ohne ausdrückliche Einwilligung des Verbrauchers solle es in Zukunft keine Datenspeicherung und vor allem keine Datenweitergabe zu Werbezwecken geben. Überdies dürfe der Abschluss von Verträgen nicht davon abhängig gemacht werden, ob gleichzeitig Daten zu Werbezwecken übermittelt werden dürfen. Conrad forderte bei Verstößen gegen das Datenschutzrecht die Verschärfung der Straf- und Bußgeldvorschriften sowie die Möglichkeit zur Abschöpfung von Gewinnen, die durch Datenmissbrauch erzielt wurden.

Einig waren sich alle Diskutanten darin, dass die Kompetenz für den Umgang mit den neuen Medien, aber auch für die Wahrnehmung ihrer Rechte als Verbraucher, schon frühzeitig durch eine intensive Informationsarbeit von Schulen und anderen staatlichen und gesellschaftlichen Kräften gestärkt werden muss.

5.5 Illegale Entsorgung von Daten

Aufgrund der Beobachtungen eines aufmerksamen Anwohners wurde der LfD im September 2009 davon in Kenntnis gesetzt, dass sich in mehreren Müll-Containern in Mainz-Weisenau hunderte von Personalakten frei zugänglich befanden. Nach den Feststellungen des LfD wurde – offenbar von einer Marketing-Firma aus dem Telekommunikationsbereich – eine große Anzahl von Personalakten, Steuerunterlagen und Bewerbungsmappen mit sensiblen und geschützten Daten wie Lebensläufen, Fotografien, Bankverbindungen, Telefon- und Mobilfunknummern etc. illegal deponiert. Auf Ersuchen des LfD stellte das Polizeipräsidium Mainz die Müllcontainer umgehend sicher.

Die Verantwortung für den entdeckten Datenschutzverstoß der Marketing-Firma konnte rasch aufgeklärt werden. Der verantwortliche Unternehmensleiter stellte sich aufgrund des öffentlichen Drucks den Behörden und legte ein umfassendes Geständnis ab. Die von den Polizeibehörden sichergestellten Unterlagen wurden unter Aufsicht des LfD eingehend gesichtet und sodann ordnungsgemäß vernichtet, so dass weiterer Schaden für die betroffenen Arbeitnehmer sowie die früheren Bewerber nicht mehr entstehen konnte. Wegen der gravierenden Verstöße gegen datenschutzrechtliche Bestimmungen zur sorgfältigen Vernichtung personenbezogener Daten wurde außerdem ein Bußgeldverfahren eingeleitet, welches mit der Verhängung eines Bußgeldes in vierstelliger Höhe abgeschlossen wurde.

Bewerbungsunterlagen, die neben Adressdaten meist ausführliche Informationen über Werdegang und Persönlichkeit eines Menschen enthalten, sind – sollten sie nach einer erfolglosen Bewerbung nicht an den Bewerber zurückgesandt werden – ordnungsgemäß zu vernichten. Mit Einwilligung der Betroffenen können die Unterlagen auch über die Frist des Allgemeinen Gleichbehandlungsgesetzes hinaus aufbewahrt werden, um sie zu weiteren Auswahlverfahren hinzuzuziehen. Allgemein sollte festgelegt werden, an welchem Ort die Bewerberdaten aufzubewahren sind und wer Zugriff auf sie erhält. Unzulässiger Datenentsorgung wird durch Schulungen der Mitarbeiter und durch ein geregeltes Abfallmanagement mit Einsatz von Aktenvernichtern entgegengewirkt.

Ingesamt zeigte der Vorfall, dass die Unternehmen mit Personaldaten besonders sorgfältig umgehen müssen. Dies gilt nicht nur bei der Erhebung und der Verwendung der Daten, sondern auch bei deren Vernichtung. Wer gegen diese Sorgfaltspflichten verstößt, richtet nicht nur erheblichen Schaden an, er enttäuscht auch das Vertrauen seiner Mitarbeiter und muss mit erheblichen Geldstrafen rechnen. Trotz des offenkundig gravierenden Verstoßes gegen datenschutzrechtliche Bestimmungen konnte der LfD als sehr positiv festhalten, dass der Aufmerksamkeitsgrad in der Bevölkerung hinsichtlich datenschutzrechtlicher Probleme offenbar immer weiter zunimmt. Zudem lobte der LfD die äußerst zügige und kollegiale Zusammenarbeit mit den Mainzer Polizeibehörden.

5.6 Datenschutz in Vereinen

Auch Vereine haben Daten zu schützen. Vielen Vereinen ist jedoch nicht bewusst, dass die Verarbeitung von Mitgliedsdaten oder von personenbezogenen Daten, die sich aus Vereinsaktivitäten ergeben, datenschutzrechtlichen Anforderungen unterliegt.

Dies gilt z.B. für die von vielen Vereinen betriebenen Internet-Angebote. In diesem Zusammenhang haben sich u.a. folgende Problembereiche gezeigt:

- Online-Formulare für den Vereinsbeitritt weichen von vorhandenen Papiervordrucken ab. Mit Blick auf § 3a BDSG sollten als obligatorisch ausschließlich die für einen Mitgliedsantrag unabdingbaren Datenfelder gekennzeichnet werden, als optional diejenigen Daten, deren Angabe eine schnellere Bearbeitung oder Zusatzleistungen ermöglicht (z.B. Telefonnummer, E-Mail-Adresse).
- Ein Online-Antrag auf Mitgliedschaft muss, wenn eine Nutzung der Daten auch für Werbung, Marktforschung oder die bedarfsgerechte Gestaltung des Internet-Angebots beabsichtigt ist, hierzu eine separate Einwilligungsmöglichkeit vorsehen. Ist dies nicht der Fall, willigt der Nutzer entsprechend §§ 12 Abs. 1, 13 Abs. 2 TMG nur in die Verarbeitung der Daten für die Betreuung der Mitgliedschaft ein. Eine Nutzung für andere Zwecke ist nach § 12 Abs. 2 TMG an eine ausdrückliche weitere Einwilligung geknüpft und bei deren Fehlen unzulässig. Dies gilt in gleicher Weise auch für den Mitgliedsantrag in Papierform. Ein Antrag auf Mitgliedschaft darf nicht dazu führen, dass die Mitgliedsdaten ohne Einwilligung auch für Werbezwecke verwendet werden.
- In Mitgliedsforen bedarf die Erhebung und Verarbeitung von Registrierungs- und Nutzungsdaten einer Unterrichtung nach § 13 Abs. 1 TMG. Damit sollten zu Zweck, Art und Umfang der Datenverarbeitung einschließlich der Frage der Weitergabe an Dritte und der Löschung in FAQs der Foren bzw. der Registrierung vorgeschaltet, entsprechende Hinweise erfolgen.
- Wenn für Sportveranstaltungen Tickets online erworben werden können und die technische Abwicklung Dritten übertragen wird, sollten, um den Anforderungen des § 13 Abs. 1 TMG zu entsprechen, im Rahmen des Shop-Zugangs bzw. der Kundenregistrierung entsprechende Hinweise aufgenommen werden. Diese sollten klarstellen, welche Daten durch welche Stelle zu welchem Zweck verarbeitet werden, in welchem Umfang eine Weitergabe an Dritte erfolgt und wann die Daten ggf. gelöscht werden.
- Bei Internet-Angeboten von Vereinen handelt es sich um Telemedien i.S.d. § 1 Abs. 1 TMG. Um die Nutzung des jeweiligen Online-Angebots auszuwerten und dieses besser an die Bedürfnisse der Nutzer anzupassen, werden häufig die Zugriffe auf die Webseite protokolliert. Der Verein hat in diesem Fall nach § 13 Abs. 4 Nr. 2 TMG sicher zu stellen, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden. Hierunter fällt z.B. die jeweilige IP-Adresse des Nutzers. Soweit keine ausdrückliche Einwilligung der Nutzer in die Speicherung ihrer IP-Adressen vorliegt – die eine Unterrichtung nach § 13 Abs. 1 TMG voraussetzt –, können Konflikte mit der o.g. Regelung vermieden werden, indem die IP-Adressen um den Teil gekürzt werden, der einen unmittelbaren Bezug auf den aufrufenden Rechner liefert. Entsprechende Hinweise stehen im Internet-Angebot des LfD unter http://www.datenschutz.rlp.de/downloads/oh/info_webserverlogfiles.pdf zur Verfügung.
- Soweit für Fan-Foren, Ticket-Shops etc. eine Anmeldung erforderlich ist, bedarf es einer gesicherten Übertragung der Login-Daten im Rahmen einer Verschlüsselung über das HTTPS-Protokoll.

Eine Videoüberwachung im Zusammenhang mit Sportveranstaltungen muss sich auf das Vereinsgelände und ggf. die Zuwege beschränken. Bereiche, die mit der Veranstaltung nicht in Zusammenhang stehen, dürfen nicht überwacht werden. In allen Bereichen, die überwacht werden, muss in geeigneter Weise, auf vorhandene Videoanlagen hingewiesen werden (s.a. Tz. 3.2).

Auch bei der Veröffentlichung von Bildern im Internet sind die Vorschriften des Bundesdatenschutzgesetzes sowie des Kunsturhebergesetzes zu beachten.

In Zusammenarbeit mit dem Landessportbund wurden relevante Einzelpunkte bezüglich ihrer datenschutzrechtlichen Umsetzung angesprochen. Der LfD erstellt eine Orientierungshilfe zur Datenverarbeitung in Vereinen.

5.7 Veröffentlichung von Subventionsdaten im Internet

Hohe Wellen auch über Rheinland-Pfalz hinaus hat die Frage geschlagen, ob Empfänger von Agrarsubventionen mit Namen und Wohnort sowie Art und Höhe der Fördermittel auf dem Internet-Portal der Bundesregierung veröffentlicht werden dürfen. Im Rahmen der sog. Transparenzinitiative der EG war diese Offenlegung zum 30. April 2009 vorgeschrieben worden.

Die von der Europäischen Kommission im Jahre 2005 initiierte Transparenzinitiative hatte unter anderem zum Ziel, die Europäische Union offener und zugänglicher zu machen, besser über die Verwendung der EU-Haushaltsmittel zu informieren und der Öffentlichkeit mehr Rechenschaft über die Arbeit der EU-Organe und -Einrichtungen zu geben.
Im Ergebnis dieser Initiative hat sich die EU zu vollständiger Transparenz in Bezug auf die Empfänger von Geldern aus dem EU-Haushalt verpflichtet. Seit dem Jahre 2008 sind die Daten der Empfänger von Zuschüssen aus den Strukturfonds, ab 2009 die Daten der Empfänger von Geldern im Rahmen der Gemeinsamen Agrarpolitik zu veröffentlichen. Es besteht nunmehr auf Gemeinschaftsebene eine Verpflichtung für die Mitgliedstaaten, Informationen über Empfänger von EU-Geldern zu veröffentlichen. Diese Verpflichtung wurde durch das Gesetz zur Veröffentlichung von Informationen über die Zahlung von Mitteln aus den Europäischen Fonds für Landwirtschaft und Fischerei (AFIG) umgesetzt

Die Länder haben die Daten der Bundesregierung zur Verfügung gestellt. Diese hat sie mittlerweile – mit einiger Verzögerung – veröffentlicht.

In der Zwischenzeit hatten sich mehrere Gerichte mit Klagen betroffener Landwirte gegen die Offenlegung ihrer Identität im Zusammenhang mit der Veröffentlichung der Fördermitteldaten befasst, auch das Verwaltungsgericht Mainz und das Oberverwaltungsgericht Koblenz. Während die erste Instanz das Verwaltungsgericht Mainz auf Antrag verschiedener rheinland-pfälzischer Landwirte im Eilverfahren entschied, dass die Veröffentlichung von Subventionsdaten im Internet zunächst zu unterbleiben habe, sah das Oberverwaltungsgericht Koblenz auf die Beschwerde des zuständigen Landwirtschaftsministeriums hin keine durchgreifenden Bedenken.

Es sah in einem Teil der Fälle einen wirksamen Verzicht der Landwirte auf ihr Datenschutzrecht, denn in den Antragsformularen aus dem Jahr 2008 sei bereits auf die Veröffentlichung hingewiesen worden. Mit Einreichung des Antrags hätten sie dies also hingenommen. Bei früheren Anträgen könne offen bleiben, ob auch hier ein Verzicht vorliege, denn die Veröffentlichung sei durch überwiegende öffentliche Interessen gerechtfertigt. Nach den europarechtlichen Vorschriften diene sie der Herstellung von Transparenz und damit der öffentlichen Kontrolle der zweckentsprechenden Verwendung von EU-Geldern. Hierfür bestehe hinsichtlich der Agrarsubventionen ein besonderes Bedürfnis, weil die EU jährlich fast die Hälfte des gesamten EU-Haushalts für die Agrarpolitik ausgebe. Die Veröffentlichung der Zuwendungen belaste den Antragsteller auch nicht unverhältnismäßig, weil die Daten über erhaltene Subventionen nicht den Kernbereich seiner persönlichen Lebensführung betreffen würden.

Der LfD hatte dies in seiner Stellungnahme gegenüber dem Oberverwaltungsgericht Koblenz anders beurteilt: Ein Verzicht durch Stillschweigen ist dem Datenschutzrecht fremd. Basis für eine Datenverarbeitung kann, neben einem rechtmäßigen Gesetz, nur die Einwilligung des Betroffenen sein. Diese muss freiwillig, d.h. frei von – auch faktischen – Zwängen sein und kann, anders als das Oberverwaltungsgericht dies für den Verzicht angenommen hat, auch jederzeit widerrufen werden (vgl. § 5 Abs. 2 LDSG). Diese Voraussetzungen sieht der LfD hier nicht erfüllt. Im Übrigen sieht er im zunehmenden Transparenzbestreben der öffentlichen Hand die Gefahr einer Aushöhlung des informationellen Selbstbestimmungsrechts. Insbesondere durch die Nutzung des Mediums Internet findet eine erhebliche Grenzverschiebung zwischen Privatheit und Öffentlichkeit statt. Transparenz bedeutet, das Handeln der staatlichen Organe nachvollziehbar zu machen, aber nicht die Adressaten dieser Handlungen der Öffentlichkeit preiszugeben. In den konkreten Fällen hätte man z.B. durch das Festlegen einer Bagatellgrenze und die Beschränkung des Zugriffs auf EU-Bürger einen besseren Schutz des Persönlichkeitsrechts erzielen können, ohne dabei auf die gebotene Transparenz verzichten zu müssen.

Fazit:
Der Gedanke der Transparenz wird allzu oft pauschal gegen den Datenschutz ausgespielt – und das nicht nur bei der Veröffentlichung von Subventionsdaten. Auch in anderen Bereichen beobachtet der LfD besorgt die zunehmende, oftmals gedankenlose Veröffentlichung persönlicher Daten im Internet, um Verwaltungshandeln transparent zu machen. Die Grenze zwischen verfassungsrechtlich gebotener und verfassungsrechtlich begrenzter Transparenz muss im Einzelfall auf der Grundlage einer umfassenden Rechte- und Güterabwägung festgelegt werden, wobei immer ein schonender Ausgleich der betroffenen Interessen versucht werden muss.

(Weitere Informationen unter http://www.lda.brandenburg.de/sixcms/detail.php?id=bb2.c.539008.de)

6. Verbraucherschutz und Beschäftigtendatenschutz

6.1 Verbraucherschutz

6.1.1 RFID (Radio Frequency Identification)

Die RFID-Technologie ist eine Anwendung mit großem Potential, deren technische Entwicklung lange noch nicht abgeschlossen ist. Der Einsatz der RFID-Technologie ermöglicht es, Daten mittels Radiowellen ohne Sichtkontakt und berührungslos zu übertragen. Das System besteht aus einem Transponder (sog. „Tag“), der auf dem zu kennzeichnenden Trägerobjekt angebracht wird und einem Lesegerät. Die RFID-Tags bestehen aus einem elektrischen Mikrochip nebst Antenne zum Senden und Empfangen von Funkwellen. Sie sind direkt an dem Produkt, beispielsweise in einem Klebeetikett oder in einer kleinen Plastikkarte, angebracht. Auf diesen Tags können Informationen wie ein Nummerncode gespeichert werden. Um die auf dem Chip gespeicherten Informationen erfassen zu können, wird ein entsprechendes Lesegerät benötigt. Dieses setzt sich aus einem Sender, einem Empfänger und einer Antenne zusammen. Die meisten Lesegeräte sind mit einer Schnittstelle zu einem IT-System ausgestattet, damit ausgelesene Daten weitergeleitet und verarbeitet werden können. Das Lesegerät sendet in einer bestimmten Frequenz Funkwellen aus, die von dem Tag erfasst werden. Die auf dem Chip gespeicherten Daten werden dann an das Lesegerät übertragen, wo sie erfasst und gespeichert werden.

Derzeit wird RFID überwiegend im vorgelagerten Produktbereich, d.h. im Produktions- und Logistikbereichbereich sowie in der Qualitätskontrolle eingesetzt. Aus datenschutzrechtlicher Sicht bestehen hier keine Bedenken. In diesen Bereichen besteht keine Verbindung der von dem RFID-System erfassten Daten zu einzelnen Personen. Ein Personenbezug dürfte daher in der Regel nicht gegeben sein.

RFID wird aber bereits vereinzelt auch im Endkundenbereich eingesetzt. So sind zum Beispiel Kleidungsstücke, Skipässe, Fahrkarten, Veranstaltungstickets und Bibliotheken mit der RFID-Technologie ausgestattet. Es ist zu erwarten, dass in naher Zukunft die Anwendung der RFID-Technologie auch in weiteren Bereichen zunimmt. Dies kann für die Verbraucher Vorteile bringen. Zu denken ist etwa an einen besseren Schutz vor Fälschungen und die vereinfachte Geltendmachung von Gewährleistungsrechten. Die kontaktlose Übertragung der Daten bei dem Einsatz von RFID führt allerdings aus datenschutzrechtlicher Sicht auch zu speziellen Risiken. Problematisch ist, dass der Einsatz von RFID-Systemen für den Kunden nicht erkennbar ist. Der Kunde ist ohne Schutz- und Kontrollmöglichkeit der Gefahr einer ungewollten und unkontrollierbaren Datenerfassung und Verarbeitung ausgesetzt. Auch können die Lesegeräte grundsätzlich automatisch alle in ihre Reichweite gelangenden Tags erfassen, soweit die technischen Voraussetzungen dazu bestehen. Gleichgültig dabei ist, ob der Tag zufällig in die Reichweite des Lesegerätes gelangt oder nicht. Solange ein Chip nicht deaktiviert ist, kann er grundsätzlich auch ausgelesen werden. Sowohl das Missbrauchsrisiko als auch das Risiko, dass Bewegungsprofile erstellt werden, ist daher besonders hoch.

Betrachtet man sich die bestehenden Regelungen des Bundesdatenschutzgesetzes, so gilt für den Einsatz von RFID Folgendes:

Werden personenbezogene Daten unmittelbar auf den Tag gespeichert (z.B. Ausweis- und Signaturkarten oder personalisierte Veranstaltungstickets), kommt das Bundesdatenschutzgesetz mit seinen gesetzlichen Vorgaben unmittelbar zur Anwendung. Die Vorschriften des BDSG sind ebenso einschlägig, wenn ein Kunde ein mit einem RFID-Tag gekennzeichnetes Produkt kauft, mit einer Kunden- oder Kreditkarte zahlt und eine Verknüpfung zwischen den Produktdaten und dem Kunden hergestellt wird. Problematischer sind die Fälle des potentiellen Personenbezuges. Kauft z.B. ein Kunde in einem Supermarkt oder in einer Apotheke ein und wird dort RFID eingesetzt, so gibt der Kunde zunächst keine personenbezogenen Daten preis, wenn er bar bezahlt. Trägt er jedoch eine Einkaufstüte mit Produkten bei sich, die ebenfalls RFID-Tags enthalten, und hat er diese mit einer Kunden- oder Kreditkarte bezahlt, so könnten die gespeicherten Daten mit ausgelesen und mit dem aktuellen Einkauf verknüpft werden. Gleiches gilt, wenn der Kunde z.B. Ausweis- oder Signaturkarten mit RFID-Tags bei sich trägt und diese mit ausgelesen werden.

Im Verbraucherbereich ist daher davon auszugehen, dass an sich nicht personenbezogene Daten zumindest „potentiell personenbeziehbar“ sind. Hier muss unterschieden werden zwischen einer gezielten und einer zufälligen Verknüpfung. Bei einer gezielten Verknüpfung mit personenbezogenen Daten findet das Bundesdatenschutzgesetz Anwendung, mit der Folge, dass die Erhebung, Verarbeitung und Nutzung dieser Daten nur noch nach den gesetzlichen Vorschriften zulässig ist. Problematischer stellt sich das zufällige Auslesen dar. Hier muss unterschieden werden: Das rein zufällige Auslesen fremder Daten führt mangels Zielgerichtetheit nicht zur Anwendung des Bundesdatenschutzgesetz. Erst wenn die ausgelesenen Daten weiter verarbeitet werden, sind die

Vorschriften des Bundesdatenschutzgesetzes einschlägig. Die Daten werden in diesen Fällen in der Regel ohne Einwilligung des Betroffenen erhoben und sind sofort zu löschen.

Aufgrund der dargestellten Problematik erkennen die Betroffenen oft nicht, dass ein zufälliges Auslesen erfolgt und ob ein Personenbezug hergestellt wurde. Da das BDSG in diesen Fällen nicht einschlägig ist, liegt eine gefährliche Grauzone vor.

Die Gefahren wurden sowohl auf nationaler als auch auf europäischer Ebene erkannt.

So hat die Bundesregierung im Januar 2008 einen Bericht zu den Aktivitäten, Planungen und zu einem gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der zukunftsträchtigen Technologie vorgelegt. Darin werden folgende Bedingungen für den Einsatz von RFID geknüpft (BT-Drs. 16/7891):

- Der Einsatz von RFID-Chips und Lesegeräten muss gekennzeichnet sein, auf Art und Verwendungszweck der gespeicherten Daten muss hingewiesen werden.
- Auf heimliche Profilbildung muss verzichtet werden.
- Die Sicherheit der ausgelesenen Daten muss gewährleistet sein.
- Deaktivierungsmöglichkeiten sollten bevorzugt nach dem „Opt-in Prinzip“ vorgesehen werden.
- Datensparsamkeit ist zu gewährleisten.
- Bevorzugt wird eine Selbstverpflichtung der Wirtschaft.

Die mit dem Einsatz der RFID-Technologie verbundene Datenschutzproblematik war auch ein Thema der 72. Datenschutzkonferenz des Bundes und der Länder sowie der Konferenz der obersten Datenschutzaufsichtbehörden für den nicht-öffentlichen Bereich. Es wurde jeweils eine Entschließung hierzu gefasst.

- http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=072_rfid
- http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20061109_rfid

Auch hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe erarbeitet. Diese ist auf der Internetseite des LfD unter folgendem Link abrufbar:

http://www.datenschutz.rlp.de/downloads/oh/ak_oh_rfid_14_12_06.pdf

Auf europäischer Ebene wurde am 12. Mai 2009 eine Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützen Anwendungen erlassen. Die wesentlichen Inhalte der Empfehlung lassen sich wie folgt zusammenfassen:

Datenschutzfolgenabschätzung
Vor dem Einsatz neuer Anwendungen sollen alle RFID-Betreiber die Konsequenzen für den Datenschutz und die Privatsphäre abschätzen und dabei auch abklären, ob die Anwendung zur Überwachung einer Person eingesetzt werden könnte. Die Anforderungen der Datenschutzfolgenabschätzung hängen dabei von den Datenschutzrisiken der Anwendung ab. Die Betreiber sollen die technischen und organisatorischen Voraussetzungen treffen, um den Datenschutz zu gewährleisten. Die Datenschutzfolgenabschätzung soll spätestens sechs Wochen vor der Einführung der Anwendung der zuständigen Stelle zur Verfügung gestellt werden. Dabei sollen die Betreiber eine Person oder Personengruppe benennen, die für die Prüfung der Folgenabschätzung und die Kontrolle der dauerhaften Eignung der technischen und organisatorischen Maßnahmen zum Datenschutz verantwortlich ist. Die Wirtschaft soll in Zusammenarbeit mit den jeweiligen Beteiligten aus der Zivilgesellschaft zur Unterstützung der Umsetzung der Datenschutzfolgenabschätzung einen Rahmen für eine Datenschutzfolgenabschätzung aufstellen. Dieser Rahmen ist der Artikel 29-Datenschutzgruppe bis Mai 2010 vorzulegen.

Information und Transparenz
Die Mitgliedstaaten sollen dafür Sorge tragen, dass unabhängig von den bestehenden Rechtsvorschriften zum Datenschutz und zur Wahrung der Privatsphäre die Betreiber für jede ihrer Anwendung eine kurze, genaue und leicht verständliche Information ausarbeiten und veröffentlichen. Diese Information soll mindestens folgende Angaben enthalten:

- Name und Anschrift des Anbieters
- Zweck der Anwendung
- Art der Daten, die durch die Anwendung verarbeitet werden, insbesondere, ob personenbezogene Daten verarbeitet werden und ob der Standort des RFID-Tags überwacht wird
- Zusammenfassung der Datenschutzfolgenabschätzung
- wahrscheinliche Risiken, die sich aus dem Einsatz von RFID-Tags in Anwendungen ergeben können, und Maßnahmen zur Minderung der Risiken
- Information über die Präsenz von RFID-Lesegeräten und RFID-Tags (nur im Einzelhandel) durch ein europaweit einheitliches Logo

Deaktivierungspflicht im Einzelhandel
Einzelhändler sollen die in ihrer Anwendung genutzten RFID-Tags am Verkaufsort deaktivieren oder entfernen, es sei denn,

die Verbraucher stimmen nach Aufklärung über die erforderlichen Informationen der weiteren Betriebsfähigkeit des RFID-Tags zu.
Eine Deaktivierung oder Entfernung ist auch dann nicht erforderlich, wenn nach der Datenschutzfolgenabschätzung feststeht, dass wahrscheinlich keine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten durch die Einzelanwendung des RFID-Tags besteht.
Die Deaktivierung soll sofort und kostenlos erfolgen. Auch soll ermöglicht werden, dass die Verbraucher überprüfen können, ob eine Deaktivierung oder Entfernung tatsächlich erfolgt ist.
Empfohlen wird generell ein einfaches und kostenloses Mittel zur Deaktivierung oder Entfernung des RFID zur Verfügung zu stellen.

Nach wie vor wird diskutiert, ob es ausreicht, dass die Wirtschaft sich selbst verbindliche Regeln für den Einsatz der RFID-Technologie auferlegt, um den Gefahren für die Privatsphäre im Zusammenhang mit dem Einsatz von RFID zu begegnen. Eine wirksame verbindliche Selbstverpflichtungserklärung der Wirtschaft liegt bisher nicht vor.

Alternativ könnte eine gesetzliche Regelung für den Einsatz von RFID geschaffen werden. Denkbar wäre es, eine Vorschrift ähnlich dem § 6b BDSG (Videoüberwachung) in das Bundesdatenschutzgesetz selbst einzufügen oder ein eigenständiges „RFID-Gesetz“ zu erlassen. Die Gesetzgebungskompetenz liegt beim Bund, solange öffentliche Stellen des Bundes oder nichtöffentliche Stellen RFID einsetzen. Wird die RFID-Technologie jedoch von öffentlichen Stellen des Landes eingesetzt, wie dies beispielsweise in der Zentralbibliothek der Johannes Gutenberg-Universität in Mainz der Fall ist, ist der Landesgesetzgeber zuständig.

Bereits jetzt ist es erforderlich, dass die Betroffenen umfassend über die Chancen und die Risiken der RFID-Technologie informiert werden. Der LfD hat daher im Zusammenhang mit dem Ministerium für Umwelt, Forsten und Verbraucherschutz im Jahr 2008 einen Verbraucherdialog RFID begonnen. Nach der Auftaktveranstaltung am 25. August 2008 wurden drei Arbeitgruppen gebildet und zwar

- Transparenz/Anwendungsbereiche
- Datenschutz
- Verbraucherinformation.

Ende Oktober traf sich die Arbeitsgruppe Datenschutz ein zweites Mal. Die Beratungen sind noch nicht abgeschlossen. Es deutet sich bereits jetzt an, dass die Forderungen der Wirtschaft und des LfD für einen datenschutzgerechten Einsatz der RFID-Technologie weit auseinander liegen. Vertreter der RFID einsetzenden Wirtschaft sind weitgehend der Auffassung, dass im Hinblick auf die europäischen Entwicklungen derzeit weder eine Selbstverpflichtungserklärung noch eine nationale gesetzliche Regelung sinnvoll seien. Diese Position ist für den LfD nicht haltbar. Der LfD hält gerade auch deshalb, weil es bisher keine wirksame verbindliche Selbstverpflichtungserklärung der Wirtschaft gibt, eine gesetzliche Regelung für erforderlich und notwendig.

6.1.2 Auskunfteien

Beinahe wöchentlich erreichen den LfD Anfragen zum Thema Auskunfteien. Dabei geht es immer wieder um die Fragen: Woher hat die Auskunftei meine Daten? An wen hat sie sie weitergegeben? Werden diese Daten jetzt gelöscht?

Das Bundesdatenschutzgesetz regelt die Datenverarbeitung durch Auskunfteien ausdrücklich in § 29. Nach dieser Bestimmung ist den Wirtschaftsauskunfteien die Speicherung personenbezogener Daten (zum Zweck der Übermittlung/Auskunftserteilung) erlaubt, wenn kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen berührt wird. Solche schutzwürdigen Interessen der Betroffenen sind im allgemeinen dann nicht gegeben, wenn von den Auskunfteien ausschließlich für Kreditentscheidungen bzw. Bonitätsprüfungen bedeutsame Daten gespeichert werden und diese Daten richtig sind (z.B. Beruf, Einkommensverhältnisse, Vermögen, geschäftliche Aktivitäten, Zahlungsweise, usw.). Die Daten stammen meist aus allgemein zugänglichen Quellen wie aus Telefon- und Adressbüchern, aus öffentlichen Registern oder aus den Schuldnerverzeichnissen der Amtsgerichte.

Das Bundesdatenschutzgesetz erkennt mit § 29 an, dass Wirtschaftsauskunfteien zum Schutze der Wirtschaft und der Allgemeinheit vor Kreditbetrug und sonstigen Zahlungsausfällen ihre Berechtigung haben. Denn bekanntermaßen werden nicht alle Rechnungen ordnungsgemäß bezahlt, nicht alle Kredite vereinbarungsgemäß zurückgeführt, usw. Die redlichen Teilnehmer am Wirtschaftsleben müssen solche Zahlungsausfälle zwangsläufig mittragen.

Eine Übermittlung von personenbezogenen Daten an Dritte (Auskunftserteilung) ist den Auskunfteien nach dem Bundesdatenschutzgesetz erlaubt, wenn der Empfänger (Anfragende) zuvor ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung bzw. Auskunftserteilung hat.

Ein berechtigtes Interesse an einer Wirtschaftsauskunft wird vor allem in den Fällen gesehen, in denen ein Vertragspartner gegenüber dem anderen Vertragspartner Vorleistungen erbringt oder sonst ein finanzielles Risiko eingeht bzw. einzugehen beabsichtigt, wie z. B. Bestellung bzw. Lieferung auf Rechnung, Ratenkauf, Kreditvergaben, Hypothekenangelegenheiten, Leasinggeschäfte, Mobiltelefonverträge, Mietverträge, Werkverträge, usw.

Zur Verhinderung von Missbrauchsfällen prüfen die Wirtschaftsauskunfteien selbst und die Datenschutzaufsichtsbehörden Einzelfälle von Auskunftserteilungen stichprobenmäßig dahingehend nach, ob zu dem bei der Auskunftseinholung geltend gemachten Interesse auch ein realer Hintergrund besteht.

Nach § 33 Abs. 1 BDSG müssen Auskunfteien die Betroffenen über die erstmalige Übermittlung und die Art der übermittelten Daten benachrichtigen. Dies geschieht üblicherweise durch ein Formschreiben, das viele Betroffene veranlasst, sich an den LfD zu wenden.

Nach § 34 Abs. 1 BDSG besteht ein Anspruch auf Auskunft über die zur Person gespeicherten Daten. Auskunft über Herkunft und Empfänger der Daten kann nach den gesetzlichen Vorschriften allerdings nur dann verlangt werden, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

Wenn Daten unrichtig sind, kann gem. § 35 Abs. 1 BDSG Berichtigung verlangt werden. Dies setzt voraus, dass der Betroffene die Unrichtigkeit nachweist.

Daten müssen nur dann von der Auskunftei gelöscht werden, wenn ihre Speicherung unzulässig ist oder wenn eine Prüfung am Ende des vierten Kalenderjahres nach erstmaliger Speicherung ergibt, dass eine längere Speicherung nicht mehr erforderlich ist. Wenn eine Auskunftei also nur die o. g. kreditrelevanten Daten speichert, ist davon auszugehen, dass dies – auch ohne Einwilligung des Betroffenen – datenschutzrechtlich zulässig ist.

Fazit:
Auskunfteien dürfen grundsätzlich personenbezogene Daten erheben, speichern und übermitteln, wenn sie für Bonitätsprüfungen relevant sind. Betroffene haben Anspruch auf Auskunft, was über sie gespeichert ist, woher die Daten stammen und an wen sie übermittelt wurden.

6.1.3 Bonitätsabfragen durch die Wohnungswirtschaft

Eine besondere Situation ergibt sich im Bereich der Wohnungswirtschaft: Viele Vermieter wollen sich – vermeintlich – absichern, bevor sie Wohnraum vermieten, um Mietausfällen entgegenzuwirken. Aus diesem Grund fragen sie bei Wirtschaftsauskunfteien nach, ob dort Kreditrisiken über potentielle Mieter bekannt sind. Das ist als berechtigtes Interesse der Vermieter durchaus anzuerkennen. Auf der anderen Seite stehen aber auch die schutzwürdigen Interessen der zukünftigen Mieter am Ausschluss einer solchen Abfrage. Beides ist bei einer datenschutzrechtlichen Bewertung gegeneinander abzuwägen.

Die Aufsichtsbehörden befassen sich schon lange mit dieser Problematik. Sie haben im Oktober 2009 daher ihre Auffassung zu den Rechtmäßigkeitsvoraussetzungen solcher Anfragen in einem Beschluss veröffentlicht (http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20091022Umlauf_boniauskmiet).

Eine Umfrage bei den rheinland-pfälzischen Wohnungsbaugesellschaften nach der dort üblichen Praxis hat ergeben, dass knapp die Hälfte der Befragten Bonitätsauskünfte über zukünftige Mieter einholt. Die Vorgehensweise ist dabei durchaus unterschiedlich, aber in kaum einem Fall den gesetzlichen Bestimmungen entsprechend. Die datenschutzrechtliche Problematik zeigt sich in folgenden Punkten:

- Zeitpunkt der Anfrage
  Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrages mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt. Denn berechtigtes Interesse an der Auskunft heißt, dass ein finanzielles Ausfallrisiko bestehen muss. Dies besteht noch nicht bei bloßem Interesse an einer Wohnung, sondern erst unmittelbar vor Abschluss eines Mietvertrages.
- Umfang der Auskünfte
  Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen sind unproblematisch. Bei sonstigen Daten über negatives Zahlungsverhalten muss die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen sein oder es darf – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegen. Zudem muss eine Bagatellgrenze von insgesamt 1.500 Euro überschritten werden (diese berechnet sich aus durchschnittlich drei Monatsmieten). Denn nur dies sind Daten, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen.

- Protokollierung
  Die Protokollierung ist eine vorbeugende Maßnahme der Zugriffskontrolle nach Nr. 3 der Anlage zu § 9 BDSG. Die Rechnungsstellung der Auskunfteien stellen keine hinreichende Protokollierung im Sinne dieser Vorschrift dar, denn daraus können missbräuchliche Zugriffe dem einzelnen Nutzer nicht zugeordnet werden. Schufa-Kunden beispielsweise sind vertraglich zur zeitgenauen und mitarbeiterbezogenen Protokollierung verpflichtet. Dokumentationspflichten gelten übrigens auch bei telefonischen Abfragen.
- Nutzung einer Zugangskennung durch mehrere Mitarbeiter
  Dies stellt einen Widerspruch zu Nr. 2 in Verbindung mit Nr. 5 sowie Nr. 3 der Anlage zu § 9 BDSG dar. Denn auch bei dieser Konstellation können missbräuchliche Zugriffe dem einzelnen Nutzer nicht zugeordnet werden.
- Aufzeichnungspflicht bei Online-Abfragen
  Eine solche Aufzeichnungspflicht sieht § 29 Abs. 2 Nr. 4 BDSG ausdrücklich vor. Bei Online-Abfragen müssen durch die Wohnungsbaugesellschaft daher die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung aufgezeichnet werden.
- Schufa-Selbstauskünfte/Einwilligung
  Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten stellt eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen dar und ist daher nicht zulässig.
- Aufbewahrung der Abfrageergebnisse
  Es ist völlig ausreichend die Tatsache der Abfrage mit Grund (= berechtigtes Interesse), das Datum und das Endergebnis aufzubewahren.
- Interne Regelungen der Arbeitsabläufe
  Die Arbeitsabläufe sollten schriftlich festgehalten sein: Wer darf in welchen Fällen Abfragen tätigen und wie wird mit erhobenen Daten weiter verfahren?

Die befragten Wohnungsbaugesellschaften wurden aufgefordert, diese Vorgaben – soweit noch nicht erfolgt – umzusetzen. Da die betroffenen Auskunfteien entsprechende Abfrageformate mit reduziertem Umfang nicht zur Verfügung stellen, tun sich die Wohnungsbaugesellschaften mit einer Anpassung ihrer Verfahren schwer. Der LfD befindet sich weiterhin im Dialog mit den Wohnungsbauverbänden, um eine datenschutzgerechte Lösung zu erzielen.

Wie wichtig die Einhaltung auch der technisch-organisatorischen Datenschutzregelungen ist, zeigte sich am konkreten Fall:

Nach Pressehinweisen auf unzulässige Bonitätsabfragen im Vorfeld der Kommunalwahl hat der LfD bei der betroffenen Wohnungsbaugenossenschaft örtliche Feststellungen getroffen und die in Anspruch genommene Wirtschaftsauskunftei über die zuständige Datenschutzaufsichtsbehörde um Stellungnahme gebeten. Dies hat ergeben, dass in mehreren Fällen Bonitätsabfragen zu Personen erfolgt sind, die mit der Wohnungsbaugenossenschaft in keinerlei Geschäftsbeziehung standen. In technischer Hinsicht ist dabei von Bedeutung, dass kein Nachweis darüber vorlag, wann und an welche Personen die beantragten Zugangskennungen ausgegeben wurden. Darüber hinaus befand sich die Liste mit den Zugangsdaten einschließlich der vergebenen Passwörter entsprechend beschriftet in einem unverschlossenen Schrank der Geschäftsstelle, so dass prinzipiell alle Beschäftigen, einschließlich Auszubildende und Praktikanten Bonitätsabfragen vornehmen konnten.

Derartige Abfragen konnten grundsätzlich an jedem PC mit Internet-Browser erfolgen, zusätzliche Sicherungsmechanismen wie Client-Zertifikate oder sonstige zusätzlichen Authentifizierungsmechanismen kamen nicht zum Einsatz. Eine nach den Vertragsbedingungen der Auskunftei vorgeschriebene Protokollierung der einzelnen Abfragen war nicht erfolgt.

Da in der Angelegenheit von den Betroffen bereits Strafanträge nach § 34 BDSG gestellt wurden, hat der LfD hiervon abgesehen. Für die Einleitung eines Bußgeldverfahrens ist die Klärung erforderlich, inwieweit die Abfragen durch Mitarbeiter der Wohnungsbaugenossenschaft vorgenommen oder die Zugangsdaten an Dritte weitergegeben wurden. Entsprechende aufsichtliche Maßnahmen wurden daher zunächst bis zum Abschluss des laufenden staatsanwaltschaftlichen Ermittlungsverfahrens zurückgestellt.

6.1.4 LottoCard

Im Berichtszeitraum haben sich viele LottoCard-Inhaber an den LfD gewandt. Denn das Verfahren zur Verlängerung bzw. Neubeantragung einer solchen Karte gab Anlass zu datenschutzrechtlicher Kritik.

Die LottoCard ist eine personengebundene Karte mit dem Zweck, das Lottospielen zu vereinfachen: Man kann sich das Ausfüllen eines Lottoscheines sparen und mögliche Gewinne werden automatisch auf das Bankkonto überwiesen. Diese Karte muss alle zwei Jahre erneuert werden. Zu diesem Zeitpunkt ist es üblich, dass die Annahmestelle bei Vorlage der LottoCard ein Formular ausdruckt, in dem die bekannten Daten bereits ausgefüllt sind. Dies sind Name, Anschrift und Kontoverbindung. Die Lotto-

kunden sollten diese Angaben überprüfen und ggf. korrigieren. Zudem sollten sie auch ihren Geburtstag und ihren Geburtsort angeben. Die Kontoverbindungsdaten der Spieler waren also für die Annahmestellen offen einsehbar, sowohl bei Verlängerung der Karte als auch bei Neuantrag. Gerade die Kenntnis dieser Daten war für die Annahmestellen aber nicht erforderlich.

Die Lotto Rheinland-Pfalz GmbH in Koblenz hat das Verfahren auf Betreiben des LfD nunmehr modifiziert: Bei Beantragung einer LottoCard trägt der Spielteilnehmer seine Kontoverbindungsdaten auf dem Antragsformular ein und verschließt dieses in einem vorbereiteten Umschlag, der dann direkt an die Zentrale weitergeleitet wird, ohne dass Mitarbeiter davon Kenntnis nehmen können. Bei den Aktualisierungsbögen werden zukünftig nur die letzten vier Stellen der Kontonummer ausgedruckt werden. Somit haben die Annahmestellen keinen Zugriff auf die vollständigen Kontoverbindungsdaten.

Auch die Abfrage von Geburtstag und Geburtsort traf auf Unverständnis bei den Lottospielern. Hiergegen bestanden jedoch keine datenschutzrechtlichen Bedenken, da die Lotto Rheinland-Pfalz GmbH als Veranstalterin von Glücksspielen nach dem Glücksspielstaatsvertrag zur Erhebung der Daten verpflichtet ist. Um diese Datenerhebung zu vermeiden, haben die Spielteilnehmer die Möglichkeit, auf eine LottoCard zu verzichten und anonym am Lottospiel teilzunehmen.

Nach § 8 Glücksspielstaatsvertrag sind alle Veranstalter von Glücksspielen, also auch die Lotto Rheinland-Pfalz GmbH, verpflichtet, ein übergreifendes Sperrsystem zu unterhalten. Die zur Teilnahme am Sperrsystem verpflichteten Veranstalter sperren Personen, die dies beantragen (Selbstsperre) oder von denen sie aufgrund der Wahrnehmung ihres Personals oder aufgrund von Meldungen Dritter wissen oder aufgrund sonstiger tatsächlicher Anhaltspunkte annehmen müssen, dass sie spielsuchtgefährdet oder überschuldet sind, ihren finanziellen Verpflichtungen nicht nachkommen oder Spieleinsätze riskieren, die in keinem Verhältnis zu ihrem Einkommen oder Vermögen stehen (Fremdsperre). In der Sperrdatei werden die für eine Sperrung erforderlichen Daten verarbeitet und genutzt. Gem. § 23 Glücksspielstaatsvertrag gehören hierzu auch das Geburtsdatum und der Geburtsort. Diese Daten werden als erforderlich angesehen, um Personenverwechslungen zu vermeiden.

6.1.5 Scoring

Besondere Beachtung bei den Verbrauchern findet das sog. Scoring. Viele wissen nicht, was das überhaupt ist bzw. wie sich ihr persönlicher Scorewert zusammensetzt und welche Auswirkungen er auf ihr tägliches Leben hat bzw. haben kann. Der LfD betreibt hier Aufklärungsarbeit so gut er kann bzw. so gut es ihm der Gesetzgeber bisher ermöglicht hat:

Scoring ist ein mathematisch-statistisches Verfahren zur Berechnung der Wahrscheinlichkeit, mit der eine bestimmte Person ein bestimmtes Verhalten zeigen wird.

Viele Auskunfteien, darunter als bekannteste die Schufa, bilden Scorewerte, die sie an ihre Kunden übermitteln. Aber auch Kreditinstitute selbst berechnen Scorewerte. Sie stellen dann in der Regel einen Richtwert dafür dar, ob ein Vertrag mit dem Betroffenen abgeschlossen wird. Derzeit erhalten zwar Betroffene Auskunft über ihren Scorewert, aber nicht darüber, wie er sich zusammensetzt. Dabei können viele Merkmale eine Rolle spielen: z.B. die Adresse oder die Zugehörigkeit zu einer bestimmten Berufs- oder Altersgruppe. Wenn die Betroffenen jedoch nicht wissen, auf welcher Grundlage ihr Scorewert gebildet wird, haben diese nur wenig Möglichkeiten, sich dagegen zur Wehr zu setzen, indem sie z.B. die zugrunde liegenden Werte berichtigen. Die Zusammensetzung des Scorewertes bleibt sozusagen das Geheimnis der Auskunfteien.

Die sog. Scoring-Novelle des Bundesdatenschutzgesetzes, die am 1.April 2010 in Kraft tritt, soll hier für Verbesserungen sorgen (s.a. Tz. 2.2.2). Künftig wird geregelt, wann ein Scorewert erhoben und verwendet werden darf (§ 28b BDSG n.F.). Zudem wird der Auskunftsanspruch ausdrücklich auf die dem Scorewert zugrunde liegenden Datenarten und eine verständliche Erklärung des Scoringverfahrens ausgedehnt (§ 34 Abs. 2 BDSG n.F.).

Es gilt aber bereits heute gem. § 6a BDSG der Grundsatz, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Praktisch bedeutet dies, dass das Kreditinstitut nicht ausschließlich aufgrund eines Scorewertes über eine Kreditvergabe entscheiden darf. Der Scorewert ist immer nur ein Bestandteil der Entscheidung, die letztlich von einem Menschen aufgrund einer Gesamtwürdigung der bekannten Tatsachen getroffen werden muss. Wenn sich eine Bank also darauf beruft, dass ein Kredit wegen eines „schlechten“ Scorewertes abgelehnt wurde, so kann dies einen Verstoß gegen § 6a BDSG bedeuten.

Verbraucherinformation Scoring
http://www.bmelv.de/cae/servlet/contentblob/638114/publicationFile/36026/Scoring.pdf

6.2 Beschäftigtendatenschutz bei öffentlichen Arbeitgebern

6.2.1 Arztgeheimnis im Disziplinarverfahren

Wie dem LfD bekannt wurde, hatte ein Finanzamt in einer Disziplinarangelegenheit versucht, bei einer Klinik medizinische Daten des Beschäftigten in Form eines Reha-Entlassberichts zu erhalten. In dem Schreiben an die Klinik führte das Finanzamt aus, durch die Übersendung des Berichts könne aus Vereinfachungsgründen eine mündliche Vernehmung des behandelnden Arztes vermieden werden; es bestehe eine diesbezügliche Auskunftsverpflichtung der Klinik nach dem Landesdisziplinargesetz auch in Bezug auf den Namen des behandelnden Arztes.

Der LfD hat das Finanzamt auf Folgendes hingewiesen: Das Landesdisziplinargesetz regelt in § 30 Abs. 1, dass die Bestimmungen der Strafprozessordnung über die Pflicht, als Zeuge auszusagen oder als Sachverständiger ein Gutachten zu erstatten, entsprechend gelten. Nach § 53 Abs. 1 Nr. 3 StPO sind Ärzte über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist, zur Verweigerung des Zeugnisses berechtigt.

Ohne ausdrückliche Schweigepflichtsentbindungserklärung des Beamten besteht demnach keine Verpflichtung der Klinik, den Namen des behandelnden Arztes mitzuteilen. Für die Aufforderung, den vollständigen Reha-Entlassbericht zu übersenden, gilt Entsprechendes, da ansonsten die o.g. Bestimmungen der Strafprozessordnung umgangen würden.

Soweit die Klinik vorliegend den Reha-Entlassbericht als Leistungserbringer i.S.d. Sozialgesetzbuches für einen Sozialleistungsträger gefertigt hat, kommen darüber hinaus die Vorschriften zum Schutz des Sozialgeheimnisses zur Anwendung. Die Verwendung des Berichts für ein behördliches Disziplinarverfahren stellt datenschutzrechtlich eine Nutzungsänderung dar. Diese ist u.a. dann zulässig ist, wenn die Daten für die Erfüllung von Aufgaben nach einer anderen Vorschrift des Sozialgesetzbuches als derjenigen, für die sie erhoben wurden, erforderlich ist (§ 67c Abs. 2 SGB X). Eine solche Vorschrift existiert im Sozialgesetzbuch jedoch nicht, so dass die Nutzung der vorhandenen Daten für ein behördliches Disziplinarverfahren (und damit selbstverständlich auch die Weitergabe der Daten an das Finanzamt) nicht zulässig ist. Dies betrifft auch die Mitteilung des Namens des behandelnden Arztes; auch diese Information wird vom Sozialgeheimnis umfasst.

Da das Finanzamt den Vorgang an die Oberfinanzdirektion Koblenz abgab, konnte die Angelegenheit bisher noch nicht abgeschlossen werden.

6.2.2 „Bewerbergooglen“ durch öffentliche Arbeitgeber

Laut einer im Sommer 2009 veröffentlichten Studie des Bundesverbraucherministeriums suchen rund ein Viertel der Arbeitgeber gezielt im Internet nach Informationen über Bewerber. Bei rund 25 Prozent der Firmen kommt es vor, dass ein Bewerber erst gar nicht zum Vorstellungsgespräch eingeladen wird. Der LfD geht aufgrund der Rückmeldungen in Fortbildungsveranstaltungen davon aus, dass auch öffentliche Arbeitgeber den Verlockungen des Internets bei der Informationsbeschaffung für die Bewerberauswahl erliegen, wenn auch nicht in dem genannten Ausmaß.

Eine datenschutzrechtliche Prüfung dieser Vorgehensweise hat eine Vielzahl von Gesichtspunkten zu berücksichtigen:

- Das Bundesverfassungsgericht hat in der sog. Computergrundrechtsentscheidung (Az. 1 BvR 370/07 und 1 BvR 595/07) Grundsätze für Internetrecherchen durch öffentliche Stellen aufgestellt (s.a. Tz. 2.2.1, Tz. 2.2.5, Tz. 7.3, Tz. 13.3): Hiernach ist dem Staat die Kenntnisnahme öffentlich zugänglicher – auch personenbezogener – Informationen grundsätzlich nicht verwehrt. Daher liege kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. So liege es etwa, wenn die Behörde eine allgemein zugängliche Webseite im World Wide Web aufruft, eine jedem Interessierten offen stehende Mailingliste abonniert oder einen offenen Chat beobachtet. Ein Eingriff in das Recht auf informationelle Selbstbestimmung könne allerdings gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und ggf. unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Hierfür bedürfe es einer Ermächtigungsgrundlage.
- In diesem Zusammenhang ist auch die Regelung des § 2 Abs. 5 LDSG zu sehen, wonach personenbezogene Daten, die allgemein zugänglich sind bzw. vom Betroffenen zur Veröffentlichung bestimmt wurden, grundsätzlich nicht dem Landesdatenschutzgesetz unterliegen. Etwas anderes gilt nur dann, wenn die allge-

mein zugänglichen Daten gesondert gespeichert und weiter verarbeitet werden.

Demnach hängt die datenschutzrechtliche Bewertung einer Internetrecherche durch öffentliche Arbeitgeber davon ab, ob Informationen erhoben werden, die mittels Suchmaschinen allgemein verfügbar sind, oder ob es sich um solche Daten handelt, die nach dem Willen des Betroffenen nur (bestimmten) Nutzern eines sozialen Online-Netzwerks zur Verfügung stehen sollen. Weiterhin muss differenziert werden, ob es sich um Daten handelt, die von dem Betroffenen selbst oder von Dritten über den Betroffenen eingestellt wurden. Ebenfalls nicht unwichtig ist die Frage, wie sich der Arbeitgeber Zugang zu diesem Netzwerk verschafft (Nutzung des eigenen privaten Accounts oder Vorgeben einer falschen Identität) und mit den erhobenen Daten umgeht. Außerdem muss geprüft werden, welcher Zweckbestimmung das Online-Netzwerk nach seinen Allgemeinen Geschäftsbedingungen unterliegt.

Der LfD geht im Rahmen seiner datenschutzrechtlichen Bewertung von folgenden Überlegungen aus:

Nutzt der Arbeitgeber personenbezogene Daten von Bewerbern, die nach der Zweckbestimmung des Netzwerks auch der Arbeitsvermittlung dienen (z.B. „XING“), ist dies datenschutzrechtlich unproblematisch und deshalb zulässig. Vor dem Hintergrund der o.g. Feststellungen des Bundesverfassungsgerichts und der Regelung in § 2 Abs. 5 LDSG bestehen auch keine Bedenken dagegen, wenn der öffentliche Arbeitgeber Informationen zur Kenntnis nimmt, die allgemein unter Verwendung von Suchmaschinen zugänglich sind.

Werden jedoch die im Internet über Bewerber verfügbaren Daten systematisch in einer Liste oder Tabelle erfasst und ausgewertet, ist hierfür eine gesonderte Rechtsgrundlage zu fordern. Die insoweit in Betracht kommenden Vorschriften im Landesbeamtengesetz bzw. § 31 LDSG setzen die „Erforderlichkeit“ dieser Datenerhebung voraus, was mit Blick auf die ansonsten zur Verfügung stehenden Erkenntnismöglichkeiten eines Bewerbungsverfahrens bezweifelt werden kann. Außerdem liegt bei verdeckten Informationsbeschaffungen regelmäßig ein Verstoß gegen den Grundsatz der Direkterhebung beim Betroffenen vor, so dass im Ergebnis die personaldatenschutzrechtlichen Vorgaben dieser Vorgehensweise grundsätzlich entgegenstehen.

Datenschutzrechtlich unzulässig ist nach Auffassung des LfD ebenfalls das Erheben von Informationen, die Betroffene in sozialen Online-Netzwerken einem nur eingeschränkten Personenkreis gegenüber veröffentlicht haben, z.B. nur den registrierten Nutzern des Netzwerks oder nur den sog. Freunden des Betroffenen. Denn die Allgemeinen Geschäftsbedingungen der Netzbetreiber sehen in aller Regel die Nutzung nur für private Zwecke vor. Außerdem bringen die Nutzer durch die Beschränkung der bestehenden Zugriffsmöglichkeiten zum Ausdruck, dass ihre Daten gerade nicht außerhalb der Zweckbestimmung des Netzwerks durch jedermann Verwendung finden sollen. Öffentliche Arbeitgeber verstoßen mit verdeckten Recherchen gegen die Allgemeinen Geschäftsbedingungen der Netzbetreiber, und zwar unabhängig davon, ob dabei der eigene private Account zweckwidrig verwendet wird oder sich der Arbeitgeber unter einem falschem Namen Zugang verschafft. Staatliche Stellen sind aufgrund von Art. 20 Abs. 3 GG an Recht und Gesetz gebunden. Eine heimliche Informationsbeschaffung hinter dem Rücken des Betroffenen ist mit diesen Vorgaben grundsätzlich nicht zu vereinbaren und würde die insoweit schutzwürdigen Belange der Betroffenen unverhältnismäßig beeinträchtigen.

Inwiefern diese Bewertung auch auf den privaten Bereich übertragen kann, wird derzeit unter den Datenschutzaufsichtsbehörden diskutiert. Gerichtliche Entscheidungen, die die Grenzen der Informationsbeschaffung durch den künftigen Arbeitgeber aufzeigen, liegen zumindest bislang nicht vor.

6.2.3 Datenschutz bei Telearbeit

Zu der Frage, welche rechtlichen und technisch-organisatorischen Anforderungen an die Einrichtung von Telearbeitsplätzen aus datenschutzrechtlicher Sicht zu stellen sind, hat sich der LfD im 16. Tb. (Tz. 21.7), 17. Tb. (Tz. 17.3) und 20. Tb. (Tz. 17.1) ausführlich geäußert.

Neu in diesem Zusammenhang ist die Frage, inwiefern vom Heimarbeitsplatz aus auf landes- bzw. bundeseinheitliche Verfahren (z.B. Einwohnermeldedaten, polizeiliche Verbunddateien, wie INPOL/POLIS, Daten des Kraftfahrzeugbundesamtes) zugegriffen werden darf.

Wie eine Auswertung der Protokolldaten von Zugriffen auf das landeseinheitliche Einwohnermeldeverfahren ergeben hat (21. Tb., Tz. 4.2), fanden in einem nennenswerten Umfang unzulässige Abfragen statt. Es ist jedenfalls davon auszugehen, dass durch die Situation am Heimarbeitsplatz das ohnehin vorhandene Missbrauchspotenzial noch vergrößert wird.

Eine datenschutzrechtliche Bewertung hat ebenfalls den allgemeinen Verhältnismäßigkeitsgrundsatz zu berücksichtigen. Vor dem Hintergrund, dass mit der Einrichtung

eines Zugriffs auf zentrale Verfahren ein enorm großer Personenkreis betroffen ist (mehrere Millionen Datensätze) und die erforderlichen Zugriffe bei alternierenden Telearbeitsplätzen durch eine entsprechende Arbeitsaufteilung grundsätzlich auch von der Dienststelle aus erledigt werden können, bestehen gegen die Einrichtung von Telearbeitsplätzen mit Zugriff auf landes- bzw. bundesweite Informationssysteme erhebliche datenschutzrechtliche Bedenken. Der LfD hat sich gegenüber anfragenden Stellen aus dem Bereich der Kommunen, der Oberfinanzdirektion und der Polizei in diesem Sinne geäußert.

Der LfD hält es für notwendig, dass die Institutionen, die eine Zertifizierung von öffentlichen Arbeitgebern zur Vereinbarkeit von Familie und Beruf anbieten, den datenschutzrechtlichen Belangen mehr Beachtung schenken würden.

6.3 Beschäftigtendatenschutz bei privaten Arbeitgebern

Der Schutz personenbezogener Daten in Arbeitsverhältnis ist aus verschiedenen Gründen ein besonderer Schwerpunkt in der Tätigkeit des LfD: Zum einen sind die betroffenen Arbeitnehmer in besonderer Weise darauf angewiesen, dass ihre personenbezogenen Daten im Beschäftigungsverhältnis sorgsam behandelt werden. Zum anderen belegt die Vielzahl von Eingaben gerade in diesem Bereich, dass sich viele Arbeitnehmer an ihrem Arbeitsplatz überwacht und kontrolliert fühlen und daher den LfD besonders häufig um Unterstützung bitten. Schließlich hat der Datenschutz durch die Neufassung des Bundesdatenschutzgesetzes zum 1. September 2009 mit dem neuen § 32 BDSG zur „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ eine erhebliche Stärkung erfahren. Anders als noch im Gesetzgebungsverfahren diskutiert, schützt § 32 Abs. 1 BDSG personenbezogene Daten im Beschäftigungsverhältnis nämlich nunmehr wesentlich intensiver als zuvor. Der Maßstab für den Umgang mit personenbezogenen Daten ist nun nicht mehr jener der Dienlichkeit, sondern der wesentlich schärfere der Erforderlichkeit: Nur für das Arbeitsverhältnis notwendige Datenverarbeitungen sind noch gestattet. Zudem ist der Anwendungsbereich des Bundesdatenschutzgesetzes in § 32 Abs. 2 auch auf nicht automatisierte Dateien erweitert worden, also auch auf die regelmäßig in Schriftform vorliegenden Personalakten. Damit erweitern sich auch die Kontroll- und Eingriffsmöglichkeiten des LfD erheblich.

Von den zahlreichen Problemfeldern im Bereich des Arbeitnehmerdatenschutzes können hier nur einige stellvertretend kurz beleuchtet werden:

6.3.1 Videoüberwachung von Mitarbeitern

Auch der LfD macht die Feststellung, dass aufgrund der mittlerweile relativ billigen Videotechnik viele Arbeitgeber auf die Idee kommen, ihre Arbeitnehmer am Arbeitsplatz bzw. während ihrer Tätigkeit mit oder ohne Aufzeichnung der Videobilder zu überwachen, beispielsweise in Bäckereien, Pflegeeinrichtungen, in der Systemgastronomie und in Einzelhandelsgeschäften. Immer häufiger werden Kameras zur gezielten Personalüberwachung eingesetzt, wobei auch Pausen oder Umkleidebereiche ins Visier kommen. Teilweise werden Minikameras in Rauchmeldern oder in der Deckenverkleidung von Geschäften installiert. Anders als bei der Überwachung eines unbestimmten Personenkreises in öffentlich zugänglichen Räumen sind die Arbeitnehmer im Betrieb dem Arbeitgeber persönlich bekannt; jede Verhaltensweise und Kommunikation unterliegt so der Kontrolle. Wer sich aber nicht sicher ist, zu welchem Zweck und wann er überwacht wird, wird versuchen, sich angepasst zu verhalten. Dieser Anpassungsdruck wird durch die wirtschaftliche Abhängigkeit der Beschäftigten vom Arbeitgeber verstärkt. Für die Beschäftigten gibt es oft keine Möglichkeit, sich der Erfassung durch Kameras zu entziehen.

Arbeitgeber führen in erster Linie den Schutz ihres Personals vor Übergriffen und den Diebstahlschutz als Gründe für diese Überwachungsmaßnahmen an. Der eigentliche Grund ist aber häufig die Leistungs- und Verhaltenskontrolle der Beschäftigten durch die Geschäftsführung. Dabei kontrolliert sie auch das Verhalten ihrer Angestellten gegenüber den Kunden, die korrekte Abrechung bei Bezahlvorgängen oder die Einhaltung von Pausenzeiten. Viele solcher Kameras werden zudem heimlich installiert. Eine heimliche Kamerainstallation ist jedoch ohne ein konkretes Verdachtsmoment stets rechtswidrig (vgl. § 32 Abs. 1 Satz 2 BDSG).

Darüber hinaus sind stets arbeitsrechtliche Vorgaben zu beachten. Insbesondere ist die Zulässigkeit der Überwachung am Arbeitsplatz mittels Videobeobachtung am Persönlichkeitsrecht der Beschäftigten zu messen. Bereits die Möglichkeit der jederzeitigen Überwachung erzeugt einen Überwachungsdruck, der mit dem Anspruch der Beschäftigten auf Wahrung ihrer Persönlichkeitsrechte nicht zu vereinbaren ist. Insoweit ist eine Videoüberwachung am Arbeitsplatz nur durch besondere Sicherheitsinteressen des Arbeitgebers ausnahmsweise gerechtfertigt.

Beschäftigte sollten vor Installation einer Videoüberwachungsanlage in jedem Falle schriftlich von ihrer Geschäftsführung informiert werden. Der Arbeitgeber sollte seine Angestellten über den Überwachungszweck, die Speicherdauer der Bilddaten und die Zugriffsmöglichkeiten auf die Daten in Kenntnis setzen. Dieser Zugriff und damit das Sichten und Auswerten des Bildmaterials darf nur bei begründetem Tatverdacht und nur im Zusammenwirken von Geschäftsführung und Betriebsrat erfolgen.

Folgende Grundsätze sind daher zu beachten:

- Das berechtigte Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl, Unterschlagung oder Verrat von Betriebsgeheimnissen, muss vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine vage Vermutung oder ein pauschaler Verdacht gegen die gesamte Belegschaft reicht hierfür nicht aus.
- Eine unter diesen Voraussetzungen statthafte Videoüberwachung ist grundsätzlich offen nach vorheriger Information der Belegschaft durchzuführen.
- Eine Überwachung durch verdeckte Kameras ist als letzte Möglichkeit nur ausnahmsweise zulässig, wenn dieses Mittel die einzige Möglichkeit darstellt, berechtigte schutzwürdige Interessen des Arbeitgebers zu wahren. Eine Totalüberwachung ist ebenso unzulässig wie die Aufzeichnung von Räumen, in denen Beschäftigte in ihrer körperlichen Intimsphäre betroffen wären (Tabubereiche Toilette, Dusche, Umkleidekabine).
- Die Videoüberwachung unterliegt der Mitbestimmung des Betriebsrates oder der Personalvertretung. Aber auch die Zustimmung des Betriebs- oder Personalrates kann eine unzulässige Videoüberwachung nicht rechtfertigen.
- Die durch eine datenschutzwidrige Überwachung gewonnenen Erkenntnisse unterliegen einem Verwertungsverbot und können im arbeitsgerichtlichen Verfahren regelmäßig nicht verwertet werden.

6.3.2 Einsatz von Ortungssystemen

Ein besonders gravierender Fall der Verletzung des informationellen Selbstbestimmungsrechts von Mitarbeitern hat den LfD im Jahre 2009 beschäftigt. Im Raum Trier ließ der Geschäftsführer eines mittelständischen Unternehmens ohne Kenntnis der betroffenen Mitarbeiter heimlich GPS-Ortungssysteme in die Betriebs-Kraftfahrzeuge einbauen, um sich jederzeit ein Bild über den Standort seiner Außendienstmitarbeiter machen zu können. Damit nicht genug, setzte der Geschäftsführer dieses Ortungssystem sogar an Wochenenden gegenüber solchen Mitarbeitern ein, denen Betriebsfahrzeuge auch zur privaten Nutzung überlassen worden waren.

Man mag in engen Grenzen ein berechtigtes Interesse des Arbeitgebers anerkennen, sich über den Standort seiner Kundendienstfahrzeuge einen Überblick zu verschaffen. Durch das eingesetzte Verfahren könnte – so die Geschäftsführung – während der Geschäftszeiten stets der Standort der Fahrzeuge auf einem Monitor in den Betriebsräumen der Firma angezeigt, die zurückgelegten Fahrstrecken und die Fahrtunterbrechungen nach Ort und Zeit festgehalten und diese Daten gespeichert werden. Das Informationssystem sei installiert worden, um Fahrzeuge und Mitarbeiter optimal einsetzen zu können. So ließen sich, während das Fahrzeug unterwegs ist, leichter Aufträge erteilen und ändern. Auch könne man die elektronischen Aufzeichnungen für die Abrechnung der Anfahrts- und Arbeitszeiten mit den Kunden nutzen. Eine Überwachung der Mitarbeiter sei zwar möglich, aber keineswegs beabsichtigt gewesen.

Datenschutzrechtlich ist demgegenüber festzuhalten, dass ein solcher Überblick regelmäßig auch dadurch erzielt werden kann, dass die Mitarbeiter bei bestehendem Anlass auf dem dienstlichen Mobiltelefon angerufen und nach ihrem Standort befragt werden. Werden solche Überwachungsmaßnahmen zudem noch heimlich und auch außerhalb der Arbeitszeiten der Mitarbeiter durchgeführt, so handelt es sich um einen äußerst gravierenden Verstoß gegen datenschutzrechtliche Bestimmungen, welcher mit einem spürbaren Bußgeld sanktioniert werden muss.

Da mit einer derartigen Nutzung eines GPS das Risiko eines nicht unerheblichen Eingriffs in das Persönlichkeitsrecht der Mitarbeiter verbunden ist, muss die Firma zudem eine so genannte Vorabkontrolle nach § 4d Abs. 5 BDSG durchführen. Ferner muss sie schriftlich festlegen, welche mit Hilfe des GPS erlangten Informationen für welche Zwecke und wie lange gespeichert und genutzt werden dürfen. Dabei müssen die Grundsätze der Erforderlichkeit und der Angemessenheit beachtet werden. Ferner muss es eine Datenlöschkonzeption geben. Diese muss unter anderem vorsehen, dass die Angaben über den Standort der Kundendienstfahrzeuge alsbald nach Beendigung der Betriebsfahrten gelöscht werden.

6.3.3 Internet- und E-Mail-Nutzung am Arbeitsplatz

Auch die Nutzung moderner Kommunikationstechnologien am Arbeitsplatz ist ein sehr häufiger Eingabegegenstand beim LfD. Bei unsachgemäßer Einrichtung der Kommunikationssysteme und bei unberechtigten Kontrollmaßnahmen des Arbeitgebers macht dieser sich im Einzelfall sogar strafbar.

Umgekehrt stellt der LfD bei der Bearbeitung von Eingaben immer wieder fest, dass eine große Anzahl von

Arbeitnehmern sich auch bei der erlaubten Nutzung von Internet oder E-Mail am Arbeitsplatz beobachtet und kontrolliert fühlen und sich – ebenso wie die Arbeitgeberseite – häufig über die Zulässigkeit ihres Verhaltens im Unklaren sind.

Eine Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder steht zum Abruf bereit:

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

6.3.4 Betriebliches Eingliederungsmanagement

Durch die Eingabe eines Bürgers wurde der LfD darauf aufmerksam gemacht, dass in einem bundesweit tätigen Unternehmen mit Zweigniederlassung in Rheinland-Pfalz so genannte Krankenrückkehrgespräche durchgeführt werden. Dies wurde zum Anlass genommen, ein persönliches Gespräch mit Vertretern des Betriebsrates durchzuführen.

Dabei stellte sich heraus, dass dieses Gesundheits- und Fehlzeitenmanagement bereits seit einigen Jahren praktiziert wird. Hauptsächliches Ziel ist Fehlzeitenreduktion, da der Krankenstand in den 1990er Jahren in einem für das Unternehmen grenzwertigen Bereich stand. Von Unternehmensseite her suchte man einen Weg, die Arbeitsbedingungen in dieser Hinsicht zu verbessern bzw. die Mitarbeiter gemäß ihren Einschränkungen, ggf. auch an einer anderen Stelle als bisher, einzusetzen.

Im Einzelnen ist folgende Praxis vorgesehen: Nach jeder krankheitsbedingten Abwesenheit eines Mitarbeiters, unabhängig davon, wie lange diese andauerte, wird mit dem Vorgesetzten ein Gespräch geführt, in welchem ergründet werden soll, ob die Krankheit betriebsbedingte Ursachen hatte und falls ja, welche. Insofern erfolgt eine Protokollierung des Besprochenen, welche jedoch beim Vorgesetzten verbleibt. Tritt innerhalb eines bestimmten Zeitraums erneut eine Fehlzeit auf, findet ein Gespräch, nunmehr der Stufe zwei, statt. Möglich sind Gespräche bis zur Stufe fünf, wobei ab Stufe drei Betriebsrat und werksärztlicher Dienst hinzugezogen werden können. Tritt hingegen innerhalb dieses Zeitraums keine erneute Krankheit auf, fällt der betreffende Mitarbeiter wieder in Stufe eins zurück.

Gegen diese Praxis bestehen nach Auffassung des LfD dann keine datenschutzrechtlichen Bedenken, wenn die gesetzlichen Vorgaben zum sog. Betrieblichen Eingliederungsmanagement (vgl. § 84 Abs. 2 SGB IX) beachtet werden. Dem Arbeitgeber/Dienstherrn sind bei der Erhebung von Krankheitsdaten im Zusammenhang mit der Arbeitsunfähigkeit nämlich enge Grenzen gesetzt. Zwar ist es ihm im Rahmen seiner Fürsorgepflicht unbenommen, einzelne Mitarbeiter auf ihre Fehlzeiten und die damit einhergehende Mehrbelastung der Kolleginnen und Kollegen hinzuweisen. Datenschutzrechtlich unzulässig ist es jedoch, wenn die Mitarbeiter bei sog. Rückkehrgesprächen aufgefordert werden, dem Arbeitgeber Auskunft über ihre Erkrankung zu geben. Bei Arbeitsunfähigkeit ist ein Bediensteter – abgesehen bei Gesundheitsgefahren für Kollegen, etwa durch eine ansteckende Krankheit – nicht verpflichtet, dem Arbeitgeber Näheres über seine Erkrankung (z. B. Diagnose, Symptome, Ursachen) mitzuteilen. Dies ergibt sich aus den arbeits- und sozialrechtlichen Vorschriften zur Arbeitsunfähigkeitsbescheinigung, die die Weitergabe von Informationen über die Art der Erkrankung des Arbeitnehmers an den Arbeitgeber gerade nicht vorsehen.

Das betriebliche Eingliederungsmanagement, welches bei jedem Beschäftigten mit wiederholten oder ununterbrochenen Fehlzeiten von mehr als sechs Wochen im Jahr durchzuführen ist, steht und fällt folgerichtig mit der informierten Einwilligung des Betroffenen. Er ist über die Ziele des betrieblichen Eingliederungsmanagements sowie darauf hinzuweisen, dass er zur Offenbarung über Art, Ausmaß und Hintergründe seiner Erkrankung weder verpflichtet ist noch seine Weigerung, Gesundheitsdaten zu offenbaren, zu beruflichen Nachteilen führt. Die Dokumentation von Gesprächen im Zusammenhang mit dem betrieblichen Eingliederungsmanagement ist ebenso wie sonstige Aufzeichnungen über sog. Mitarbeiter- oder Personalführungsgespräche, deren Ergebnisse in einer Zielvereinbarung festgehalten werden, aufgrund ihrer Zielsetzung (Verbesserung der Führungs- und Kooperationsbeziehungen zwischen Vorgesetztem und Mitarbeiter) kein zulässiger Gegenstand der Personalakte. Es empfiehlt sich, Fragen des Datenschutzes (Aufbewahrungsdauer, Zweckbindung, Zugriffsbefugnisse) in der Integrationsvereinbarung nach § 83 SGB IX zu regeln.

7. Polizei

7.1 Vorbemerkung

Der LfD hat sich besonders intensiv um den Datenschutz im Bereich der inneren Sicherheit gekümmert. Gerade hier wird der Datenschutz oft als nachrangig angesehen und allgemeinen Sicherheitsinteressen „geopfert“. Diesen Eindruck kann man gewinnen, wenn man sich die vielen Sicherheitsgesetze vergegenwärtigt, die der Bund und die Länder seit dem September 2001 erlassen haben und wenn man zugleich die einschlägigen Entscheidungen des Bundesverfassungsgerichts mit berücksichtigt, mit denen immer wieder einschlägige Gesetze zumindest teilweise als verfassungswidrig verworfen wurden.

Der LfD verkennt allerdings nicht, dass es vor dem Hintergrund vor allem terroristischer Bedrohungen schwierig ist, den notwendigen Ausgleich zwischen Sicherheit und Datenschutz zu finden. Dies ist letztendlich überhaupt nur möglich, wenn man die Interessen und Anliegen der jeweils anderen Seite versteht. Der LfD hat deshalb in vielen Gesprächen den Kontakt mit dem zuständigen Ministerium und den jeweiligen Sicherheitsorganen gesucht und für eine hinreichende Berücksichtigung des Datenschutzes geworben.

Aus diesen Gesprächen und den vielen örtlichen Feststellungen und Prüfungen in den Polizeidienststellen des Landes hat der Lfd die Überzeugung gewonnen, dass Polizei und Verfassungsschutz durchaus sensibel auf datenschutzrechtliche Anforderungen reagieren. Die Bereitschaft, dem Datenschutz in der täglichen Arbeit Rechnung zu tragen, ist groß.

Grundlage dafür ist ein beachtliches Vertrauensverhältnis zwischen den beiden Seiten, das bereits seit vielen Jahren besteht und von allen Beteiligten gefördert und ausgebaut wird. Dazu zählt auch, dass der LfD künftig regelmäßig mit den Datenschutzbeauftragten im Polizeibereich zusammenkommen wird. Angestrebt ist ein ähnlich intensiver Kontakt wie zu den behördlichen Datenschutzbeauftragten in anderen Bereichen (vgl. Tz. 3.4 und Tz. 5.1).

7.2 Vorratsdatenspeicherung – ein prinzipielles Problem

7.2.1 Ausgangslage

Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren bestehen. Kommunikationsinhalte sind von dieser Pflicht nicht betroffen, es müssen ausschließlich sog. „Verbindungsdaten“ erfasst und gespeichert werden. Mit Hilfe der auf Vorrat zu speichernden Daten lässt sich – ohne dass auf Kommunikationsinhalte zugegriffen wird – das Kommunikationsverhalten jedes Teilnehmers analysieren. Diese Pflicht wurde auf europäischer Ebene begründet (Richtlinie 2006/24/EG), um den Strafverfolgungsbehörden zu ermöglichen, im konkreten Verdachtsfall Kommunikationsstrukturen der Verdächtigen aufzuklären. Diese Möglichkeit soll einheitlich allen Strafverfolgern in der EU zur Verfügung stehen. Organisierte Kriminalität und Terrorismus sind die Bedrohungslagen, denen in erster Linie damit begegnet werden soll.

Die Vorratsdatenspeicherung ist in Deutschland durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ eingeführt worden, das mit dem 1. Januar 2008 in Kraft trat.

7.2.2 Konkrete Reichweite der Maßnahme

Verpflichtet werden die Anbieter von Telefondiensten einschließlich Mobilfunk- und Internet-Telefondiensten, folgende Daten zu speichern:

- die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses;
- Beginn und Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone;
- in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst;
- im Fall mobiler Telefondienste ferner: die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss; die internationale Kennung des anrufenden und des angerufenen Endgerätes; die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen;
- im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle;
- im Fall von Internet-Telefondiensten auch die IP-Adresse des anrufenden und des angerufenen Anschlusses. Das gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

Die E-Mail-Diensteanbieter müssen Folgendes speichern:

- bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die IP-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,
- bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die IP-Adresse der absendenden Telekommunikationsanlage,
- bei Zugriff auf das elektronische Postfach dessen Kennung und die IP-Adresse des Abrufenden, die Zeitpunkte der Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

Anbieter von Internetzugangsdiensten haben zu speichern:

- die dem Teilnehmer für eine Internetnutzung zugewiesene IP-Adresse,
- eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,
- den Beginn und das Ende der Internetnutzung unter der zugewiesenen IP-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

7.2.3 Anonymisierungsdienste als Ausweg?

Die Vorratsdatenspeicherung könnte die Entwicklung und Verbreitung technischer Mittel zur Verschleierung elektronischer Spuren begünstigen. Dies könnte eine Überwachung selbst in konkreten Verdachtsfällen vereiteln. Ein Beispiel ist das Onion-Routing-Verfahren, das von Anonymisierungsdiensten wie „Tor“ oder „JAP“ genutzt wird: Damit wird nicht nur der Traffic verschlüsselt, sondern es werden sogar Traffic-Analysen verhindert.

7.2.4 Verfassungsrechtliche Problematik

Die Vorratsdatenspeicherung ist verfassungsrechtlich umstritten, da sie anlasslos in die Grundrechtspositionen sämtlicher Nutzer elektronischer Dienste eingreift. In dem Maße, in dem die Kommunikation über elektronische Medien zunimmt, wird die Bedeutung solcher Analysen für die Erstellung von Persönlichkeitsprofilen wachsen. Bei Auswertung der Informationsquellen und Kommunikationspartner kann auf das Verhalten und die Interessengebiete bestimmter Personen geschlossen werden, wodurch Informationen über die politische, religiöse oder weltanschauliche Ausrichtung von Bürgern entstehen können und Einblicke in das Privatleben ermöglicht werden.

Unter diesen Aspekten hat der LfD stets – in Kontinuität mit seinem Vorgänger – die Auffassung vertreten, dass eine solche gesetzliche Regelung unverhältnismäßig und damit verfassungswidrig ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ebenfalls wiederholt betont, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz hat die Bundesregierung aufgefordert, die Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung zu unterlassen.

Inwieweit dieses Gesetz mit dem Grundgesetz vereinbar ist, wird derzeit aufgrund einer Vielzahl von Verfassungsbeschwerden verbindlich durch das Bundesverfassungsgericht geklärt. Allerdings hat das Bundesverfassungsgericht eine einstweilige Anordnung erlassen, die zwischenzeitlich wiederholt verlängert worden ist, die aus der Sicht des LfD einen deutlichen Hinweis darauf darstellt, dass dieses Gericht die Pflicht zur Vorratsdatenspeicherung in der gegenwärtig vorgesehenen Form nicht billigen wird (Beschlüsse vom 11. März und 1. September 2008 sowie vom 22. April 2009, Az. 1 BvR 256/08). In diesen Anordnungen wird bis zur Entscheidung in der Hauptsache die Nutzung der allein aufgrund dieser neuen gesetzlichen Pflicht gespeicherten Daten untersagt. Die Pflicht der Diensteanbieter zur Speicherung dieser Daten bleibt jedoch zunächst bestehen.

7.3 Online-Durchsuchung

Im letzten Tätigkeitsbericht (21. TB, Tz. 7.2.3) hatte der LfD über die offenen Fragen und seine Klärungsbemühungen im Zusammenhang mit den heimlichen Online-Durchsuchungen durch Strafverfolgungsbehörden und Verfassungsschutz berichtet.

Das Urteil des Bundesverfassungsgerichts über die Verfassungswidrigkeit entsprechender Regelungen im nordrhein-westfälischen Verfassungsschutzgesetz hat insoweit ein erhebliches Stück an Klärung gebracht (vom 27. Februar 2008, Az. 1 BvR 370/07; 1 BvR 595/07 – s.a. Tz. 2.2.1, Tz. 2.2.5, Tz. 6.2.2, Tz. 13.3).

Der LfD hat selbst im Land eine Arbeitsgruppe mit Vertretern des Justiz- und des Innenministeriums ins Leben gerufen, in der es gelungen ist, die rechtlichen und technischen Probleme klarer zu formulieren. Insbesondere auch die Notwendigkeiten der sog. „Quellen-TKÜ“, also der Möglichkeit, Internet-Telefonate vor bzw. nach der Verschlüsselung in den EDV-Geräten der Beteiligten

abhören zu können, wurde erörtert; entsprechende Techniken wurden aufgezeigt.

Aus der Sicht des LfD ist besonders ein Aspekt wesentlich: Ein heimliches Betreten von Wohnungen zum Zweck der Installation von Abhörtechniken ist aus seiner Sicht keinesfalls zu gestatten.

7.4 Überwachung der Telekommunikation

Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) greifen tief in das Datenschutzgrundrecht der Betroffenen ein. Sie bedürfen deshalb der besonderen Aufmerksamkeit der Datenschützer. Der LfD richtete im Berichtszeitraum sein Augenmerk besonders auf die über das Internet abgewickelte Telekommunikation. Von Interesse war, in welchem Umfang Informationen aus solchen Kommunikationsvorgängen im Rahmen von TKÜ-Maßnahmen auf der Grundlage des § 100a StPO aufgezeichnet und ausgewertet werden können und in der Praxis ausgewertet werden. Vor diesem Hintergrund hat der LfD bei Polizeidienststellen, die Überwachungen insbesondere von DSL-Anschlüssen durchgeführt haben, örtliche Feststellungen getroffen. Er hat außerdem die zugehörigen staatsanwaltschaftlichen Ermittlungsakten beigezogen, um die Ergebnisse solcher Maßnahmen erkennen und beurteilen zu können. Es hat sich gezeigt, dass die durchgeführten Maßnahmen datenschutzrechtlich nicht zu beanstanden waren. Überwachungsmaßnahmen, die sich auf verschlüsselte IP-Telefonie bezogen hätten, konnten nicht festgestellt werden.

Unabhängig von der überwachten Telekommunikationstechnik fiel auf, dass sich bei Ermittlungsverfahren wegen Verstößen gegen das Betäubungsmittelgesetz aus dem Ursprungsverfahren zahlreiche Folgeverfahren ergaben, für deren Abwicklung die TKÜ-Daten des Ursprungsverfahrens erforderlich erschienen. Dieser Aspekt führt in datenschutzrechtlicher Hinsicht dazu, dass auch die in Folgeverfahren zuständigen Staatsanwaltschaften im Zeitpunkt des Verfahrensabschlusses eine Anordnung über die Vernichtung der nicht mehr erforderlichen Telekommunikationsdaten erlassen. Ähnlich stellt sich die Situation bei der Polizei dar. Die Prüfung, ob ältere, für Folgeverfahren „umgewidmete“ Telekommunikationsdatenbestände noch benötigt werden, bleibt der Eigeninitiative der Sachbearbeiter der Polizeipräsidien überlassen. Deshalb hat der LfD empfohlen, automatisierte Überwachungsverfahren einzuführen, die ein „Vergessen“ solcher Prüfungen verhindern und die Löschung nicht mehr erforderlicher TKÜ-Daten sicherstellen. Im Nachgang legte die Polizei eine für alle Polizeidienststellen verbindliche Verfahrensregelung zur TKÜ vor, die neben einer automatisierten Prüffristenüberwachung auch eine aktive Nachfragepflicht bei der Staatsanwaltschaft vorsieht und zum 1. Juli 2009 in Kraft gesetzt wurde. Diese Verfahrensweise begrüßt der LfD.

Die Landesregierung hat gemäß ihrer gesetzlichen Pflicht (§ 31 Abs. 7 i.V.m. § 29 Abs. 12 POG) über im Jahre 2007 durchgeführte auf dem Polizeigesetz beruhende TKÜ-Maßnahmen berichtet (LT-Drs. 15/2236 vom 19. Mai 2008). Der LfD hat sich aus diesem Anlass darüber informiert, ob die entsprechenden Lösch- und Benachrichtigungspflichten hinsichtlich der Betroffenen und „Dritter“ beachtet worden sind.

Die in Rede stehenden beiden Verfahren betrafen die inhaltliche Überwachung von insgesamt sieben privaten Mobiltelefonanschlüssen eines Störers sowie eines Nichtstörers. In einer dreißig Tage währenden richterlich angeordneten Maßnahme wurden 560 Einzelgespräche und in der zweiten im Rahmen eines Strafverfahrens weitergeführten Maßnahme in einem Zeitraum von vier Tagen sechs Einzelgespräche überwacht. Im ersten Verfahren schloss sich an die präventive Maßnahme kein Strafverfahren an. In beiden Verfahren wurde nach Beendigung der Kommunikationsüberwachungsmaßnahmen zunächst von einer Benachrichtigung abgesehen, da die Gefahr bestand, den fortbestehenden Zweck der Maßnahme zu gefährden bzw. weil sich ein strafrechtliches Ermittlungsverfahren anschloss.

Die von den TKÜ-Maßnahmen Betroffenen wurden nach Abschluss der Maßnahmen unverzüglich schriftlich unterrichtet und sämtliche gespeicherten Telekommunikationsdaten gelöscht. Ein Anlass für weitergehende datenschutzrechtliche Forderungen ergab sich nicht.

7.5 Videoüberwachung durch die Polizei

Im Berichtszeitraum wurde die Zahl der durch die Polizei betriebenen Videoaufzeichnungsanlagen ermittelt. Es handelt sich um 1.141 Kameras und 611 Funkstreifenwagen mit digitaler Videoüberwachung.

Die Videoüberwachungsmaßnahmen unterstützen die polizeiliche Aufgabenwahrnehmung hinsichtlich der stationären und mobilen Verkehrsüberwachung, des Schutzes von Veranstaltungen und Versammlungen sowie der Sicherung eigener Liegenschaften. Rechtsgrundlage für die Datenerhebung ist, sofern es sich um eine Datenerhebung im Einzelfall und um die Wahrnehmung spezifisch polizeilicher Aufgaben handelt, § 27 POG. Sonstige Datenverarbeitungen zu Polizeiverwaltungszwecken sowie bei der stationären und unbefristeten Videoüberwachung

polizeieigener Liegenschaften richten sich nach § 34 LDSG.

Es hat sich gezeigt, dass gegen den konkreten Einsatz der Videobeobachtungs- bzw. -aufzeichungseinrichtungen aus datenschutzrechtlicher Sicht keine Bedenken bestehen. Die detaillierten Regelungen zum Einsatz der Videoüberwachung in einer Dienstanweisung sind als datenschutzfreundlich einzustufen.

7.6 Rückfallgefährdete Straftäter

Im Dezember 2007 stellte das Ministerium des Innern und für Sport dem LfD den Entwurf einer rheinland-pfälzischen Konzeption eines Datenverarbeitungsverfahrens zum Umgang mit rückfallgefährdeten Straftätern vor. Ziel dieses Verfahrens ist ein verbesserter Informationsaustausch zwischen Polizei und Justiz, um notwendige Maßnahmen nicht zu versäumen.

Als Grundlage für die in Rheinland-Pfalz favorisierte Konzeption diente das von der Polizei Bayern genutzte Verfahren „Heads“. Jedoch sollte die Zielgruppe erweitert werden, insbesondere um Personen, die gemeingefährliche Verbrechen (mit Gewaltkomponente und Rückfallgefährdung) begangen haben oder bei denen der Verdacht besteht, dass sie solche Taten begehen werden. Der LfD empfahl, konkrete Deliktsarten zu beschreiben und zunächst die Zielgruppe auf den Kernbereich (Sexualstraftäter) zu beschränken und erst bei Notwendigkeit in einem zweiten Schritt eine Erweiterung vorzunehmen. Vom LfD wurde zunächst auch die Speicherung personenbezogener Daten im Freitextfeld „Bemerkungen zur Person“ kritisch bewertet.

Im Januar 2009 konnte der Abstimmungsprozess mit der justiziellen und polizeilichen Praxis abgeschlossen werden. Das Anliegen des LfD bezüglich des Freitextfeldes wurde durch eine Begrenzung des zulässigen Inhalts dieses Textfelds auf das unbedingt notwendige Mindestmaß ausgeräumt. Da die Anregungen des LfD bei der abschließenden Fassung des von der ressortübergreifenden Arbeitsgruppe „Gefährliche Entlassene“ erarbeiteten Fachkonzepts „Visier.rlp“ auch im Übrigen Berücksichtigung fanden, konnten die datenschutzrechtlichen Bedenken sowohl gegen das Fachkonzept als auch gegen die im Oktober 2008 vorgelegte Generalerrichtungsanordnung für die Datei „Visier.rlp“ ausgeräumt werden. Begrüßt wird die ein Jahr nach Inkrafttreten vorgesehene Evaluierung.

7.7 Längerfristige Observationen

Im Rahmen örtlicher Feststellung prüfte der LfD bei einem Polizeipräsidium, ob und ggf. wie Einzelheiten der Vorbereitung, Durchführung und Nachbereitung von längerfristigen, planmäßig angelegten Observationseinsätzen in polizeilichen Einsatzprotokollen (Observationsprotokollen) dokumentiert werden und welchen Inhalt die auf der Grundlage dieser Protokolle gefertigten Observationsberichte haben.

Alle im Zusammenhang mit der Observation entstandenen Datenerhebungen, sowohl die elektronisch als auch in Papierform verarbeiteten Informationen, werden Bestandteil der Observationsakten. Nur verfahrensrelevante Informationen fließen in die staatsanwaltschaftliche Akte (Observationsakte bzw. Zweitakte der Polizei) ein. Sofern die Daten für künftige Verfahren nicht (mehr) erforderlich sind, erfolgt die Löschung der Daten in der EDV und die Vernichtung der Akten in Papierform.

Problematisiert wurde jedoch der die Observationsvorgänge begleitende E-Mail-Verkehr, weil diese Informationen bei dem in Rede stehenden Polizeipräsidium auf einem gesonderten Laufwerk vorgehalten werden. Da aus datenschutzrechtlicher Sicht eine Dezentralisierung von Daten auf unterschiedlichen Speicherplätzen nicht ohne Bedenken ist, wurden die Polizeidienststellen durch das Ministerium des Innern und für Sport angewiesen, die vom LfD empfohlene Poladis-annex-Lösung anzuwenden.

Darüber hinaus wurde der Anspruch auf Benachrichtigung Drittbetroffener erörtert. Da diesbezügliche eine obergerichtliche Entscheidung zu erwarten ist, wurde von einer abschließenden Beurteilung zunächst abgesehen.

7.8 Gesichtserkennung

Bei der biometrischen Gesichtserkennung wird das Gesicht einer Person von einer Kamera aufgenommen und mit einem oder mehreren zuvor gespeicherten Gesichtsbildern verglichen. Dabei wird zunächst das Bild digitalisiert. Die Erkennungssoftware lokalisiert sodann das Gesicht und berechnet seine charakteristischen Eigenschaften. Das Ergebnis dieser Berechnung, das sog. Template, wird mit den Templates der gespeicherten Gesichtsbilder verglichen.

Bisher konnten automatisierte Absuchverfahren innerhalb größerer Datenbestände nicht genutzt werden, um in polizeilichen Ermittlungsverfahren vorliegende Lichtbilder unbekannter Personen zu identifizieren. Dies wurde erstmals durch das seit Mai 2008 vom Bundeskriminalamt

genutzte Gesichtserkennungssystem (GES) möglich. Es erlaubt die automatisierte Suche im großen digitalen Datenbestand (derzeit ca. 2,5 Millionen Lichtbilder) von INPOL-Z. Dieses System ist vergleichbar mit der AFIS-Recherche im Bereich der Daktyloskopie.

Weil diese neue Möglichkeit der Personenidentifizierung einen deutlichen Zuwachs an Lichtbildvergleichen erwarten ließ, wurde den Polizeien der Länder die Einrichtung eines eigenen Zugriffs über eine INPOL-GES-Schnittstelle angeboten.

Das datenschutzrechtliche Interesse des LfD richtete sich vor allem auf das zu erwartende zusätzliche Potential, das sich dem Landeskriminalamt Rheinland-Pfalz durch diese Schnittstelle eröffnete. Die Recherche ergab, dass das Landeskriminalamt nunmehr in der Lage ist, Lichtbilder in GES einzulesen, Recherchen im Lichtbildbestand des INPOL-Z selbständig durchzuführen und bisherige Identifizierungsmöglichkeiten zu optimieren. Eine Überprüfung hinsichtlich ausreichender datenschutzrechtlicher bzw. technisch organisatorischer Anforderungen an die neue Option ist für Anfang 2010 geplant.

7.9 Umgang mit demenzkranken Menschen

Bei der Kampagne mit dem Schwerpunktthema „Demenz“, einer Kooperation zwischen der Landeszentrale für Gesundheitsförderung in Rheinland-Pfalz e. V. und der Polizei, war der LfD beratend in die Vorbereitung einer Broschüre, die über den polizeilichen Umgang mit an Demenz leidenden Personen informieren soll, eingebunden. Die abgestimmte Publikation wurde bei der Auftaktveranstaltung am 5. November 2008 im Polizeipräsidium Trier, zu dessen Zuständigkeitsbereich 102 Altenheime und ca. 8.000 Demenzkranke zählen, durch die Landesregierung der Öffentlichkeit vorgestellt.

Ziel der polizeilichen Aktivitäten ist es, vorbereitende Maßnahmen zu treffen, um die Suche nach vermissten Demenzkranken zu erleichtern. So ist beabsichtigt, eine „Vermisstenakte“, die ein Datenblatt für den Eintritt des Vermisstenfalls enthält, zu erstellen. Aufbewahrt werden soll die Akte entweder im Pflegeheim oder im privaten Haushalt und im Vermisstenfall der Polizei bei Anzeigenerstattung zur Verfügung gestellt werden.

Bei der Gestaltung der Broschüren wurden die datenschutzrechtlichen Anregungen berücksichtigt. Sie bezogen sich vor allem darauf, den Umfang der zu erhebenden Daten eng am Verwendungszweck zu orientieren. Die Frage, ob der Betreuer für den Betroffenen über die Datenerhebung bzw. -übermittlung entscheiden darf, wurde einvernehmlich in dem Sinne entschieden, dass dies nur dann der Fall ist, wenn eine umfassende und uneingeschränkte Betreuungsvollmacht vorliegt.

7.10 POLIS-Abfragen

Ende November 2009 wurde bekannt, dass sich zwei Abgeordnete des Mainzer Landtags, die Mitglieder im Nürburgring-Untersuchungsausschuss waren, auf rechtswidrige Weise Daten aus dem polizeilichen Informationssystem POLIS verschafft hatten.

POLIS ist der Landesteil von INPOL, dem bundesländerübergreifenden Informationssystem der Polizei beim Bundeskriminalamt. INPOL ist als Verbunddatei aufgebaut. Das Verbundsystem besteht aus den Bereichen INPOL-zentral beim Bundeskriminalamt und den bei den jeweiligen Landespolizeien betriebenen Systemen INPOL-Land. In diesem komplexen Informationssystem befinden sich vor allem Angaben zu allen Personen, die als Tatverdächtige auffällig geworden sind. Es ist das tägliche Arbeitsmittel der Polizei, das zur Sachbearbeitung nahezu aller polizeilichen Vorgänge genutzt wird. Pro Monat erfolgen im Land von ca. 7.500 abfrageberechtigten Polizeibeamten ca. 220.000 Abrufe. Im Aktennachweis von INPOL sind bundesweit insgesamt etwa 4,3 Millionen Datensätze (Vorgänge) erfasst, wobei einer Person mehrere Vorgänge zugeordnet sein können (vgl. BT-Drs. 16/13563 vom 25. Juni 2009, Anlage 1). Seine Rechtsgrundlage findet dieses System in § 11 BKAG und in §§ 33, 34 und 36 POG Rheinland-Pfalz.

Die unzulässigen Datenabrufe waren jeweils durch Polizeibeamte erfolgt. Dies gab dem LfD Veranlassung, das Verfahren der POLIS-Abrufe daraufhin zu überprüfen, ob über die vorhandenen Vorkehrungen zur Verhinderung unzulässiger Datenabrufe hinaus weitere Maßnahmen zu diesem Zweck getroffen werden können. Außerdem begann er mit einer systematischen stichprobenweisen Überprüfung aller Abrufe eines Monats des Jahres 2009.

Diese Prüfungen sind derzeit noch nicht abgeschlossen.

8. Soziales und Gesundheit

8.1 Hartz IV

Mit Urteil vom 20. Dezember 2007 hat das Bundesverfassungsgericht die Konstruktion der Arbeitsgemeinschaften nach § 44b SGB II für verfassungswidrig erklärt. Die mit Einrichtung der Arbeitsgemeinschaften praktizierte gemeinsame Aufgabenwahrnehmung von Bund und Kommunen stellt hiernach eine vom Grundgesetz nicht zugelassene Form der Mischverwaltung dar. Ein maßgeblicher Grund hierfür war auch die nach der bestehenden Rechtslage unklare Zuordnung der datenschutzrechtlichen Aufsichtszuständigkeit über die Arbeitsgemeinschaften (vgl. 21. Tb., Tz. 11.1.1). Das Bundesverfassungsgericht hat allerdings im Interesse einer kontinuierlichen Gewährung der Grundsicherungsleistungen eine Übergangsfrist bis zum 31. Dezember 2010 eingeräumt. Spätestens dann hat der Gesetzgeber einen verfassungsgemäßen Zustand herbeizuführen.

Trotz des inzwischen deutlich näher gerückten Endes der Übergangsfrist ist bislang die Neuordnung der Grundsicherung für Arbeitsuchende nicht geglückt. Ein in der abgelaufenen Legislaturperiode des 16. Deutschen Bundestages erarbeiteter Referentenentwurf zur Regelung der gemeinsamen Aufgabenwahrnehmung in der Grundsicherung für Arbeitsuchende, der die Einrichtung sog. Zentren für Arbeit und Grundsicherung vorsah und im Ergebnis die gemeinsame Aufgabenwahrnehmung von Bund und Kommunen durch eine Grundgesetzänderung ermöglichen sollte, fand in der Regierungskoalition keine Mehrheit. Damit bleibt auch weiterhin unklar, wie die datenschutzrechtliche Aufsichtszuständigkeit in diesem Bereich künftig aussehen wird. Es bleibt insbesondere abzuwarten, ob die anstehende Neuregelung die im gescheiterten Gesetzentwurf vorgesehene datenschutzrechtliche Alleinzuständigkeit des Bundes aufgreifen wird.

Im Berichtszeitraum stellten die Anfragen und Eingaben im Zusammenhang mit der Gewährung von Leistungen nach dem SGB II allein quantitativ wieder einen Schwerpunkt der Tätigkeit des LfD dar. Hervorzuheben sind folgende Fragestellungen:

8.1.1 Feststellung der Erwerbsfähigkeit

Eine Voraussetzung für die Gewährung von Leistungen der Grundsicherung für Arbeitsuchende ist die Erwerbsfähigkeit der Hilfesuchenden. Insbesondere im Hinblick auf die Vermittlungsmöglichkeiten kommt es auf die körperliche Verfassung und Leistungsfähigkeit der Betroffenen an. Bei Unklarheiten haben die Leistungsträger grundsätzlich die Möglichkeit, die Erwerbsfähigkeit der Antragsteller durch die Gesundheitsämter oder den Ärztlichen Dienst der Bundesagentur für Arbeit begutachten zu lassen.

In mehreren Eingaben kam die Frage auf, ob und ggf. in welchem Umfang die begutachtenden ärztlichen Stellen die Leistungsträger über die medizinischen Inhalte der durchgeführten Untersuchungen unterrichten dürfen. So hatte in einem konkreten Fall das beauftragte Gesundheitsamt der zuständigen Arbeitsgemeinschaft nach der amtsärztlichen Untersuchung ein schriftliches Gutachten übersandt, das neben den Aussagen zum Leistungsbild des Betroffenen und entsprechender Einsatzbeschränkungen auch konkrete Befunde und Diagnosen enthielt.

Nach Auffassung des LfD ist eine regelmäßige Weitergabe von Diagnose- und Befundangaben an die leistungsgewährenden Stellen im Zusammenhang mit der ärztlichen Begutachtung der Erwerbsfähigkeit der Hilfesuchenden für deren Aufgabenerfüllung nicht erforderlich und damit unzulässig. Denn für die Festlegung der konkreten Vermittlungsmöglichkeiten der Antragsteller reicht grundsätzlich die Kenntnis aus, welche Arbeiten von diesen verrichtet werden können (sog. positives Leistungsbild) und welche Arbeiten oder Belastungen auszuschließen sind (sog. negatives Leistungsbild). Dagegen bedarf es im Regelfall keiner genauen Kenntnis der zugrunde liegenden Befunde oder Diagnosen, so dass eine routinemäßige Übermittlung dieser Informationen mit den datenschutzrechtlichen Vorgaben kollidiert. Lediglich in begründeten Einzelfällen oder bei bestimmten Einschränkungen, bei denen es auf die konkrete Kenntnis der Erkrankung ankommt, ist eine entsprechende Unterrichtung der leistungsgewährenden Stelle durch den Gutachter hinzunehmen.

8.1.2 Vorlage von Kontoauszügen und sonstigen Beweismitteln

Zu einer grundsätzlichen Klärung des schon seit Jahren umstrittenen Umfangs einer Vorlagepflicht von Kontoauszügen bei der Gewährung von Sozialleistungen hat das Urteil des Bundessozialgerichts vom 19. September 2008 (Az. B 14 AS 45/07 R) geführt. Hiernach besteht nach § 60 Abs. 1 Nr. 3 SGB I eine grundsätzliche Pflicht zur Vorlage von Kontoauszügen, einer Kontenübersicht und der Lohnsteuerkarte. Die Antragsteller sind nach der Entscheidung zur Vorlage der Unterlagen im Rahmen ihrer Mitwirkungspflicht sowohl bei der erstmaligen Leistungsbeantragung als auch bei allen weiteren Folgeanträgen verpflichtet, selbst wenn keine Anhaltspunkte für einen Leistungsmissbrauch vorliegen. Nach Auffassung des BSG ist zumindest die Anforderung der

Kontoauszüge der letzten drei Monate vor Antragstellung nicht unverhältnismäßig. Die Vorlagepflicht wird auch nicht durch die Vorgaben des Sozialdatenschutzes eingeschränkt, da eine Einsichtnahme in die Kontoauszüge regelmäßig zur Aufgabenerfüllung der Leistungsträger erforderlich ist. Eine Ausnahme erkennt das Bundessozialgericht lediglich dann an, wenn auf der Ausgabenseite der Kontoauszüge besonders schutzwürdige Einzelangaben wie z.B. Informationen über die ethnische Herkunft, das Sexualleben oder die politische Gesinnng ersichtlich sind. Diese dürfen nach Auffassung des Bundessozialgerichts von den Betroffenen geschwärzt werden, wobei die überwiesenen Beträge als solche erkennbar bleiben müssen. Der Leistungsträger ist grundsätzlich gehalten, in seinen Mitwirkungsaufforderungen auf ein solches Schwärzungsrecht hinzuweisen.

Mit der Entscheidung wird die im Kreise der Datenschutzbeauftragten des Bundes und der Länder vertretene Auffassung zur Vorlagepflicht von Kontoauszügen und sonstigen Beweisunterlagen bei Folgeanträgen korrigiert. Das Bundessozialgericht stellt klar, dass auch bei Fortzahlungsanträgen regelmäßig und nicht nur in konkreten Verdachtsfällen eine Vorlage von Kontoauszügen zumindest der der Antragstellung vorangegangenen drei Monate verlangt werden darf. Darüber hinaus bestätigt das Bundessozialgericht erstmals das von den Datenschutzbeauftragten schon seit langem für besonders schutzwürdige Einzelangaben geforderte Schwärzungsrecht, auch wenn die Folgen eines Verstoßes gegen die Hinweispflicht leider offen bleiben.

Auch wenn mit dem Urteil des Bundessozialgerichts vom 19. September 2008 eine wichtige datenschutzrechtliche Problematik bei der Gewährung von Leistungen nach dem SGB II und SGB XII geklärt werden konnte, schließen sich weitere Fragen an die Vorlagepflicht von Beweisunterlagen an. Diskutiert wird beispielsweise, ob das routinemäßige Kopieren und Ablegen der im Rahmen der Mitwirkungspflicht nach § 60 Abs. 1 Nr. 3 SGB I vorgelegter Dokumente wie z.B. Mietverträge oder Kontoauszüge datenschutzrechtlich zulässig ist. Der LfD vertritt dabei die Auffassung, dass eine Speicherung der von den Antragstellern vorgelegten Beweisunterlagen nach den Vorgaben des § 67c Abs. 1 SGB X nur dann erforderlich und damit datenschutzrechtlich unbedenklich ist, wenn sich daraus Abweichungen zu den bisherigen Antragsangaben ergeben oder zusätzliche leistungsrelevante Inhalte ersichtlich sind. Nur in diesen Fällen bedarf es einer Speicherung der vorgelegten Dokumente insbesondere unter dem Aspekt der Nachvollziehbarkeit der Behördenentscheidung z.B. zu Prüfzwecken, da nur dann die Bescheidung des Antrags auf die erstmalig aus der Beweisurkunde ersichtlichen Angaben gestützt wird. In allen anderen Fällen dient die Vorlage der Unterlagen lediglich dem Beweis der Richtigkeit der bisherigen Angaben. Dieser kann durch Aufnahme eines entsprechenden Vermerks in die Verfahrensakte für Dritte nachvollziehbar aktenkundig gemacht werden.

8.2 Vollzug des Landeskinderschutzgesetzes

8.2.1 Einladungsverfahren

Nach dem Inkrafttreten des Landeskinderschutzgesetzes überprüfte der LfD in örtlichen Feststellungen bei einzelnen Gesundheits- und Jugendämtern den Gesetzesvollzug und insbesondere die Einhaltung der dargestellten datenschutzrechtlichen Vorgaben. Dabei wurde u.a. offenbar, dass die weit überwiegende Zahl der von der Zentralen Stelle an die Gesundheitsämter abgegebenen Fälle Sachverhalte betrafen, in denen die Früherkennungsuntersuchungen tatsächlich durchgeführt oder die betroffenen Kinder hierzu angemeldet waren. Trotzdem mussten diese sog. falsch positiven Fälle an die Gesundheitsämter abgegeben werden, da der Zentralen Stelle die erforderlichen Untersuchungsbestätigungen innerhalb der vorgesehenen Frist nicht vorlagen. Die unterbliebenen Unterrichtungen resultierten einerseits aus Meldeversäumnissen durch die Ärzte, andererseits aus fehlenden Meldebögen im Untersuchungstermin. Im Ergebnis entsprach die Weiterleitung der Fälle an die Gesundheitsämter zwar formell den gesetzlichen Anforderungen. Allerdings war die originäre Aufgabe der Gesundheitsverwaltung, bei den Betroffenen auf die Inanspruchnahme der Vorsorgeuntersuchungen hinzuwirken, längst erfüllt.

Nach Auffassung des LfD ist die Vermeidung falsch positiver Fälle datenschutzrechtlich geboten. Es ist dauerhaft nicht hinzunehmen, dass aufgrund administrativer und organisatorischer Versäumnisse mehrere Stellen Daten über Personen, die sich nach dem Verständnis des Gesetzes unauffällig verhalten, parallel speichern. Zugleich sind in diesen Fällen die gleichen Löschungsvorgaben heranzuziehen, die bei einer sachlich richtigen Weitergabe der Untersuchungsbestätigung an die Zentrale Stelle bereits zu beachten gewesen wären. Demzufolge forderte der LfD eine deutlich vor dem Ablauf der in § 10 Abs. 2 LKindSchuG enthaltenen Maximalspeicherfrist von drei Jahren liegende Löschung dieser Daten bei den Gesundheitsämtern.

8.2.2 Neugeborenenprojekt eines Landkreises

Im Zuge der Umsetzung der im Landeskinderschutzgesetz vorgesehenen Maßnahmen zur Schaffung frühzeitiger und niedrigschwelliger Nutzungsmöglichkeiten qualifizierter

Förder- und Hilfsangebote legte eine Kreisverwaltung ein sog. Neugeborenenprojekt auf. Dabei sollten im Kreisgebiet ansässige Eltern neugeborener Kinder vom Jugendamt direkt angeschrieben und über bestehende Beratungs- und Hilfsangebote aufgeklärt werden. Zugleich wurde ein bereits terminierter Hausbesuch von Mitarbeitern des Jugendamtes angekündigt, bei dem den Betroffenen neben einem Willkommenspaket für das Neugeborene auch ein neu entwickeltes Elternbegleitbuch mit zahlreichen Tipps und Ansprechpartnern überreicht werden sollte. Offen blieb, ob und wenn ja mit welchen Folgen sich die Betroffenen einem solchen Hausbesuch widersetzen konnten.

Die datenschutzrechtliche Brisanz der Angelegenheit lag vor allem in der von der Kreisverwaltung gegenüber den Meldebehörden erbetenen regelmäßigen Übermittlung von Meldedaten der Neugeborenen. Nach der für die Weitergabe der Meldedaten heranzuziehenden Regelung des § 31 MG ist die Datenübermittlung an andere öffentliche Stellen nur zulässig, wenn die Kenntnis der Meldedaten für die Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgaben erforderlich ist. Dies war aber hier nicht der Fall. Insbesondere ist eine Aufklärung der Eltern von Neugeborenen über bestehende Hilfsangebote der Jugendhilfe auch auf anderen Wegen und ohne Vornahme eines Hausbesuchs zu erreichen, zumal deren Inanspruchnahme immer freiwillig ist. Zudem begründet allein die Tatsache einer Geburt noch keine Befugnis der Jugendhilfe, auch ohne Einverständnis der Betroffenen tätig zu werden. Selbst wenn jedoch die direkte Ansprache der jungen Eltern als sachlich notwendig erachtet wird, bedarf es hierzu nicht einer Übermittlung von Meldedaten. In Betracht kommt vielmehr das Instrument der Datenmittlung. Hiernach stellt das Jugendamt den Meldebehörden eigene vorbereitete Schreiben an die Betroffenen zur Verfügung, die dann von den Meldebehörden unter Nutzung der bei ihnen vorhandenen Daten an die konkrete Zielgruppe versandt werden. Datenschutzrechtlich hat dies den Vorteil, dass an das Jugendamt keine Meldedaten übermittelt werden müssen und insoweit dort auch keine Datei der Eltern neugeborener Kinder aufgebaut werden kann.

Nach einer entsprechenden Bewertung durch den LfD sah die betroffene Kreisverwaltung von ihren ursprünglichen Plänen ab und wird sich nun in Form der Datenmittlung an die jeweiligen Eltern wenden. In diesem Zusammenhang war noch zu klären, ob das von der Jugendhilfe neu entwickelte Elternbegleitbuch ausschließlich im Rahmen eines Hausbesuchs zur Verfügung gestellt werden kann oder die Betroffenen auch auf anderen Wegen wie z. B. einem Besuch in der Kreisverwaltung Zugang zu diesem Ratgeber erhalten können. Auf Anregung des LfD wird die Kreisverwaltung beide Alternativen anbieten.

8.3 Elektronische Gesundheitskarte

Nur wenige Projekte haben die Datenschutzbeauftragten des Bundes und der Länder in der Vergangenheit ähnlich anhaltend beschäftigt wie die Entwicklung der Elektronischen Gesundheitskarte (vgl. u.a. 21. Tb., Tz. 10.1). Auch fast vier Jahre nach dem ursprünglich vorgesehenen Einführungstermin ist es immer noch nicht zu einem flächendeckenden Einsatz der Chipkarte gekommen. Im Gegenteil: in der öffentlichen Diskussion hat der Widerstand gegen das ambitionierte Telematikvorhaben insbesondere aus Kreisen der Ärztevertreter deutlich zugenommen. Als ein Hauptargument wird der mangelnde Datenschutz und die Gefahr des gläsernen Patienten genannt. Doch diese Befürchtungen finden angesichts der eindeutig datenschutzfreundlichen rechtlichen Vorgaben des § 291a SGB V wohl keine Bestätigung. Die darin enthaltenen Anforderungen an die der Elektronischen Gesundheitskarte zugrunde liegende Telematikinfrastruktur sind beispielhaft und betonen deutlich die Prinzipien der Patientensouveränität und Datensicherheit.

Gleichwohl bleiben im Zusammenhang mit der Einführung der Elektronischen Gesundheitskarte aus der Sicht des Datenschutzes zentrale Fragen weiterhin offen. Daran hat auch der mittlerweile von der Gesellschaft für Telematik (gematik) vorgelegte Entwurf eines übergreifenden Datenschutzkonzepts nichts geändert:

- Die Zuordnung der datenschutzrechtlichen Verantwortlichkeit der am System der Elektronischen Gesundheitskarte beteiligten Stellen ist immer noch nicht abschließend geklärt, obwohl dies sowohl im Hinblick auf die Gewährung der den Versicherten zustehenden Rechte als auch hinsichtlich der von den datenverarbeitenden Stellen zu erfüllenden Pflichten von großer Bedeutung ist. Auf Initiative des LfD wurde die Fragestellung im Kreise der Datenschutzbeauftragten des Bundes und der Länder erörtert. Dabei herrschte Einvernehmen, dass die Krankenkassen hinsichtlich der Organisation, Verwaltung und Ausgabe der Elektronischen Gesundheitskarte sowie der Verarbeitung der Versichertenstammdaten die datenschutzrechtlich verantwortlichen Stellen sind. Gleiches gilt für die beteiligten Ärzte hinsichtlich der von ihnen bereit gestellten medizinischen Daten. Offen ist dagegen bislang, welche Verantwortlichkeit für die technische Funktionsfähigkeit der Elektronischen Gesundheitskarte der gematik als Betreiber der Telematikinfrastruktur sowie den weiteren Betreibern der einzelnen

Fachdienste zukommt. Der LfD tritt dafür ein, dass die Versicherten unabhängig von dem letztendlich Verantwortlichen zur praktikablen Wahrnehmung ihrer Rechte sich lediglich an einen einheitlicher Ansprechpartner wenden müssen.

- Ein besonderes Augenmerk der Datenschutzbeauftragten richtet sich auf die den Versicherten eingeräumten Zugriffsmöglichkeiten auf die mit der Elektronischen Gesundheitskarte verarbeiteten Daten. Denn der dahinter stehende Auskunftsanspruch gehört datenschutzrechtlich zu den grundlegenden Rechten der Betroffenen. Die in der Gesamtarchitektur der Elektronischen Gesundheitskarte hierzu vorgesehenen Instrumente sind jedoch trotz dieser zentralen Bedeutung bislang weder verbindlich spezifiziert noch im Hinblick auf ihre Praxistauglichkeit getestet worden.

Derzeit vorgesehene Zugriffswege der Versicherten auf die Daten der Elektronischen Gesundheitskarte:

- pin@home
Den Versicherten soll mit dieser Anwendung vom heimischen PC aus ein lesender Zugriff auf die Daten der Pflichtanwendungen sowie die generelle Rechteverwaltung ermöglicht werden. Damit könnte der Versicherte beispielsweise elektronische Verordnungen oder einzelne Einträge in seiner Patientenakte für bestimmte Zielgruppen verbergen, die Nutzung freiwilliger Anwendungen deaktivieren oder Zugriffsprotokolle sichtbar machen. Unklar ist, ob auch die Erteilung bzw. der Entzug individueller Berechtigungen über pin@home realisiert werden soll. Anders als vom LfD zunächst befürwortet ist dagegen ein Zugriff der Versicherten auf ihre in den einzelnen freiwilligen Anwendungen gespeicherten medizinischen Daten nicht vorgesehen, es sei denn, diese befinden sich im Patientenfach (s.u.).

- Patienten- oder Versichertenfach
Nach dem derzeitigen Konzept der gematik sollen sämtliche in den freiwilligen Anwendungen der Elektronischen Gesundheitskarte verarbeiteten medizinischen Daten in das Patientenfach (§ 291a Abs. 3 Nr. 5 SGB V) kopiert und den Versicherten über die Anwendung pin@home mit den hierfür gesetzlich vorgesehenen Zugriffsvoraussetzungen von zu Hause aus zugänglich sein. Dem Patientenfach kommt somit nach der bestehenden Konzeption für die eigenständige und jederzeitige Wahrnehmung des Auskunftsanspruchs der Versicherten eine zentrale Rolle zu. Offen ist jedoch beispielsweise, ob und mit welchen technischen Voraussetzungen die Leistungserbringer die teilweise sehr umfangreichen medizinischen Daten in das Patientenfach kopieren können.

- eKiosk
Die bisherigen Überlegungen im Zusammenhang mit der Wahrnehmung der Betroffenenrechte sehen die Einrichtung von sog. eKiosken vor. Bei diesen handelt es sich um unentgeltlich bereit gestellte Umgebungen, über die der Versicherte autark ohne Anwesenheit eines Dritten auf die in der Elektronischen Gesundheitskarte gespeicherten Daten zugreifen kann. Geplant ist die Errichtung von eKiosken einerseits für überwachte und geschützte Räume bei den Leistungserbringern, andererseits für öffentlich zugängliche Bereiche. Das bislang vorliegende übergreifende Datenschutzkonzept der gematik sieht allerdings aus Gründen der Datensicherheit keine Zugriffsmöglichkeit der Versicherten vom eKiosk auf medizinische Daten der freiwilligen Anwendungen vor. Bislang ist auch nicht geklärt, inwieweit die Leistungserbringer überhaupt zur Errichtung von eKiosken in ihren Räumen bereit sind und unter welchen Bedingungen die Versicherten diese nutzen können.

- Auskunftsanspruch direkt bei den Leistungserbringern
Sofern die dargestellten Instrumentarien zur Sicherstellung der Einsichtsrechte der Versicherten auf die mit der Elektronischen Gesundheitskarte verarbeiteten medizinischen Daten nicht zur Verfügung stehen oder nutzbar sind, kommt ein direkter Auskunftsanspruch der Betroffenen gegen die einzelnen Leistungserbringer in Betracht. Es ist allerdings fraglich, ob und ggf. zu welchen Konditionen beispielsweise die Ärzte oder Apotheker derartigen Auskunftsverlangen entsprechen werden.

Der LfD hat sowohl über das in der Region Trier angesiedelte Modellprojekt zur Einführung der Elektronischen Gesundheitskarte als auch über die von den Datenschutzbeauftragten des Bundes und der Länder eingerichtete Arbeitgruppe eine unverzügliche Konzeption und Spezifikation der dargestellten Instrumentarien und deren Erprobung in den bestehenden Testvorhaben gefordert. Nun soll sich der Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unmittelbar mit diesem Anliegen an die gematik wenden. Angesichts der anstehenden Einführung der Elektronischen Gesundheitskarte ist eine baldige Klärung der aufgeworfenen Fragen geboten.

8.4 Das „oscare“-Verfahren

Unter Federführung des LfD hat die von den Datenschutzbeauftragten des Bundes und der Länder eingerichtete Arbeitsgruppe zur Begleitung der neuen AOK-Software oscare (vgl. 21. Tb., Tz. 11.3) wesentliche Erfolge bei der datenschutzgerechten Ausgestaltung des Verfahrens erzielt. Dies ist deshalb von besonderer Bedeutung, da oscare zwischenzeitlich nicht nur im AOK-Verbund, sondern auch darüber hinaus bei anderen Krankenkassen der Gesetzlichen Krankenversicherung zum Einsatz kommt.

Schwerpunkte der mit dem oscare-Management diskutierten Inhalte waren das dem Verfahren zugrunde liegende Rollen- und Berechtigungskonzept, die vorgesehenen

Archivierungs- und Löschungsmöglichkeiten sowie die Sicherstellung der Revisionsfähigkeit des Softwareeinsatzes insbesondere durch eine geeignete Zugriffsprotokollierung. Die in diesem Zusammenhang von den Datenschutzbeauftragten erhobenen Forderungen wurden bei der Verfahrensentwicklung weitgehend berücksichtigt.

Das bestehende Rollen- und Berechtigungskonzept ist grundsätzlich geeignet, den datenschutzrechtlichen Anforderungen gerecht zu werden. Die im Verfahren bereit gestellten Einzelrollen lassen die Einrichtung von Zugriffsberechtigungen in dem für die jeweilige Aufgabenerfüllung erforderlichen Umfang zu. Dies gilt auch für die von den Datenschutzbeauftragten schon seit langem geforderte Möglichkeit zur regionalen Beschränkung von Zugriffen. Es bleibt jedoch abzuwarten, ob die einzelnen Krankenkassen, bei denen oscare eingesetzt wird, die nun vorhandenen Möglichkeiten einer differenzierten und am Erforderlichkeitsgrundsatz orientierten Vergabe von Rollen und Berechtigungen auch tatsächlich nutzen.

Eine deutliche Verbesserung gegenüber der bislang im AOK-Verbund genutzten Software stellt das oscare zugrunde liegende Archivierungs- und Löschkonzept dar. Dieses basiert daten- und dokumentenbezogen auf der Festlegung einer Gesamtresidenzzeit sowie einer konkreten Ablagestrategie und ermöglicht anders als bisher nun auch eine physikalische Löschung der automatisiert gespeicherten Daten. Während die Festlegung der Gesamtresidenzzeiten der mit oscare gespeicherten Kategorien von Sozialdaten systemseitig entsprechend den gesetzlichen Vorgaben auf Master-Ebene erfolgt, obliegt es den einzelnen das Verfahren nutzenden Krankenkassen zu entscheiden, wie lange sie Daten bzw. Dokumente im Produktivbestand und im Archivbestand sowie in davon getrennten Speichermedien bis zur endgültigen Löschung vorhalten. Nach Ablauf der gesetzlichen Speicherfrist ist selbst bei unterbliebener physikalischer Vernichtung der Speichermedien aus der Software heraus eine Wiederherstellung der Daten nicht mehr möglich.

Mit der mittlerweile zur Verfügung stehenden grundsätzlichen Möglichkeit einer Protokollierung auch lesender Zugriffe in einer SAP-basierten Anwendung wird ein aus datenschutzrechtlicher Sicht bestehender gravierender Mangel des Projekts beseitigt werden. Ein von der SAP AG entwickeltes und erst im August 2009 der Arbeitsgruppe präsentiertes zusätzliches Modul soll die revisionssichere und umfassende Protokollierung der aus dem Verfahren erzeugten Datenzugriffe gewährleisten. Das oscare-Management wird nun in Abstimmung mit den Datenschutzbeauftragten die konkrete Ausgestaltung der im Verfahren oscare erforderlichen Protokollierungen festlegen.

8.5 Ärztliche Schweigepflicht und private Krankenversicherung

Im Berichtszeitraum erreichten den LfD zahlreiche Eingaben, die datenschutzrechtliche Beanstandungen zur Forderung einer umfassenden Schweigepflichtenbindungserklärung durch eine private Krankenversicherung beinhalteten. Im Rahmen der Leistungsgewährung sollte dem Versicherer durch Unterzeichnung dieser Einwilligungserklärung die Möglichkeit gegeben werden, Einblick in umfangreiche Gesundheitsunterlagen zu nehmen. Begründet wurde dieses Vorgehen mit Regelungen in den Allgemeinen Versicherungsbedingungen sowie damit, im Interesse der Mitglieder dieser Krankenversicherung die Anspruchsvoraussetzungen für den Erhalt einer Leistung zu prüfen. Dabei war oftmals nicht ersichtlich, ob die Schweigepflichtentbindungserklärung pauschal oder aber konkret auf die beantragte Leistung bezogen gefordert werden sollte.

Von den Datenschutzaufsichtsbehörden werden solche Schweigepflichtentbindungserklärungen bereits seit langem bemängelt. Aus diesem Grunde finden in regelmäßigen Abständen Zusammenkünfte der Aufsichtsbehörden und des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. (GDV) statt. Diese Unterredungen haben allerdings bislang zu keinem greifbaren Erfolg geführt: Ein von Seiten der Versicherungswirtschaft vorgelegter „Code of Conduct“, der im Wege der Selbstregulierung datenschutzrechtliche Standards im Versicherungsgewerbe setzen soll (Verhaltensregeln im Sinne des § 38a BDSG), ist bis heute nicht in Kraft – was sicherlich auch mit der nicht immer einheitlichen Position der Aufsichtsbehörden der Länder zusammenhängt.

Aus Sicht des LfD sind datenschutzrechtliche Einwilligungsklauseln, welche die Verarbeitung besonders sensibler personenbezogener Daten betreffen, einzelfallbezogen und so bestimmt wie möglich abzufassen. Pauschale oder generelle Einwilligungsklauseln werden demgegenüber abgelehnt, da für die Versicherungsnehmer dann nicht mehr absehbar ist, welche Informationen sich ihr Versicherer bei welcher Stelle beschaffen darf. Zudem soll den Betroffenen die Möglichkeit eingeräumt werden, selbst zu entscheiden, ob sie zur Prüfung der Leistungspflicht des Versicherers die Schweigepflichtentbindungserklärung abgeben möchten oder aber die hierfür erforderlichen Informationen selbst einholen und dann dem Versicherer zur Verfügung stellen möchten. Letzteres kann zwar zu zeitlichen Verzögerungen bei der Leistungsgewährung führen, darf aber mit keinerlei weiteren Nachteilen für die Versicherungsnehmer verbunden sein. In jedem Fall besteht seitens des Versicherers die Verpflichtung, Rückfragen bei Leistungs-

erbringern ausschließlich im zwingend erforderlichen Umfang und anlassbezogen zu tätigen und dies den Versicherten gegenüber entsprechend kenntlich zu machen.

Diese Position des LfD wird durch einen Beschluss des Bundesverfassungsgerichts vom 23. Oktober 2006 (1 BvR 2027/02) gestärkt, worin festgestellt wird, dass eine formularmäßige und sehr allgemein umschriebene Schweigepflichtentbindungserklärung (im konkreten Fall handelte es sich um eine Berufsunfähigkeitsversicherung) dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung entgegensteht. Statt eine umfassende pauschale Schweigepflichtentbindung zu verlangen, müsse ein Weg angeboten werden, der die durch die Schweigepflichtentbindung ermöglichten Auskünfte im Einzelfall und konkret beschreibe.

Durch das Gesetz zur Reform des Versicherungsvertragsgesetzes vom 23. November 2007 ist in § 213 VVG nunmehr eine Regelung zur Erhebung von Gesundheitsdaten bei Dritten aufgenommen worden, die seit dem 1. Januar 2009 auch für sog. Altverträge gilt. Die Datenschutzaufsichtsbehörden begrüßen diese Neuregelung ausdrücklich, da sie die Datenschutzrechte der Versicherten stärkt.

Der LfD steht mit dem rheinland-pfälzischen Versicherungsgewerbe in engem, regelmäßigen Kontakt und hat sich wiederholt von dessen grundsätzlich hohen Datenschutzstandards, die insbesondere auch die intensive Mitarbeiterschulung umfassen, überzeugen können. Aufgetretene Probleme konnten zumeist einvernehmlich gelöst werden; mangels länderübergreifender Lösungsansätze in Grundsatzfragen (Stichwort „Code of Conduct“) soll daher künftig verstärkt auf bilaterale Lösungen gesetzt werden.

9. Bildung und Wissenschaft

9.1 Bildung

9.1.1 Schulregelungen

Im Berichtszeitraum war der LfD wiederholt gefordert, bei der Neufassung von schulrechtlichen Normen aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Bei der Neufassung der Übergreifenden Schulordnung etwa wurde die Rechtslage auf Anregung des LfD an die Bedürfnisse der Praxis angepasst. So wurde in der Verordnung ergänzt, dass auch die Daten ehemaliger Schüler und Lehrkräfte in „Dokumentationen“, also Jahresberichten, Festschriften, Jubiläumsschriften etc. veröffentlicht und mit Klassenfotos untermalt werden dürfen. Um die Aktualität und Pflege der Erreichbarkeitsangaben von Eltern bzw. Schülern zu erleichtern, wurde die Übergreifende Schulordnung dahingehend ergänzt, dass die entsprechende Liste künftig auch online mit entsprechenden Zugriffsbefugnissen (Benutzername und Passwort) vorgehalten werden darf.

Der Vorschlag des LfD, die Veröffentlichung personenbezogener Daten von Eltern, Lehrkräften und Schülern im Internet in einer eigenen Bestimmung zu regeln, wurde leider nicht aufgegriffen. Umso wichtiger ist es, dass den Schulen, was die Internetnutzung angeht, konkrete Handlungsempfehlungen zu rechtlichen und technischen Fragen zur Verfügung gestellt werden konnten. Die Schule kann dabei selbst darüber entscheiden, ob sie die private Internetnutzung gestattet oder untersagt. In jedem Fall aber sollte für die Schüler eine Nutzungsordnung bzw. für die Lehrkräfte eine Dienstanweisung oder -vereinbarung die datenschutzrelevanten Fragen bei der Internetnutzung (z.B. Protokollierung, Auswertung und Löschung von Daten) regeln.

Der LfD hat für die beiden möglichen Varianten „Verbot“ und „Erlaubnis“ einer außerschulischen/privaten Internetnutzung Mustertexte erarbeitet und mit dem Bildungsministerium abgestimmt. Diese können unter folgenden Links abgerufen werden:

- http://www.datenschutz.rlp.de/downloads/oh/Musternutzungsordnung_IKT_Schule_keine_private_Nutzung.pdf
- http://www.datenschutz.rlp.de/downloads/oh/Musternutzungsordnung_IKT_Schule_private_Nutzung_zugelassen.pdf

9.1.2 Videoüberwachung an Schulen

Nachdem das Bildungsministerium noch im Jahr 2004 keine Kenntnis von Videokameras im Schulbereich hatte, ergab die vom LfD veranlasste Umfrage (s. Tz. 3.2) ein gänzlich anderes Bild: An 85 Schulen kommen derzeit insgesamt 193 Kameras zum Einsatz. Da die Rücklaufquote nur bei ca. 68 Prozent lag, muss von einer noch größeren Anzahl von Videoüberwachungsmaßnahmen im Schulbereich ausgegangen werden.

Auffällig war, dass sich der Kameraeinsatz nicht nur auf die Außenbereiche (Schulhof, Fahrradabstellplätze) beschränkt, sondern auch im Innenbereich eine Überwachung selbst von solch sensiblen Bereichen wie z.B. Lehrerzimmer, Sekretariatseingang oder Toiletten stattfindet. Eine Schule beklagte sich kurioserweise sogar darüber, dass die Videokamera bei einem Einbruch entwendet wurde.

Die Rückmeldungen ergaben, dass den gesetzlichen Voraussetzungen des § 34 LDSG in der Praxis vielfach nicht Rechnung getragen wird. So wurde beispielsweise die erforderliche Kennzeichnung der Videoüberwachung unterlassen, die aufgezeichneten Daten zu lange gespeichert oder allgemein gegen den Verhältnismäßigkeitsgrundsatz verstoßen. Die Ergebnisse der Umfrage wurden dem Bildungsministerium und den Lehrerpersonalräten zur Verfügung gestellt.

Der LfD hat zwischenzeitlich eine Orientierungshilfe zur Zulässigkeit von Videoüberwachungsmaßnahmen im Schulbereich erstellt, welche derzeit mit dem Bildungsministerium und dem kommunalen Spitzenverbänden abgestimmt wird. Sobald diese vorliegt, wird es die Aufgabe der schulischen Datenschutzbeauftragten sein, die praktische Situation vor Ort an diese Vorgaben anzupassen.

9.1.3 Online-Vertretungspläne

Immer wieder wenden sich Schulen mit der Frage an den LfD, ob der Vertretungsplan zulässigerweise auch im Internet-Angebot der Schule veröffentlicht werden darf. Datenschutzrechtlich gilt es dabei die berechtigten Interessen der Schüler, gerade bei langen Wegezeiten möglichst frühzeitig über Unterrichtsausfall informiert zu sein, abzuwägen mit dem ebenfalls berechtigten Interesse der Lehrkräfte, dass Hinweise über dienstliche Abwesenheiten als Personaldaten nicht allgemein zugänglich sein sollten. Dabei gilt folgende Regel: Je weniger personenbezogene Daten im Vertretungsplan selbst vorgehalten werden, desto geringer sind auch die zu stellenden technisch-organisatorischen Anforderungen.

Wenn beispielsweise lediglich Raumänderungen mitgeteilt werden oder über die bloße Tatsache des Unterrichtsausfalls informiert wird und dabei lediglich die Klassen bzw. Kurse genannt werden, genügt es, wenn der Zugang über eine Benutzerkennung und ein schulintern bekanntes Passwort erfolgt. Für den Fall, dass im Vertretungsplan dagegen Lehrkräfte namentlich bezeichnet werden, ist aus technisch-organisatorischer Sicht die Einrichtung einer geschlossenen Benutzergruppe unter Verwendung eines individuellen Passwortes zu fordern.

9.1.3 Agentur für Qualitätssicherung (AQS)

- Freiwillige oder verpflichtende Teilnahme?

Zu Zwecken der Evaluation von Schule können die Schulbehörden geeignete Verfahren einsetzen und durch Befragungen und Unterrichtsbeobachtungen erhobene Daten verarbeiten. Rechtliche Grundlage für die Verarbeitung personenbezogener Daten ist § 67 Abs. 2 SchulG, wonach personenbezogene Daten für diese Zwecke auch ohne Einwilligung der Betroffenen verarbeitet werden dürfen, wenn das öffentliche Interesse an der Durchführung eines von der obersten Schulbehörde genehmigten Verfahrens die schutzwürdigen Belange derBetroffenen erheblich überwiegt und der Zweck des Vorhabens auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann. Die Betroffenen sind über die Evaluationsmaßnahme zu unterrichten; eine Mitwirkungspflicht besteht allerdings nur dann, wenn die vorzunehmende Güterabwägung ein deutliches Überwiegen des öffentlichen Interesses gegenüber den schutzwürdigen Belangen der Betroffenen ergibt.

In Rheinland-Palz hat die Agentur für Qualitätssicherung, Evaluation und Selbständigkeit von Schulen (AQS) den Auftrag, die externe Evaluation der rund 1.600 rheinland-pfälzischen Schulen in öffentlicher Trägerschaft durchzuführen. Mit diesem Blick von außen, der externen Evaluation, will die AQS die Schulen dabei unterstützen, die Qualität des Unterrichts und der Schule langfristig und nachhaltig weiter zu entwickeln. Dabei setzt die AQS empirische Methoden der Datenerhebung und Auswertung ein. Über das Ergebnis der Evaluation erhalten die Schulen eine Rückmeldung in Form eines schriftlichen Berichts. Die AQS bildet eine eigenständige Organisationseinheit im Geschäftsbereich des Ministeriums für Bildung, Wissenschaft, Jugend und Kultur und ist dem Präsidenten der Aufsichts- und Dienstleistungsdirektion unterstellt. Nach Abschluss der Erstevaluation aller rheinland-pfälzischen Schulen durch die AQS-Teams sind Schulbesuche im fünfjährigen Turnus vorgesehen.

Da die vorzunehmende Güterabwägung im Rahmen des § 67 Abs. 2 SchulG in Bezug auf Schüler sowie Eltern ein Überwiegen der schutzwürdigen Interessen dieser Betroffenen gegenüber dem öffentlichen Interesse an der Evaluation ergibt, ist die Befragung der AQS für Schüler sowie deren Eltern lediglich auf freiwilliger Basis möglich. Für Lehrkräfte fällt die Abwägung mit Blick auf die beamtenrechtliche Gehorsampflicht jedoch zugunsten des öffentlichen Interesses aus; für sie ist die Teilnahme daher verpflichtend. Der Gesetzgeber hielt es gleichwohl für angezeigt, die Mitwirkungsverpflichtung der Lehrkräfte im Rahmen der Evaluation gleich mehrfach gesetzlich zu verankern: §§ 23 Abs. 2, 25 Abs. 1 SchulG sowie die neue Vorschrift in § 97a Abs. 3 SchulG sehen entsprechende Mitwirkungsobliegenheiten für Lehrkräfte ausdrücklich vor.

Die zum Einsatz kommenden Erhebungsinstrumente der AQS sehen teilweise vor, dass die Schüler auch über ihre Eltern befragt werden. Z.B. sollten als zutreffend oder unzutreffend deklariert werden: „Meine Eltern fordern zu viele schulische Leistungen von mir“, „Zu Hause kann ich machen, was ich will“ oder „Meine Eltern sind meistens so genervt, dass ihnen meine Hausaufgaben egal sind“. Weiterhin wurden die Schüler über die berufliche Situation ihrer Eltern und deren Bildungsabschlüsse befragt. Schließlich sollte angegeben werden, ob zu Hause Kunstwerke, klassische Literatur, ein Garten, eine Spülmaschine u.v.m. vorhanden sind.

In Eingaben beim LfD ist wiederholt nachgefragt worden, warum diese Daten bei den Kindern und nicht bei den Eltern erhoben werden. Auch wurde problematisiert, dass die Eltern nicht oder nur sehr unzureichend darüber informiert werden, worüber ihre Kinder gegenüber der AQS Auskunft geben sollen.

Aus diesem Grunde hat der LfD gegenüber der AQS gefordert, dass die Eltern in einem Anschreiben über die Möglichkeit unterrichtet werden, den Fragebogen ihrer Kinder im Schulsekretariat einzusehen, damit sie auf der Basis dieser Informationen über die Teilnahme ihres Kindes entscheiden können. Dies wurde seitens der AQS zeitnah umgesetzt.

Ebenfalls aufgrund von Hinweisen erhielt der LfD davon Kenntnis, dass Schulleitungen vereinzelt über das Ziel hinausgeschossen sind, indem sie beispielsweise versuchten, einen möglichst vollständigen Rücklauf der Fragebögen durch deren Kennzeichnung oder das Führen einer Rücklaufliste sicherzustellen. Die AQS hat gegenüber den betroffenen Schulleitungen auf die Unzulässigkeit einer diesbezüglichen Praxis hingewiesen. Die Schulleitungen haben dies umgehend eingestellt.

- Datenverarbeitung durch die AQS

Der LfD hat zur Datenverarbeitung durch die AQS in Anwesenheit von Vertretern der Lehrerpersonalräte örtliche Feststellungen zum Datenschutz getroffen. Diese haben Folgendes ergeben:

Die bei der AQS eingehenden ausgefüllten Fragebögen (Befragung von Lehrkräften und Schülern erfolgt online; Eltern erhalten einen Papierfragebogen) werden wie folgt verarbeitet:

Die eingehenden Elternfragebögen werden über eine spezielle Software eingescannt. Die Bögen wurden zuvor mit einer eindeutigen ID versehen, um die richtige Zuordnung der einzelnen Seiten zu dem jeweiligen Fragebogen vornehmen zu können. Dies stellt sicher, dass fotokopierte Fragebögen als solche erkannt und aus der Auswertung herausgenommen werden können sowie gegen inhaltliche Veränderungen geschützt sind.

Nach Abschluss der Befragung erfolgt eine Zusammenführung der Daten aus der Online- und der papiergebundenen Befragung in einer auf die jeweilige Schule bezogenen Tabelle. Dazu werden die Ergebnisauswertungen der gescannten Elternfragebögen sowie die Daten der Online-Datenbank des Landesbetriebs Daten und Information (Lehrer- und Schülerbefragung) in die schulbezogenen Datensätze der AQS-Datenbank übertragen.

Im weiteren Verlauf der Bearbeitung werden für alle Schulen sog. Views erstellt, in denen Schulname und -nummer durch einen 13-stelligen Hashcode ersetzt sind.

Drei Koordinatoren verfügen über die Referenzliste mit den erzeugten Hashcodes und den dazu gehörigen Schulnamen. Ein Zugriff auf die Datenbank mit den ausgefüllten Fragebögen ist diesen Mitarbeitern aber nicht möglich. Die Koordinatoren ermitteln, bei welchen Schulen die Evaluationsdaten vollständig eingegangen sind und somit ausgewertet werden können. Die Weitergabe an das Auswertungsteam erfolgt dergestalt, dass blockweise jeweils zehn Schulen (zusammengesetzt aus unterschiedlichen Schularten) ausgewählt und durch Weitergabe des Hashcodes an die Wissenschaftler der AQS übergeben werden.

Das Auswertungsteam greift sodann anhand des übermittelten Hashcodes auf die entsprechenden Views der Datenbank zu und nimmt die Auswertung der Fragebögen vor. Den Wissenschaftlern wird dabei lediglich die Schulart, nicht jedoch Schulname oder Schulnummer bekannt.

Nach Abschluss der Auswertung werden die Ergebnisse der Befragung (aggregierte Datensätze ohne Personenbezug) in einem speziellen Ordner elektronisch abgelegt und an die Koordinatoren übermittelt. Anschließend werden die ausgewerteten Daten in Tabellen und Grafiken übertragen. Erst nach Abschluss dieser Prozedur werden die erstellten Dateien, die nunmehr lediglich statistische Daten enthalten, durch Reidentifizierung anhand des Hashcodes mit Schulname und Schulnummer versehen und in dem jeweiligen Schulordner abgelegt.

Um die Anonymität bei der Befragung kleiner Schulen (z.B. Grundschulen mit weniger als zehn Beschäftigten) zu gewährleisten, wurde ein gesondertes Verfahren (u.a. Mittelwertbildung bei der Auswertung des Lehrkräftefragebogens) entwickelt.

Aus Sicht des LfD stellt das beschriebene Verfahren hinreichend sicher, dass ein Rückschluss auf die Person, die den Fragebogen ausgefüllt hat, nicht möglich ist.

9.1.5 Pädagogische Netzwerke in Schulen

Die Mehrheit der Schulen im Land nutzt zur Unterrichtsunterstützung sog. pädagogische Netzwerke. Diese bieten z.T. den Lehrkräften die Möglichkeit, vom Lehrerarbeitsplatz die Bildschirminhalte der Schüler-PC durch softwaregestütztes Aufschalten einzusehen.

Seitens der Landesschülervertretung wurde gegenüber dem LfD problematisiert, dass es hierbei möglicherweise zu unbefugter Einsichtnahme kommen kann, da das Aufschalten je nach Art des pädagogischen Netzwerkes nur unzureichend bzw. in einigen Fällen gar nicht kenntlich gemacht wird. Hierbei ist anzumerken, dass eine Nutzung der PC durch die Schüler teils ausschließlich zu Unterrichtszwecken, teils zur Unterrichtsvorbereitung (z.B. in Freistunden) oder auch teilweise zur außerschulischen Nutzung zugestanden war. Die Befugnis der Lehrkräfte zur „Kontrolle“ ist hierbei – in Abhängigkeit vom Einsatzszenario – unterschiedlich zu bewerten.

In Zusammenarbeit mit dem Bildungsministerium sind hierzu durch den LfD zwei Musternutzungsordnungen „Informations- und Kommunikationstechnik an Schulen“ entstanden, die entsprechende Regelungsvorgaben enthalten:

- http://www.datenschutz.rlp.de/downloads/oh/Musternutzungsordnung_IKT_Schule_keine_private_Nutzung.pdf
- http://www.datenschutz.rlp.de/downloads/oh/Musternutzungsordnung_IKT_Schule_private_Nutzung_zugelassen.pdf

Der LfD konnte erreichen, dass das Aufschalten von Lehrkräften auf die Schüler-PC für die Schüler eindeutig erkennbar ist.

Die Nutzung pädagogischer Netzwerke bei Fragebogenaktionen der Agentur für Qualitätssicherung, Evaluation und Selbständigkeit von Schulen (AQS) ist untersagt.

9.1.6 Bildungsberichterstattung und Schulstatistik

Nach einem Beschluss der Kultusministerkonferenz soll länderübergreifend jeder Schüler über die Vergabe einer Identifikationsnummer möglichst für den gesamten Bildungsverlauf nur mit einem Datensatz geführt werden. Zur Begründung wurde darauf hingewiesen, dass die „Nutzung von Individualdaten als Instrument der Koordinierung politischer und planerischer Maßnahmen sowie für die internationale Zusammenarbeit“ notwendig sei.

Die von den Datenschutzbeauftragten geäußerte Kritik an diesem Vorhaben konnte auch mit einem im Jahr 2008 vorgelegten überarbeiteten Konzept nicht vollständig ausgeräumt werden. Eine erneute Stellungnahme der Kultusministerkonferenz bzw. deren Arbeitsausschuss „Statistik“ zu den von den Datenschutzbeauftragten formulierten Anforderungen an eine denkbare datenschutzkonforme Ausgestaltung eines solchen Vorhabens oder eine Fortentwicklung des Konzepts steht noch aus.

In Rheinland-Pfalz ist für die Statistik im Schulbereich die Umstellung von zusammengefassten Daten (Summenbeträge) auf Individualdaten bereits erfolgt, die Darstellung von Bildungsverläufen ist nicht möglich. Auch die Umstellung auf einen Datensatz mit bundesweit übereinstimmenden Inhalten war bereits im Gang. Die Arbeit einer vom Ministerium für Bildung, Wissenschaft, Jugend und Kultur eingerichteten „Arbeitsgruppe Kerndatensatz“, in der auch Mitarbeiter des LfD vertreten sind, ist bis auf Weiteres ausgesetzt.

Der LfD wird neue Entwicklungen in diesem Bereich im Fokus behalten.

9.2 Wissenschaft

9.2.1 Von der Videoüberwachung bis zu Forschungsvorhaben

Die Arbeit in diesem Bereich wurde im Berichtszeitraum von zwei Schwerpunkten bestimmt. Dies war zum einen die Videoüberwachung an Hochschulen (s.a. Tz. 3.2). Zu diesem Zweck wurde eine Umfrage an den staatlichen Hochschulen in Rheinland-Pfalz durchgeführt und der praktizierte Einsatz von Videoüberwachungstechnik an fünf Hochschulen vor Ort in Augenschein genommen. Im Ergebnis wurde festgestellt, dass an allen Hochschulen Videoüberwachung betrieben wird und teilweise Nachbesserungsbedarf besteht. Hauptanwendungsfall für den Einsatz dieser Technik sind PC-Pools und EDV-Labore.

Um künftig eine rechtskonforme und zurückhaltende Anwendung der Videoüberwachung zu ermöglichen, wurde ein Entwurf für eine Orientierungshilfe zum Einsatz dieser Technik an Hochschulen erarbeitet. Der Abstimmungsprozess mit Vertretern der Hochschulen sowie des Ministeriums für Bildung, Wissenschaft, Jugend und Kultur dauert noch an.

Zum anderen bestimmte die datenschutzrechtliche Prüfung wissenschaftlicher Forschungsvorhaben, die mit der Verarbeitung personenbezogener Daten einhergehen, das Tagesgeschäft. So wurden dem LfD allein wegen der Verarbeitung von Daten für wissenschaftliche Untersuchungen in Schulen durch externe Stellen im Berichtszeitraum gut 100 Vorhaben zur Prüfung vorgestellt.

Aber auch im Bereich Wissenschaft und Hochschulen muss sich der LfD mit ganz alltäglichen Fragestellungen beschäftigen, wie der folgende Sachverhalt zeigt:

Ein behördlicher Datenschutzbeauftragter warf im Hinblick auf die Versteigerung von Fundsachen die Frage auf, ob auf Mobiltelefonen und USB-Speichermedien evtl. noch abgespeicherte personenbezogene Daten vor einer Versteigerung vollständig zu löschen sind. In der Abgabe von Mobiltelefonen oder USB-Speichermedien, die noch personenbezogene Daten enthalten, an natürliche Personen wäre eine Datenübermittlung an nicht-öffentliche Stellen zu sehen. Eine Rechtsgrundlage für diese Datenverarbeitung einer Hochschule als verantwortlicher Stelle ist aus § 16 Abs. 1 i.V.m. § 12 Abs. 4 und § 13 Abs. 2 LDSG nicht ersichtlich. Wenn die zivilrechtlichen Voraussetzungen für eine Versteigerung solcher Fundsachen durch eine Hochschule erfüllt sind, müssten vor der Übergabe der Gegenstände darauf befindliche personenbezogene Daten gelöscht werden. Dies gilt bei einem Mobiltelefon insbesondere für das Telefonbuch, den SMS- bzw. MMS-Speicher und die Liste der ein- sowie ausgegangenen Anrufe. USB-Speichermedien oder sonstige Datenträger sind vor der Übergabe sicher zu löschen.

9.2.2 Wissenschaftspreis des LfD

Am 1. Dezember 2008 wurde im Landtag Rheinland-Pfalz erstmals der Wissenschaftspreis des LfD verliehen. Mit ihm werden herausragende wissenschaftliche Arbeiten mit

Datenschutzbezug gewürdigt, die an rheinland-pfälzischen Hochschulen erstellt werden. Der im Kreis der Datenschutzbeauftragten bislang einzige, gemeinsam vom Ministerium für Bildung, Wissenschaft, Jugend und Kultur und dem LfD getragene und mit 1.000 Euro dotierte Preis soll die wissenschaftliche Auseinandersetzung mit datenschutzrechtlichen Fragen fördern und die Bedeutung des in der Landesverfassung ausdrücklich geregelten Rechts auf informationelle Selbstbestimmung unterstreichen.

Der LfD knüpft die Erwartung an den Preis, dass sich die Hochschulen in ihren verschiedenen wissenschaftlichen Disziplinen noch stärker als bisher mit dem Datenschutzgrundrecht befassen, da dieses nicht nur ein Individualrecht ist, sondern auch eine Vorraussetzung für unsere freiheitlich-demokratische Ordnung. Diese kann von der Entwicklung der Informationstechnologie profitieren, aber unter ihr auch Schaden nehmen. Dies abzuwenden ist nicht Aufgabe des Gesetzgebers alleine. Auch Wissenschaft und Forschung müssen einen Beitrag dazu leisten. Je komplexer die technologische Entwicklung ist, desto dringender wird die Unterstützung gerade auch von Seiten der Hochschulen.

10. Kommunales und Meldewesen

10.1 Kommunales

10.1.1 Videoüberwachung in den Kommunen

Zur Bestandsaufnahme wurde zu diesem Thema eine Umfrage bei 236 Kommunalverwaltungen durchgeführt, der Rücklauf betrug nahezu 80 Prozent. Meistgenannte Anlässe für den Einsatz von Videoüberwachungstechnik waren Einbrüche, Vandalismus und Brandstiftung, am häufigsten genannte Standorte für Videokameras waren Eingangsbereiche von Verwaltungsgebäuden, Außenbereiche von Liegenschaften, Museen u.a. Als Ergebnis der Auswertung ist festzuhalten, dass, ähnlich wie bei den Hochschulen, Nachbesserungsbedarf im Hinblick auf die vollständige Rechtmäßigkeit der Anlagen besteht.

Anhand der hierbei gewonnenen Erkenntnisse wurde auch für diesen Bereich eine Orientierungshilfe ausgearbeitet und mit den Kommunalen Spitzenverbänden sowie dem Ministerium des Innern und für Sport abgestimmt. Mittlerweile verfügt jeder behördliche Datenschutzbeauftragte einer Kommunalverwaltung über ein Exemplar.

Weiterhin wurden verschiedene bereits in Betrieb genommene Videoüberwachungsanlagen vor Ort überprüft. Teilweise stellten Kommunalverwaltungen auch erst beabsichtigte Vorhaben dem LfD mit der Bitte um Stellungnahme vor. Die Äußerungen des LfD haben regelmäßig dazu geführt, dass Kameras abgebaut oder die tägliche Dauer der Videoüberwachung eingeschränkt wurde. Teilweise haben Kommunen dann gänzlich von einem solchen Vorhaben Abstand genommen.

Im Fall einer Kommune, die trotz der vom LfD geäußerten datenschutzrechtlichen Bedenken mehrere Videokameras in Betrieb genommen hatte, führte dies allerdings zu einer förmlichen Beanstandung, der schärfsten Form der Missbilligung eines Verstoßes gegen Datenschutzrecht. Die Angelegenheit konnte bis zum Ende des Berichtszeitraumes nicht abgeschlossen werden.

Obwohl der Bereich „Kommunales“ im Berichtszeitraum vorrangig von diesem Arbeitsschwerpunkt geprägt war, bestand die Gelegenheit – wie die folgenden Ausführungen zeigen –, sich auch mit anderen Sachverhalten auseinander zu setzen.

10.1.2 Datenschutz und Kommunalwahlen

Die Wahl gab im Vorfeld Anlass zu zahlreichen Eingaben und Anfragen von Bürgern. Ein Bürger problematisierte, ob es mit dem Grundsatz der geheimen Wahl zu vereinbaren sei, wenn bei Mehrheitswahl der Stimmzettel handschriftlich ausgefüllt wird. Beispielsweise in kleineren Gemeinden sei es nicht auszuschließen, dass ein Wahlberechtigter von einem Mitglied des Wahlvorstandes aufgrund der Handschrift identifiziert werden könne.

Zu diesem Aspekt hat sich das Oberverwaltungsgericht Rheinland-Pfalz in einem Urteil (Az. 7 A 75/78) geäußert. Demnach stellt es keine Verletzung des Grundsatzes der geheimen Wahl dar, wenn die Stimmzettel handschriftlich (durch Aufschreiben des Namens des Gewählten) auszufüllen sind. Das Wesen der geheimen und freien Wahl bestehe darin, dass der Wähler von Dritten unbeobachtet und ohne irgendeine Beeinflussung von außen bei der eigentlichen und entscheidenden Abstimmungshandlung, d.h. innerhalb der Wahlkabine seinen Willen frei bekunden könne.

Eine Bürgerin warf die Frage auf, ob die auf dem Antragsformular für die Erteilung eines Wahlscheines eröffneten Auswahlmöglichkeiten und die damit ggf. verbundene zusätzliche Information für die Verwaltung – Ausübung des Wahlrechts nur bei Kommunalwahlen, kein Interesse an der Europawahl – mit dem Datenschutzrecht vereinbar ist.

Hier ist zum einen zu beachten, dass die Briefwahlunterlagen für jede Wahl gesondert beantragt werden müssen (§ 18 KWO, § 26 EuWO, § 4 der Landesverordnung über die gemeinsame Durchführung der Kommunalwahl mit der Europawahl). Zum anderen dürfen einem Wähler im Hinblick auf den Wahlrechtsgrundsatz der Freiheit der Wahl Briefwahlunterlagen nicht „aufgedrängt“ werden. Darin könnte eine Beeinflussung dahingehend gesehen werden, von der Stimmabgabe unter den erleichterten Bedingungen doch Gebrauch zu machen.

Außerdem ist die Information, wer sein Wahlrecht ausgeübt hat oder nicht, für einen bestimmten Personenkreis jedenfalls aus dem Wählerverzeichnis ersichtlich. Wenn das Grundgesetz dem Gesetzgeber gestattet, dafür zu sorgen, dass nach Möglichkeit alle Wahlberechtigten ihr Wahlrecht ausüben und dafür die Stimmabgabe durch Briefwahl erleichtert wird, muss demgegenüber die Wahrung des Wahlgeheimnisses zurücktreten. Der LfD erhob daher keine Bedenken gegen die Gestaltung des Antragsformulares.

10.1.3 Zuwendungen Privater an Kommunen

Mit dem Landesgesetz zur Änderung kommunal- und dienstrechtlicher Vorschriften vom 21. Dezember 2007 wurden Bestimmungen zur Entgegennahme von Spenden, Schenkungen und ähnlichen Zuwendungen durch kommunale Wahlbeamte getroffen. Das Verfahren ist in § 94 Abs. 3 GemO bzw. in § 58 Abs. 3 LKO geregelt. Danach hat die Verwaltung dem Gemeinderat bzw. Kreistag und der Aufsichtsbehörde sämtliche für die Entscheidung über die Annahme von Zuwendungen maßgebliche Tatsachen offen zu legen. Zu den maßgeblichen Tatsachen gehört insbesondere ein anderweitiges Beziehungsverhältnis (z.B. Lieferbeziehung oder Verwaltungsakt) mit dem Geber.

Aus der Pflicht zur Offenlegung der maßgeblichen Tatsachen kann seitens des mit der Entgegennahme von Spenden befassten Amtsträgers eine Anfrage bei allen Funktionsbereichen einer Behörde resultieren, da solche Beziehungsverhältnisse in vielen Verwaltungsbereichen denkbar sind. Rechtsgrundlagen für entsprechende Datenweitergaben innerhalb der Behörde sind grundsätzlich vorhanden, Kollisionen mit Amtsgeheimnissen sind aber nicht ausgeschlossen.

Da die Verwaltungen und Aufsichtsbehörden mit diesem Verfahren Neuland betreten haben, hat der LfD frühzeitig sein Interesse daran zum Ausdruck gebracht, in die Erstellung von Handlungsempfehlungen zur Konkretisierung der Ausführung der o.g. Vorschriften eingebunden zu werden. Der LfD hat an der Formulierung einer Handlungsempfehlung des Ministeriums des Innern und für Sport mitgewirkt und verschiedene Anmerkungen zum Schutz datenschutzrechtlicher Belange der Beteiligten eingebracht. Bisher liegen keine Erkenntnisse vor, dass dieses Verfahren in den Verwaltungen Anlass für Beschwerden seitens der Spender gibt.

10.2 Meldewesen

10.2.1 Bundesmeldegesetz

Im Zuge der Föderalismusreform ist die Gesetzgebungszuständigkeit für das Meldewesen von den Ländern auf den Bund übergegangen. Ein Referentenentwurf für ein Bundesmeldegesetz liegt bereits vor, das Gesetzgebungsverfahren ist jedoch insgesamt ins Stocken geraten, so dass derzeit noch nicht abzusehen ist, wann das neue Bundesmeldegesetz in Kraft treten wird.

In einem gemeinsamen Eckpunktepapier haben die Datenschutzbeauftragten des Bundes und der Länder ihre Bedenken gegen den Aufbau eines zentralen Bundesmelderegisters zusammengefasst und Forderungen aufgestellt, die aus datenschutzrechtlicher Sicht an ein neues Meldegesetz zu stellen sind. Hervorzuheben ist insoweit, dass die bestehenden Widerspruchsmöglichkeiten gegen die Weitergabe von Meldedaten an Adressbuchverlage oder an öffentlich-rechtliche Religionsgesellschaften oder gegen die Weitergabe von Jubiläumsdaten weitgehend von einer Einwilligungslösung abgelöst werden. Für die Wahrnehmung der Betroffenenrechte ist die Unterscheidung zwischen Widerspruch und Einwilligung von herausragender Bedeutung: Bei der „Widerspruchslösung“ müssen die Betroffenen nämlich selbst aktiv werden, um Datenweitergaben zu unterbinden und damit gewissermaßen „ihren Daten hinterherlaufen“, während bei der Einwilligungslösung die Zulässigkeit der Weitergabe vom vorherigen Einverständnis abhängt. Es versteht sich von selbst, dass sich diese Unterscheidung maßgeblich auf den Umfang der übermittlungsfähigen Daten auswirkt und die potenziellen Datenempfänger insoweit für die Beibehaltung der Widerspruchsmöglichkeit plädieren. Aufgrund der Eingabesituation lässt sich aus Sicht des LfD jedoch schon seit jeher feststellen, dass den Bürgern trotz bestehender Hinweisverpflichtungen der Meldeämter ihre gesetzlichen Widerspruchsmöglichkeiten nicht bekannt sind.

So hatte sich ein Bürger an den LfD gewandt, weil er sein Geburtstagsjubiläum zufällig im Internetnetangebot einer Zeitung fand. Auf der Basis des rheinland-pfälzischen Meldegesetzes ist es zulässig, bei nicht ausgeübtem Widerspruch u.a. auch die Presse über Alters- und Ehejubiläen zu informieren (§ 35 Abs. 3 MG). Es ist aus Sicht des LfD nicht akzeptabel, dass die bloße Nichtausübung einer (meist nicht bekannten) Widerspruchsmöglichkeit zu einer Veröffentlichung von Meldedaten im Internet führt. Hier ist der Gesetzgeber gefordert, im künftigen Meldegesetz die Datenschutzrechte seiner Bürger besser zu schützen. Die Meldegesetze von Thüringen und Sachsen etwa enthalten für diese Form der Veröffentlichung entsprechende rechtliche Grundlagen; in Berlin ist sie sogar von der Einwilligung des Betroffenen abhängig. In diesem Sinne sollte nach Auffassung des LfD auch das künftige Meldegesetz geregelt werden. Dass die Rechtsträger der Meldeämter die gegenwärtige Situation selbst als unbefriedigend empfinden, zeigt das Beispiel einer Kommune, die von sich aus und ohne Bestehen einer rechtlichen Verpflichtung den Betroffenen eine eigenständige Widerspruchsmöglichkeit gegen die Veröffentlichung von Jubiläumsdaten auf der Homepage der Gemeinde einräumte.

Lediglich aufgrund der verfassungsrechtlich garantierten Stellung der politischen Parteien ist es hinnehmbar, für die

Übermittlung von Meldedaten an politische Parteien im Vorfeld von Wahlen die Widerspruchlösung beizubehalten. In diesem Sinne hatte sich der LfD in einer Presseerklärung vor der Bundestagswahl am 27. September 2009 geäußert.

10.2.2 „Wer-kennt-wen“ im Meldeamt

Wie dem LfD im Rahmen der regelmäßigen Fortbildungsveranstaltungen zum Datenschutz im Meldeamt bekannt wurde, nutzen einzelne Sachbearbeiter ihren privaten Account bei sozialen Online-Netzwerken auch für dienstliche Zwecke. In einem Fall ging es um die Eintragung einer Auskunftssperre wegen einer Gefahrensituation (§ 34 Abs. 8 MG). Da der Sachbearbeiter durch eine Recherche in dem sozialen Netzwerk „wer-kennt-wen“ feststellte, dass der Antragsteller dort seine Anschrift selbst veröffentlicht hatte, wurde sein Antrag abgelehnt.

Gegen diese Praxis bestehen datenschutzrechtliche Bedenken: Die Nutzung des privaten Accounts stellt regelmäßig einen Verstoß gegen die Allgemeinen Geschäftsbedingungen der Netzbetreiber dar (s.a. Tz. 6.2.2). Diese Bestimmungen sehen nämlich in aller Regel vor, dass das Netzwerk nur zu privaten Zwecken genutzt werden darf. Außerdem sollten staatliche Ermittlungsmaßnahmen grundsätzlich offen und nicht heimlich unter zweckwidriger Verwendung faktischer Zugangsmöglichkeiten erfolgen. Ähnlich wie dies bei der Veröffentlichung der Anschrift in Telefonbüchern der Fall ist, sollten die Betroffenen vielmehr in einem Gespräch auf die Problematik der Veröffentlichung von im Melderegister gesperrten Daten hingewiesen werden.

10.2.3 Meldedaten für Werbezwecke und Adresshändler

In einer grundlegenden Entscheidung des Bundesverwaltungsgerichtes aus dem Jahr 2006 hatte das Gericht festgestellt, dass den Betroffenen neben den gesetzlich festgelegten Widerspruchsmöglichkeiten auch das Recht zuzuerkennen ist, der Weitegabe von Meldedaten zu widersprechen, wenn sie erkennbar für Zwecke der Direktwerbung erfolgen soll. In dem Urteil (Az: BVerwG 6 C 5.05) stützt das Gericht das Begehren des Betroffenen auf die zentrale melderechtliche Vorschrift des § 7 MRRG (bzw. § 6 MG), wonach schutzwürdige Interessen der Betroffenen durch die Verarbeitung personenbezogener Daten nicht beeinträchtigt werden dürfen. Die Vorschrift – so das Bundesverwaltungsgericht – will der Meldebehörde eine „Feinsteuerung“ gerade bei der Erteilung einfacher Melderegisterauskünfte ermöglichen. Der LfD hatte in der Vergangenheit stets auf die herausragende Bedeutung dieser Norm für das gesamte Meldewesen in Gesprächen mit dem Innenministerium und sog. Bedarfsträgern, also Stellen, die einen Zugriff auf Meldedaten begehrten, hingewiesen und sieht sich mit dieser Entscheidung auch in seiner Rechtsauffassung bestätigt, dass es sich bei Meldedaten keinesfalls um allgemein zugängliche Daten handelt. Inzwischen ist das Urteil des Bundesverwaltungsgerichts auch technisch umgesetzt worden. Die Software der Meldeämter wurde überarbeitet, die Vordrucke für die Widerspruchsmöglichkeiten und die Texte für die gesetzlich vorgeschriebenen Veröffentlichungen entsprechend ergänzt. Damit ist sichergestellt, dass alle Meldeämter in Rheinland-Pfalz die gerichtlichen Vorgaben korrekt umsetzen.

Leitsatz der Entscheidung des Bundesverwaltungsgerichts vom 21. Juni 2006 (6 C 5.05):
„Die Meldebehörde darf eine einfache Melderegisterauskunft (§ 21 Abs. 1 MRRG) nicht erteilen, wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird und der Betroffene einer Weitergabe seiner Daten für solche Zwecke zuvor ausdrücklich widersprochen hat.“

Über die Speicherung und Nutzung von Meldedaten durch gewerbsmäßige Adresshändler wurde in den vergangenen Monaten wiederholt in der Presse berichtet; sie war auch Gegenstand parlamentarischer Anfragen im rheinland-pfälzischen Landtag. Die gewerbsmäßigen Adresshändler haben nämlich ein Interesse daran, kostenspielige Anfragen bei den Meldeämtern in der Bundesrepublik durch das Speichern und Nutzen eigener Datenbestände zu vermeiden. Datenschutzrechtlich ist dies deshalb problematisch, weil die bestehenden Schutzmechanismen der Meldegesetze (§§ 7, 34 Abs. 8 MG: Beachtung der schutzwürdigen Interessen der Betroffenen vor einer Auskunftserteilung) bei dieser Vorgehensweise unterlaufen werden können.

Nach Kenntnis des LfD speichern die vier in Rheinland-Pfalz tätigen Unternehmen (Adress Research, PSI-Reiser, Regis24 und WID) die ihnen übermittelten Meldedaten nicht dauerhaft und geben sie insbeseondere auch nicht an andere Unternehmen oder Personen als die anfragenden Auftraggeber weiter.

In Bezug auf ein Unternehmen gab es jedoch weiteren Klärungsbedarf, so dass es zu einer Besprechung unter Beteiligung des Innenministeriums, der Gesellschaft für Kommunikation und Wissenstransfer mbH (KommWis) und Vertretern des LfD kam. Im Rahmen dieser Besprechung wurden die Beteiligten über die Praxis eines sog. Treuhandpool-Modells in Kenntnis gesetzt. In diesen Pool können die Kunden des Unternehmens die ermittelten Adressdaten einstellen und somit anderen Kunden für Recherchen zur Verfügung stellen. Nach

eigener Einschätzung agiert das Unternehmen insoweit lediglich als „Auftragsdatenverarbeiter“ für die Gesamtheit der am Poolkonzept teilnehmenden Auftraggeber. Das Innenministerium vertrat demgegenüber die Auffassung, dass im vorliegenden Fall die Konstruktion einer Auftragsdatenverarbeitung nicht haltbar sei und dass die datenschutzrechtlichen Zulässigkeitsvoraussetzungen nach den §§ 28, 29 BDSG mangels Einzelfallprüfung nicht gegeben seien. Aufgrund dieser Bedenken hat das Unternehmen die rheinland-pfälzischen Meldedaten zwischenzeitlich aus dem Pool entfernt und dies gegenüber dem LfD und dem Innenministerium schriftlich bestätigt.

11. Justiz

11.1 Strafprozessordnung

Erhebung von Verkehrsdaten aus der Telekommunikation und andere verdeckte Maßnahmen

Seit dem 1. Januar 2002 ist die Abfrage von Verkehrsdaten aus der Telekommunikation (also von Daten, die Auskunft über die Teilnehmer, den Zeitpunkt und die Dauer von Telekommunikationsvorgängen, nicht aber über deren Inhalt geben) zu Strafverfolgungszwecken in §§ 100g und 100h StPO geregelt. Das Gesetz sah eine Befristung dieser Befugnisse bis zum 31. Dezember 2007 vor.

Da diese Befugnisse der Strafverfolgungsbehörden stark in die Rechte der Betroffenen eingreifen, war es umstritten, ob und mit welchem Inhalt sie verlängert werden sollten. Vor diesem Hintergrund hatte der Bundestag die Bundesregierung im Jahr 2004 aufgefordert, einen Erfahrungsbericht über die praktische Umsetzung der §§ 100g, h StPO vorzulegen und dabei den Anlass, die Ergebnisse und die Anzahl der Betroffenen der Maßnahmen zu berücksichtigen. Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg wurde vom Bundesministerium der Justiz beauftragt, ein entsprechendes Gutachten über die „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ zu erstellen. Dieses Gutachten wurde durch das Bundesjustizministerium im Februar 2008 veröffentlicht (BT-Drs. 16/8434).

Der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz sahen es als nötig an, diese Studie und das zwischenzeitlich (am 1. Januar 2008) in Kraft getretene Gesetz zur Neuregelung der Telekommunikation und anderer verdeckter Ermittlungsmaßnahmen selbst einheitlich zu bewerten. Deshalb bildeten sie eine entsprechende Arbeitsgruppe, an der die Datenschutzbeauftragten der Länder Rheinland-Pfalz, Berlin, Schleswig-Holstein und Bayern sowie der Bundesbeauftragte teilgenommen haben. Als Ergebnis wurde in der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008 eine Entschließung zu der Abfrage von Telekommunikationsverkehrsdaten verabschiedet, in der die aus Datenschutzsicht bestehenden Bedenken gegen die Eignung und Verhältnismäßigkeit der gesetzlichen Befugnisse und ihrer Nutzung in der Praxis dargelegt wurden.

Auszug aus der Entschließung:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.
- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.
- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der Strafprozessordnung vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z.B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.
- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.
- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 Prozent der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen – trotz hoher Belastungen in der Praxis – unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können.

Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=076_tkverkehrsdat

11.2 Zivilrecht

11.2.1 Internet-Veröffentlichung von Wertgutachten im Zwangsversteigerungsverfahren

Eine in Schleswig-Holstein ansässige Firma betreibt ein Internet-Angebot als „Dienstleister für Amtsgerichte“ und veröffentlicht dort Zwangsversteigerungstermine mit den dazugehörigen Wertgutachten für Gebäude und Grundstücke. Nach der im Internet zugänglichen Liste nutzen derzeit 19 rheinland-pfälzische Amtsgerichte diesen Service. Viele Bürger haben das Verfahren wegen der frei für jedermann zugänglichen Einsichtmöglichkeit in die persönlichen Daten der Betroffenen (insbesondere auch in die Daten und Bilder, die in den Wertgutachten enthalten sind) beanstandet. Der LfD hat das Ministerium der Justiz um eine Stellungnahme zu dem Sachverhalt gebeten. Dieses ist der Auffassung, dass es für solche Veröffentlichungen keiner landesrechtlichen Bestimmung bedarf, da die Einstellung von Wertgutachten in das Internet im Rahmen von Zwangsversteigerungsverfahren entweder nach § 38 Abs. 2 ZVG oder nach § 40 Abs. 2 ZVG zulässig sei. Auch werde in der Veröffentlichung eines Wertgutachtens keine Beeinträchtigung datenschutzrechtlicher Vorschriften gesehen, da keine personenbezogenen Daten genannt würden.

Der LfD ist anderer Auffassung. Bei den im Internet veröffentlichten Informationen handelt es sich nach seiner Auffassung um personenbezogene Daten im Sinne des Datenschutzrechts. Zwar werden weder Name noch Anschrift des Schuldners und Eigentümers des betroffenen Grundstücks genannt, die vorhandenen Angaben (Flurstück, Straße, Hausnummer, Bilder) sind aber so genau, dass für einen beliebig großen Personenkreis durch einfach zu erlangende Zusatzinformationen Bewohner und Eigentümer der Liegenschaften ermittelt werden können. Da weder die §§ 39, 40 noch § 42 Abs. 2 ZVG eine Ermächtigungsgrundlage für die Veröffentlichung von Wertgutachten im Internet darstellen, bedarf es zwingend einer landesrechtlichen Bestimmung hierzu. Denn nach § 38 Abs. 2 ZVG ist die Einstellung eines Wertgutachtens in das Internet nur gestattet, wenn das elektronische Informationssystem landesrechtlich für das Gericht bestimmt ist. An einer solchen Regelung fehlt es. Die Erörterungen mit dem Justizministerium des Landes zu diesem Thema sind noch nicht abgeschlossen.

11.2.2 Elektronische Insolvenzbekanntmachungen

Der LfD hat bereits im 21. Tätigkeitsbericht ausführlich die aus datenschutzrechtlicher Sicht bestehenden Bedenken gegen die gesetzlichen Voraussetzungen für die insolvenzrechtlichen Bekanntmachungen im Internet dargestellt. Die öffentlichen Bekanntmachungen werden zentral und länderübergreifend im Internet bereit gestellt (§ 9 InsO). Ursprünglich gab es eine Regelung, wonach technisch zu verhindern war, dass Kopien von solchen Internet-Bekanntmachungen gefertigt werden konnten (§ 9 Abs. 2 Satz 3 Nr. 3 InsO). Diese Regelung ist mit Wirkung zum 1. Juli 2007 entfallen, weil es technisch sichere Vorkehrungen gegen solche Kopiermöglichkeiten nicht gibt. Zum Schutz der Persönlichkeitsrechte der Insolvenzschuldner wäre es aber aus Sicht des LfD notwendig, gesetzlich klarzustellen, dass eine Verbreitung der Insolvenzdaten durch Dritte verboten ist (s. 21. Tb., Tz. 7.3.2.). Eine solche Klarstellung fehlt nach wie vor.

Durch Eingabe eines Petenten wurde die Frage aufgeworfen, wann entsprechende Eintragungen zu löschen sind. Nach § 3 der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet vom 12 Februar 2002 sind die Veröffentlichungen zu einem Verfahren spätestens sechs Monate nach der Aufhebung oder der Rechtskraft der Einstellung des Insolvenzverfahrens zu löschen. Der Petent hatte ein nachvollziehbares Interesse an einer früheren Löschung dargelegt.

Das mit der Frage befasste Justizministerium vertritt trotz des insoweit offenen Wortlauts („spätestens“ nach sechs Monaten ist zu löschen) die Auffassung, dass es sich um eine feststehende nicht abkürzbare Frist handele. Auch würden – mit einer Ausnahme – alle Amtsgerichte dies in der Praxis so handhaben. Eine solche Interpretation hält der LfD aufgrund des berechtigten Interesses des Schuldners an einer alsbaldigen Löschung aber für problematisch.

11.3 Strafvollzug

11.3.1 Videoüberwachung im Strafvollzug

Auch im Bereich der Justizvollzugsanstalten ist die Videoüberwachung allgegenwärtig. Mit Ausnahme der „normalen“ Haftzellen werden fast alle anderen Bereiche videoüberwacht. Dies beginnt bei den Besucherräumen und reicht über die besonders gesicherten Hafträume und die

gesondert ausgewiesenen und ausgestatteten Überwachungshafträume bis zu den Außenanlagen.

Datenschutzrechtlich brisant ist die Videoüberwachung in den besonders gesicherten Hafträumen. Sie erfolgt hier „rund um die Uhr“ und erfasst jeden Winkel, auch den Toilettenbereich. Außerdem beschränkte sich die Videoüberwachung in der Regel nicht auf ein bloßes Monitoring, sondern schloss die Aufzeichnung des gewonnenen Materials ein. Ähnlich war die Situation in den gesondert ausgewiesenen und ausgestatteten Überwachungshafträumen. Der LfD hat gegenüber dem Ministerium der Justiz bezweifelt, dass eine solche Aufzeichnung notwendig ist. Im Übrigen hat er darauf hingewiesen, dass es durch die Totalüberwachung zu einer massiven Beeinträchtigung des Schamgefühls der Betroffenen kommt. Diese Überwachungspraxis berühre den absolut geschützten Kernbereich des allgemeinen Persönlichkeitsrechts der betroffenen Gefangenen. Das Ministerium der Justiz hat daraufhin mitgeteilt, dass die Videoüberwachung in der Zukunft auf das reine Monitoring beschränkt werde. Auf dieses könne allerdings nicht verzichtet werden, es ließe sich auch nicht räumlich begrenzen. Eine Verletzung des Schamgefühls der Betroffenen könne deshalb nicht verhindert werden.

Der LfD hat darüber hinaus deutlich gemacht, dass es für eine mit einer Aufzeichnung verbundene Videoüberwachung der Besuchsräume keine hinreichende gesetzliche Grundlage gebe. Auch in diesen Bereichen soll nach Zusage des Ministeriums die Videoüberwachung auf das reine Monitoring beschränken und im Übrigen darauf geachtet werden, dass entsprechende Hinweisschilder angebracht würden.

Lückenlos ist die Videoüberwachung der Außenbereiche. Allerdings ist auch diese unterschiedlich ausgestaltet. Teilweise erfolgt eine Speicherung der Aufzeichnung nur im Alarmfall, teilweise ständig. Aufgrund der dazu erhobenen Bedenken des LfD hat das Ministerium erklärt, künftig einheitlich nur noch im Alarmierungsfall Aufzeichnungen zu fertigen.

Schließlich hat der LfD auch darauf hingewiesen, dass der Einsatz sog. DOME-Kameras und schwenkbarer Kameras nicht dazu führen dürfe, dass Einblick in benachbarte Privatwohnungen und -häuser erfolge. Nach dem Landesdatenschutzgesetz sei dies durch entsprechende technische und organisatorische Vorkehrungen auszuschließen. Die Einsichtnahme in private Wohnungen und -häuser sei deshalb auszublenden bzw. zu verdecken. Soweit dies nicht möglich sei, seien die Kameras zu arretieren, so dass ein Schwenk zu diesen Wohnungen ausgeschlossen sei. Das Ministerium sagte dies zu.

Außerdem soll die Speicherdauer der im Alarmfall gewonnenen Daten im Rahmen einer Dienstanweisung einheitlich geregelt werden. Über die Frist besteht noch kein Einvernehmen.

Der LfD wird zeitnah gemeinsam mit dem Ministerium der Justiz eine Orientierungshilfe für die Videoüberwachung im Strafvollzug erarbeiten.

11.3.2 Eingaben Strafgefangener

Nach wie vor stellen sich im Strafvollzug eine ganze Anzahl datenschutzrechtlich relevanter Fragen. Mehrfach haben Strafgefangene gegenüber dem LfD den Umgang mit ihren persönlichen Daten gerügt. U.a. hatte sich der LfD mit folgenden Anliegen zu befassen: Da in der Regel mehrere Besucher von Gefangenen an der Einlasspforte eintreffen würden, führe das namentliche Ausrufen der Gefangenen durch die Bediensteten der JVA zu einem Datenschutzverstoß. Die Besucher würden auf diese Weise erfahren, wer sich in der JVA aufhalte. Auf eine entsprechende Intervention des LfD wurde sichergestellt, dass bei der Besucheranmeldung künftig die notwendige Diskretion gewahrt wird. Der LfD begrüßt es, dass in der entsprechenden JVA vor der Sprechanlage an der Besucherpforte eine ca. zwei bis drei Quadratmeter große Fläche mit einem Hinweisschild „Diskretion bitte Abstand halten“ angebracht wurde.

Andere Eingaben befassten sich mit der Überwachung von Telefongesprächen mit Verteidigern, der Öffnung von Verteidigerpost und dergleichen. In diesen Fällen haben sich die datenschutzrechtlichen Bedenken der Petenten in aller Regel nicht bestätigt. Aufgrund der gehäuften Eingaben hinsichtlich des Mithörens von Verteidigertelefonaten und der Kenntnisnahmemöglichkeit von persönlichen Daten anderer Gefangener in Beamtenbüros hat sich der LfD zudem selbst vor Ort von der tatsächlichen Situation ein Bild gemacht. Er hat sich vergewissert, dass die technische Möglichkeit besteht, dass ein Mithören bei Telefongesprächen mit Verteidigern ausgeschlossen werden kann. Es ist durch entsprechende Dienstanweisungen vorgeschrieben, dass diese Einrichtungen auch entsprechend genutzt werden. Eine absolute Sicherheit, dass in der Praxis in allen Fällen auch so verfahren wird, kann es allerdings nicht geben.

11.4 Bundeszentralregister

Im Zusammenhang mit dem Untersuchungsausschuss „Nürburgring“ entwickelte sich eine Debatte über die Voraussetzungen, unter denen eine oberste Landesbehörde eine unbeschränkte Auskunft aus dem Bundeszentral-

register einholen kann. Der LfD war von der Landesregierung mit Blick auf eine unmittelbar bevorstehende Plenarsitzung um eine kurzfristige datenschutzrechtliche Stellungnahme gebeten worden. In dieser Stellungnahme vertrat er die Auffassung, dass eine solche Auskunft nach Maßgabe des § 12 Abs. 4 LDSG und einer verfassungskonformen Auslegung von § 41 BZRG nur bei einem überwiegenden öffentlichen Interesse zulässig sei. Maßstab sei die besondere Sensibilität der betroffenen Daten, so dass nur ein solches öffentliches Interesse überwiege, das dem Schutz wichtiger Gemeinschaftsgüter diene. Demgegenüber wurde seitens der Oppositionsfraktionen die Auffassung vertreten, dass dem § 41 BZRG entsprechende Einschränkungen nicht zu entnehmen seien.

Die Debatte, die sich Anfang 2010 fortsetzte, ist noch nicht abgeschlossen. Der LfD hat eine Umfrage bei den Datenschutzbeauftragten des Bundes und der Länder zu dieser Thematik durchgeführt. Die Antworten liegen noch nicht alle vor.

12. Finanzen

12.1 Steueridentifikationsnummer

Im Berichtszeitraum wurde allen Bürgern ihre persönliche Steueridentifikationssummer zugesandt. Bei der Versendung gab es in Rheinland-Pfalz keine datenschutzrechtlichen Probleme. Allerdings bleibt diese einheitliche Nummer ein Dorn im Auge der Datenschützer. Diese hatten bereits im Frühjahr 2008 (Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008) vor deren Gefahren gewarnt. Die einheitliche Nummer, einmal in der Welt, würde schnell Begehrlichkeiten wecken, um Personen auch außerhalb der Finanzverwaltung schnell und unkompliziert identifizieren zu können. Die Karriere zum allgemeinen Personenkennzeichen sei vorprogrammiert. Gerade ein solches hält aber das Bundesverfassungsgericht in seinem Volkszählungsurteil (BVerfGE 65, 1) für unzulässig.

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Berlin, 4. April 2008

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z.B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

Der LfD hatte sich bereits mit einem entsprechenden Anliegen zu befassen: So wollte eine Stadtverwaltung die Steueridentifikationsnummer bei Gewährung von Hartz IV oder Arbeitslosengeld als Controlling-Maßnahme nutzen. Die Nutzung ist abschließend in § 139b AO geregelt. Gemäß Abs. 2 Satz 2 dieser Vorschrift dürfen andere öffentliche Stellen als die Finanzbehörden die Identifikationsnummer nur erheben oder verwenden, soweit dies für Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist oder eine Rechtsvorschrift die Erhebung oder Verwendung der Identifikationsnummer ausdrücklich erlaubt oder anordnet. Weiterhin dürfen ihre Dateien nur insoweit nach der Identifikationsnummer geordnet oder für den Zugriff erschlossen werden, als dies für regelmäßige Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist. Vertragsbestimmungen und Einwilligungserklärungen, die darauf gerichtet sind, eine nach den vorstehenden Bestimmungen nicht zulässige Erhebung oder Verwendung der Identifikationsnummer zu ermöglichen, sind unwirksam.

Das geplante Verfahren unter Nutzung der Steueridentifikationsnummer war, auch auf Grundlage einer Einwilligung der Betroffenen, aus datenschutzrechtlicher Sicht unzulässig.

12.2 Auskunftsrecht gegenüber der Finanzverwaltung

Grundsätzlich hat jeder Bürger Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Dieser Anspruch ist sowohl im Landesdatenschutzgesetz als auch im Bundesdatenschutzgesetz normiert. Er richtet sich sowohl an die Verwaltung als auch an private Datenverarbeiter – und auch an die Steuerverwaltung, auch wenn dies dort gerne einmal anders gesehen wird. Das hat das Bundesverfassungsgericht in seinem Beschluss vom 10. März 2008 (1 BvR 2388/03) bestätigt. Das Bundesfinanzministerium hat aufgrund dieser Entscheidung im Dezember 2008 ein Schreiben (AZ: IV A 3 – S 0030/08/10001) verfasst, in dem die näheren Voraussetzungen der Auskunftsrechte der Steuerpflichtigen geregelt sind und das für alle Finanzverwaltungen bindend ist. Darin wird als Voraussetzung genannt, dass der Betroffene ein berechtigtes Interesse geltend machen muss. Damit wird der Auskunftsanspruch nur eingeschränkt gewährt. Die Finanzverwaltung befürchtet andernfalls, dass das Geheimhaltungsinteresse des Staates, welches auch vom Bundesverfassungsgericht anerkannt wird, nicht gewährleistet werden kann. Die Regelungen im Landes- und im Bundesdatenschutzgesetz begründen aber ausdrücklich einen Auskunftsanspruch, ohne dass die Betroffenen ein berechtigtes Interesse darlegen müssten. Der Gesetzgeber bringt vielmehr zum Ausdruck, dass jedermann stets ein berechtigtes Interesse an der Auskunft hat. Er muss es gerade nicht mehr begründen. Die auskunftspflichtige Behörde hat nur zu prüfen, ob Ausnahmetatbestände vorliegen. Denn unter bestimmten Voraussetzungen, z.B. bei Geheimhaltungsinteressen des Staates, kann die Auskunft unterbleiben. Gerade wegen dieser Ausnahmetatbestände hat das Bundesverfassungsgericht auch die Regelungen zur Auskunftserteilung nach dem allgemeinen Datenschutzrecht für anwendbar gehalten. Denn hierdurch wird die ordnungsgemäße Aufgabenerfüllung der auskunftspflichtigen Stelle sichergestellt. Die Prüfung eines berechtigten Interesses bürdet der Gesetzgeber der verantwortlichen Stelle dagegen nicht auf, sie ist dazu auch nicht ermächtigt. Diese Wertung hat er bereits im Gesetz selbst vorgenommen. Folglich kann hier aus Sicht des LfD das Vortragen eines berechtigten Interesses auch den Prüfungsvorgang nicht beschleunigen.

Aus diesem Grunde steht auch das Schreiben des Bundesministeriums der Finanzen aus Sicht des LfD nicht im Einklang mit dem Gesetz: Mit der Statuierung einer Darlegungspflicht des Betroffenen stellt es das verfassungsrechtlich ausgestaltete Verhältnis von Staat und Bürger auf den Kopf.

Um Missverständnissen vorzubeugen: Ein schrankenloses Auskunftsrecht wird auch vom LfD nicht gefordert, insbesondere im Hinblick auf die besondere Aufgabenstellung der Finanzverwaltung. Der LfD hält es aber nach wie vor für nicht gesetzeskonform, von den Beteiligten die Darlegung eines berechtigten Interesses zu fordern.

Der LfD hat daher das hiesige Finanzministerium aufgefordert, sich im Sinne der Rechtmäßigkeit der Verwaltung um eine alsbaldige Korrektur der im Schreiben des Bundesministeriums der Finanzen vom 17. Dezember 2008 vertretenen Rechtsauffassung zu bemühen. Dies lehnt das Finanzministerium ab.

Dies wird von allen Landes- und dem Bundesdatenschutzbeauftragten so gesehen (vgl. Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009 „Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewähr-

leisten!“). Der Bundesdatenschutzbeauftragte hat das Schreiben des Bundesfinanzministeriums mittlerweile förmlich beanstandetet.

Fazit:
Das Bundesverfassungsgericht hat den Auskunftsanspruch des Steuerpflichtigen nach geltenden datenschutzrechtlichen Bestimmungen bekräftigt. Die Finanzverwaltung will diesen Anspruch nur bei Vorliegen eines berechtigten Interesses prüfen, obwohl das Gesetz eine solche Einschränkung nicht vorsieht. Die Datenschutzbeauftragten des Bundes und der Länder nutzen die ihnen zur Verfügung stehenden Mittel, um eine Korrektur der Rechtauffassung des Bundesfinanzministeriums zu erreichen.

13. Technisch-organisatorischer Datenschutz

13.1 Kontrollen und Beratungen

Kontrolle und Beratung bilden neben der Bearbeitung von Eingaben die Schwerpunkte der Arbeit des LfD auch im technischen Bereich. Im Berichtszeitraum sind in diesem Zusammenhang in insgesamt 70 Fällen Kontrollen und Beratungen vor Ort erfolgt, u.a. bei folgenden Stellen:

- Polizeipräsidien,
- Landeskriminalamt,
- Justizvollzugsanstalt,
- Hochschulen,
- Universitätsklinik,
- Krankenhäuser,
- Ministerien,
- Kassenärztliche Vereinigung,
- Gesundheitsämter,
- Verkehrsunternehmen,
- Internet-Portalanbieter,
- Callcenter,
- Unternehmen der Werbewirtschaft,
- Wohnungsbauunternehmen,
- Adresshandelsunternehmen,
- Wirtschaftsauskunftei,
- Sparkasse,
- Sportverein.

Ergänzt wurden diese durch 13 Informationsbesuche, bei denen die Klärung des technischen Verfahrensstands im Vordergrund stand. Kontrollen erfolgten überwiegend anlassbezogen, z.B. aufgrund von Eingaben an den LfD oder aktueller technischer Fragestellungen. Die Durchführung anlassloser Kontrollen oder allgemeiner Prüfungen der IT-gestützten Verarbeitung personenbezogener Daten wurde aufgrund der bestehenden personellen Engpässe reduziert.

Der Anteil der Online-Kontrollen, d.h. die Prüfung von Internet-Angeboten bzw. online nutzbarer Verfahren wurde intensiviert und hat sich als zunehmend bedeutsamer Bereich der Kontrolltätigkeit des LfD erwiesen (s.a. Tz. 13.6)

Mit der Übernahme der Datenschutzaufsicht auch im nicht-öffentlichen Bereich ab Oktober 2008 haben Kontrolle und Beratung in diesem Bereich sowie der gestiegene Umfang von Eingaben die personellen Ressourcen des LfD im Technikbereich überwiegend in Anspruch genommen. Eine im Rahmen der Aufgabenerweiterung vorgesehene weitere Technikerstelle war zunächst mit einer Besetzungssperre versehen und wurde dem Haushalt des LfD erst Mitte 2009 zugewiesen. Die Gewinnung qualifizierten Personals hat sich, u.a. aufgrund einer abgesenkten Dotierung, als schwierig erwiesen; im Berichtszeitraum konnte die Stelle zunächst nicht besetzt werden.

Die Praxis der Verwaltung, den LfD im Vorfeld geplanter Umstrukturierungen des IT-Einsatzes oder bei der Erstellung von Datenschutz- und Sicherheitskonzepten zu beteiligen, hat sich fortgesetzt. Insbesondere bei der Einführung zentraler Verfahren wird in der Regel frühzeitig die Abstimmung mit dem LfD gesucht. Im Bereich der Wirtschaft ist dies bislang nur ansatzweise der Fall.

Schulungsaktivitäten und Vortragstätigkeit wurden im bisherigen Umfang fortgeführt. Entsprechenden Nachfragen aus dem nicht-öffentlichen Bereich konnte angesichts der knappen Personalressourcen nur bedingt entsprochen werden. Der LfD beabsichtigt, dem hier erkennbaren Bedarf mit einer Ausweitung seines Angebots zum Selbstdatenschutz Rechnung zu tragen.

13.2 Entwicklung der Informationstechnik

Der Einsatz der Informationstechnik erfasst im beruflichen, wirtschaftlichen und privaten Umfeld immer weitere Lebensbereiche. Damit einher geht eine zunehmende Erhebung, Verarbeitung und Verknüpfung personenbezogener Daten, bei der Fragen des Datenschutzes immer bedeutsamer werden.

Um neuen, sich im Zusammenhang mit der informationstechnischen Entwicklung ergebenden Datenschutzfragen angemessen begegnen zu können, hat die Konferenz der Datenschutzbeauftragten den Arbeitskreis Technik gebeten, in regelmäßigen Abständen darüber zu berichten, welche Entwicklungen in absehbarer Zeit in der Praxis Bedeutung erlangen können und besonderen Datenschutzbezug haben werden.

Neben den weiterhin zu verzeichnenden Trends zur Leistungssteigerung, Miniaturisierung und Vernetzung sind danach u.a. folgende Entwicklungen von Bedeutung:

13.2.1 Konvergenz der Netze

Die Konvergenz von Techniken und Netzen im Bereich Telekommunikation und Mediennutzung (z.B. Konvergenz von Sprach- und Datennetzen, Triple Play). Neben den spezifischen Risiken, die von den einzelnen Diensten ausgehen, sind Wechselwirkungen und Kumulationseffekte zu befürchten.

13.2.2 Biometrie

Biometrische Verfahren kommen außer in flächendeckenden Großverfahren wie in Ausweisdokumenten (elektronischer Reisepass, elektronischer Personalausweis) auch in vergleichbar trivialen Anwendungen wie dem Bezahlen per Fingerabdruck im Supermarkt zum Einsatz. Bei der Speicherung und Verarbeitung biometrischer Daten stellen sich zahlreiche Datenschutzfragen. So ist nach der Zuverlässigkeit bei der Erzeugung der Referenzdaten (Enrolment) sowie der Wiedererkennung (Parameter wie Falschakzeptanzrate und Falschrückweisungsrate) und nach der Langzeitstabilität zu fragen. Von Bedeutung ist auch, ob biometrische Daten fälschungssicher und vertraulich gespeichert werden und wer darauf zugreifen kann (s.a. Tz. 7.8 und Tz. 13.9).

13.2.3 Standortbezogene Dienste (Location Based Services)

Standortbezogene Dienste sind über ein Netzwerk erbrachte mobile Dienste, die positions- und ggf. zeit- oder personenabhängig sind wie Routenplaner, Restaurant-Finder oder Positionsbestimmungen des eigenen oder eines fremden Mobiltelefons. Dienste dieser Art können zu umfangreichen Bewegungsprofilen führen, die mit weiteren Daten über Tätigkeiten, Beziehungen oder Vorlieben des Benutzers angereichert sind. Standortbezogene Dienste können als Vorstufe des Ubiquitous Computing angesehen werden.

13.2.4 Cloud Computing

Mit dem Schlagwort „Cloud Computing“ wird eine Entwicklung benannt, bei der IT-Leistungen je nach Bedarf von unterschiedlichen Anbietern über das Internet aus der „IT-Wolke“ bezogen werden. Bei entsprechenden Geschäftsmodellen stellen Anbieter ihren Kunden IT-Dienstleistungen zur Verfügung, die nach Nutzung abgerechnet werden („IT aus der Steckdose“). Die Bandbreite reicht dabei vom Bezug reiner Technikleistungen (Serverleistung, Bandbreite, Speicherplatz usw.) bis hin zur Verlagerung ganzer Anwendungen einschließlich der Datenhaltung in die „IT-Wolke“. Das Geschäftsmodell ist zumindest in einigen Bereichen bereits etabliert. Künftig wird mit einer höheren Marktdurchdringung zu rechnen sein. Die Aufteilung der Informationstechnik in einzelne Dienste und deren Verlagerung aus der jeweiligen Organisation heraus zu (unterschiedlichen) Anbietern reduziert den faktischen Einfluss der datenverarbeitenden Stelle und birgt Risiken hinsichtlich der Kontrollierbarkeit und des Zugriffs auf personenbezogene Daten.

13.2.5 Serviceorientierte Architekturen (SOA)

Die serviceorientierte Architektur beruht auf der bedarfsweisen Kopplung wiederverwendbarer Softwarebausteine (Services). Anwendungen lassen sich dadurch an geänderte Anforderungen leichter und schneller anpassen. Der Nutzer solcher Dienste weiß lediglich, dass ein Dienst angeboten wird, welche Eingaben er erfordert und welcher Art das Ergebnis ist. Details über die Art und Weise der Ergebnisermittlung müssen zumindest aus technischer Sicht nicht bekannt sein. Diese neue Form der Datenverarbeitung sorgt für völlig neue Herausforderungen an IT-Sicherheit und Datenschutz. Systeme, die bisher in der eigenen IT-Infrastruktur angesiedelt waren, werden nun über das Internet mit fremden Systemen und Diensten verbunden, die außerhalb der eigenen Kontrolle stehen. Oft ist unklar, wieweit man einem fremden System vertrauen kann. Aber auch eine Reihe datenschutzrechtlicher Fragen sind klärungsbedürftig. Wie kann beispielsweise sichergestellt werden, dass personenbezogene Daten, die den eigenen Herrschaftsbereich verlassen, nicht bei der Nutzung eines externen SOA-Dienstes zweckentfremdet verwendet werden? Wer ist für die Datenverarbeitung durch einen solchen Dienst verantwortlich? Sind derartige Dienste ausreichend revisionsfähig?

13.2.6 Ubiquitous Computing, RFID

Ubiquitous Computing bezeichnet die Allgegenwärtigkeit von Informationsverarbeitung im Alltag in unterschiedlichsten Lebensbereichen. Computer werden in die Umgebung eingebettet und bilden ein mobiles Netz, dessen Teile sich u.U. ändern können und das sich selbst organisiert bzw. konfiguriert.

Hierzu zählt beispielsweise die RFID-Technologie oder der kontaktlose Informationsaustausch mittels Nahfeldkommunikation (NFC), etwa zwischen zwei Mobiltelefonen oder zwischen Mobiltelefonen und Terminals verschiedenster Ausprägungen. Bei der ubiquitären Informationsverarbeitung lässt sich immer schwerer eine verantwortliche datenverarbeitende Stelle festlegen bzw. ermitteln. Auch der Begriff der Datenübermittlung passt innerhalb einer solchen IT-Umgebung nur noch bedingt. Weiterhin können je nach Gestaltung auch hier unterschiedliche und gegebenenfalls sensible Lebensgewohnheiten durch Profilbildung ermittelt werden (s.a. Tz. 6.1.1).

13.2.7 Konsequenzen

Angesichts der vielfältigen Möglichkeiten zur Vernetzung und der allgegenwärtigen Datenverarbeitung sind ggf. der Begriff und die Rolle der datenverarbeitenden bzw. verantwortlichen Stelle zu überdenken. Wenn es künftig mög-

lich sein wird, dass datenverarbeitende Systeme sich selbständig organisieren und konfigurieren, unaufgefordert Daten erfassen und untereinander austauschen, wird die traditionelle Definition der verarbeitende Stelle allein u.U. nicht mehr zielführend sein. Auch das Konzept der Einwilligung muss angesichts der zunehmend unsichtbarer werdenden Datenverarbeitung und der schwindenden Transparenz ggf. überdacht werden. Das Bundesverfassungsgericht hat im Volkszählungsurteil als Voraussetzung für die informationelle Selbstbestimmung gefordert, dass Betroffene in der Lage sein müssen sich zu informieren, wer was wann und bei welcher Gelegenheit über sie weiß. Transparenz ist unabdingbare Voraussetzung, um eigene Rechte in Anspruch nehmen zu können. Ob diese Forderung in der modernen Informationsgesellschaft und im Zeitalter des Ubiquitous Computing noch vollständig umsetzbar ist, ist zweifelhaft.

Die Datenschutzfreundlichkeit technischer Entwicklungen ist daher künftig auch daran zu messen, ob das neu abgeleitete Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme in angemessener Weise umgesetzt wurde. Eine Schwerpunktaufgabe der Datenschutzbeauftragten von Bund und Ländern im Technikbereich wird es sein, hier zu beraten und die Umsetzung der in diesem Grundrecht formulierten Anforderungen in technischen Verfahren zu verfolgen. Darüber hinaus wird es in Zukunft bedeutsamer werden, nicht nur Einzelprojekte und Verfahren zu begleiten und dort jeweils auf datenschutzfreundlichen Einsatz der Technik zu achten. Vielmehr sind übergreifende Datenschutzbetrachtungen erforderlich und es müssen einzelne Verfahren im Zusammenhang betrachtet werden.

Eine zentrale Forderung der Datenschutzbeauftragten muss deshalb darauf abzielen, die Nutzung elektronischer Verfahren künftig weitgehend anonym oder zumindest pseudonym zu ermöglichen. Die Vermeidung des direkten Personenbezugs muss für neue technische Entwicklungen zu einem grundlegenden Gestaltungsprinzip werden.

Datenschutzfördernde Technik wird jedoch nur dann die Akzeptanz der Betroffenen finden, wenn sie für die Risiken der modernen elektronischen Datenverarbeitung sensibilisiert sind und wenn sie transparente, leicht bedienbare Verfahren etwa zum Identitätsmanagement nutzen können. Deshalb wird es eine zunehmend wichtige Aufgabe der Datenschutzbeauftragten sein, die Betroffenen über die Risiken der modernen Informationsgesellschaft zu informieren und sie mit vorhandenen technischen Möglichkeiten zum Schutz der Privatshäre vertraut zu machen (Stichwort: Selbstdatenschutz).

13.3 Modernisierung der Technikregelungen der Datenschutzgesetze

Das geltende Datenschutzrecht folgt hinsichtlich der Regelungen zum technisch-organisatorischen Datenschutz in weiten Teilen einem Konzept, das sich an den Gegebenheiten zentraler Großrechner orientiert. Das Landesdatenschutzgesetz bildet hierbei keine Ausnahme. Die Regelungen in § 9 LDSG stammen im Kern aus den 1970er Jahren und bilden die Anforderungen, die an heutige IT-Szenarien zu stellen sind, nur unzureichend ab. Sie fußen auf homogenen, zentralen, einheitlich organisierten und von einer Stelle betriebenen IT-Strukturen, einer Situation, wie sie vielfach nicht mehr anzutreffen ist. Heutige IT-Lösungen sind oftmals durch ausgeprägt dezentrale Strukturen, einen hohen Vernetzungsgrad, verteilte Anwendungen und Verantwortlichkeiten und unterschiedliche Betreiber gekennzeichnet (Internet-Portale, Online-Shops, RFID-Anwendungen, ortsbezogene Dienste etc.). Mit den vorhandenen technisch-organisatorischen Regelungen kann dem nur unzureichend entsprochen werden.

Ein Novellierungsbedarf wurde für diesen Bereich schon im seinerzeitigen Gutachten des Bundesinnenministeriums zur Modernisierung des Datenschutzes (Garstka/Roßnagel/Pfitzmann, 2001) formuliert. Die damaligen Vorschläge gingen dahin, die Sicherheitsziele der Systematik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auch zur Grundlage der technischen Datenschutzanforderungen zu machen und sie um datenschutzspezifische Anforderungen zu erweitern. Einige Bundesländer sind dem gefolgt und haben ihre Datenschutzgesetze entsprechend geändert (Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Sachsen, Thüringen); andere sowie der Bund sind im Kern bei den bisherigen Regelungen geblieben. Die ursprüngliche Einheitlichkeit der Technikregelungen ging dabei verloren. Anstoß für aktuelle Novellierungsüberlegungen gab u.a. das Urteil des Bundesverfassungsgerichts (Az. 1BvR 370/07, 1 BvR 595/07) zur Online-Durchsuchung, in dem im Zusammenhang mit der Formulierung eines neuen „Computergrundrechts“ die Sicherheitsziele „Vertraulichkeit“ und „Integrität“ aufgegriffen wurden (s.a. Tz. 2.2.1, Tz. 2.2.5, Tz. 6.2.2, Tz. 7.3). Auch in der parlamentarischen Diskussion wird die Notwendigkeit einer Novellierung der Technikregelungen gesehen. So bittet der Bundesrat in der BT-Drs. 16/12011 vom 18. Februar 2009 zu prüfen, ob die bisherigen Einzelmaßnahmen in der Anlage zu § 9 BDSG entfallen und stattdessen Sicherheits- bzw. Datenschutzziele eingeführt werden können.

Datenschutz ist mehr als IT-Sicherheit, auch bei den Technikregelungen. Es wäre falsch, ihn allein auf sicherheitstechnische Aspekte zu reduzieren. Es braucht IT-

Sicherheit, um Datenschutz zu gewährleisten, es braucht aber auch Datensparsamkeit, Datenvermeidung, Löschungsregelungen, Transparenz, Nachvollziehbarkeit und Vertrauenswürdigkeit der eingesetzten IT-Lösungen. Neben Verfügbarkeit, Vertraulichkeit und Integrität - den IT-Sicherheitszielen des BSI – sollten daher „Datenschutzziele“ wie Authentizität, Revisionsfähigkeit und Transparenz zu zentralen Datenschutzvorgaben für IT-Lösungen gemacht werden und die bisherigen „Kontrollarten“ des § 9 Abs. 2 LDSG ergänzen.

Eine von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingesetzte Arbeitsgruppe unter Beteiligung des LfD wurde beauftragt, Vorschläge für eine Novellierung und Vereinheitlichung des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze im Technikbereich zu erarbeiten.Grundlage sollte dabei die Definition elementarer, technologieunabhängiger Schutzziele sein, auf deren Basis sich ein Katalog von Datenschutzmaßnahmen ableiten lässt. Die Schutzziele sollten soweit möglich mit den elementaren BSI-Schutzzielen der IT-Sicherheit korrespondieren, zugleich aber die speziellen Sichtweisen des Datenschutzes widerspiegeln. So sollen grundlegende rechtliche Anforderungen wie Datenvermeidung und Datensparsamkeit, die Einhaltung der Zweckbindung, die Wahrnehmung von Betroffenenrechten in den Anforderungen an eine datenschutzgerechte technische Gestaltung von Verfahren ihren Niederschlag finden. Dies greift die Konzepte Systemdatenschutz und Datenschutz durch Technik auf.

Auf der Grundlage der Ergebnisse der Arbeitsgruppe wird gegenwärtig ein Musterentwurf für eine Technik-Norm der Datenschutzgesetze erarbeitet, der in die Diskussion um die Modernisierung des Datenschutzrechts insgesamt eingebracht werden soll. Zentrale Punkte sind neben den o.g. Aspekten die Sicherung der Zweckbindung, die Beherrschbarkeit von IT-Lösungen und die Erstellung eines verfahrensbezogenen Datenschutzkonzepts auf der Grundlage einer Schutzbedarfs- und Risikoanalyse.

Hinweis / Link

BT-Drs. 16/12011: „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“, Anlage 3: Stellungnahme des Bundesrates, hier Nr. 6 zu Artikel 2 (§ 9 und Anlage zu § 9 Satz 1 BDSG), http://dipbt.bundestag.de/dip21/btd/16/120/1612011.pdf

Datenschutzziele:

Vertraulichkeit:	Nur Befugte dürfen Daten zur Kenntnis nehmen.
Integrität:	Daten müssen während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und aktuell bleiben.
Verfügbarkeit:	Daten und Funktionen müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können.
Authentizität:	Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.
Revisionsfähigkeit:	Es muss feststellbar sein, wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat.
Transparenz:	Die Verfahren zur Erhebung, Verarbeitung und Nutzung müssen nachvollziehbar und aktuell dokumentiert sein.

13.4 IT-Sicherheit in der Landesverwaltung

In seinem 21. Tb. hatte der LfD unter Tz. 21.2.1 auf die Notwendigkeit hingewiesen, das Thema IT-Sicherheit in der Landesverwaltung aufzugreifen und die Umsetzung der im Rundschreiben „Planung und Realisierung der IT-Sicherheit in der Landesverwaltung Rheinland-Pfalz“ (MinBl. vom 4. Juni 2003, S. 327) genannten Punkte angemahnt.

Zwischenzeitlich wurde im Auftrag der Zentralstelle IT und Multimedia vom Landesbetrieb Daten und Information unter Beteiligung des LfD und verschiedener Ministerien eine „Informationsplattform IT-Sicherheit“ eingerichtet. Im rlp-Netz können seit dem 1. September 2009 unter http://www.it-sicherheit.rlp.de/ Informationen zur IT-Sicherheit an zentraler Stelle abgerufen werden. IT-Sicherheitsverantwortliche in der Landesverwaltung haben die Möglichkeit, sich in einem zugangsgeschützten Forum auszutauschen.

In Abstimmung mit den Ressorts ist eine kontinuierliche Weiterentwicklung dieser Plattform geplant. So soll gemäß einem Beschluss der Staatssekretäre vom 29. Januar 2007 als weiterer Schritt ein ressortübergreifendes Computer Emergency Response Team (CERT) aufgebaut werden, um durch die Beobachtung der Entwicklung im IT-Sicherheitsumfeld, die Verteilung von Informationen über Sicherheitsprobleme an die Landesverwaltung und die Durchführung vorbeugender Maßnahmen die IT-Sicherheit in der Landesverwaltung zu optimieren. Bei ressortübergreifenden Sicherheitsvorfällen soll das CERT Gegenmaßnahmen koordinieren.

Informationsplattform IT-Sicherheit-RLP im rlp-Netz:
http://www.it-sicherheit.rlp.de/

13.5 Urteil des Bundesverfassungsgerichts zu Wahlcomputern

Das Bundesverfassungsgericht hat in seinem Urteil vom 3. März 2009 (Az. 2 BvC 3/07 und 2 BvC 4/07) den Einsatz elektronischer Wahlgeräte, wie sie in der Vergangenheit auch in Rheinland-Pfalz eingesetzt wurden, für verfassungswidrig erklärt. Der Grundsatz der Öffentlichkeit der Wahl gebiete es, dass die wesentlichen Schritte der Wahlhandlung und der Ergebnismitteilung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.

Die Frage nach möglichen Auswirkungen auf die geplante elektronische Auswertung der Kommunalwahl am 7. Juni 2009 wurde auch an den LfD herangetragen.

Beim eingesetzten Verfahren wurde nach Abschluss der Wahlhandlung durch die jeweiligen Wahlvorstände im Rahmen der Ergebnisermittlung jede Stimmabgabe von den Stimmzetteln in die Auswertungssoftware übertragen. Die Software führte automatisiert eine ggf. erforderliche Bereinigung der Stimmabgabe nach den Vorschriften des Kommunalwahlrechts durch. Das Ergebnis der Heilung wurde entsprechend dargestellt und konnte durch den Wahlvorstand sowie Zuschauer eingesehen und überprüft werden. Die bereinigte Stimmabgabe wurde dann automatisiert aufsummiert. Entsprechend den Vorgaben des Landeswahlleiters und des LfD wurden nach einer festgelegten Anzahl von Erfassungen die Summenbildung sowie die Heilung überprüft.

Eine gänzlich automatisierte und nicht nachprüfbare Auswertung der Stimmabgabe erfolgte somit nicht. Eine Situation wie im Falle der Bundesverfassungsgerichtsentscheidung bestand somit nicht.

Ergänzend hat der LfD insbesondere überprüft, ob innerhalb des Auswertungsverfahrens geeignete Maßnahmen enthalten sind, um die unbefugte oder unbemerkte Veränderung der Einzelergebnisse der Stimmbezirke auszuschließen. Als Ergebnis konnte festgestellt werden, dass durch entsprechende Algorithmen innerhalb des Verfahrens Checksummen gebildet wurden, die in den jeweiligen Ergebnisniederschriften vermerkt wurden. Bei der Zusammenführung der Einzelergebnisse wurden sodann die Checksummen der Niederschrift gegen die Referenzdaten der erfassten Stimmzettel geprüft. Eine nachträgliche Veränderung der Ergebnisdaten wäre somit erkannt worden.

13.6 Mangelnde Sicherheit bei Versandapotheken

Die in Rheinland-Pfalz ansässigen Versandapotheken wiesen nach den Ergebnissen einer Kontrolle des LfD erhebliche Sicherheitsdefizite bei ihren Online-Zugängen auf. Bei nahezu allen geprüften Versandapotheken war der Einsatz von Passwörtern mangelhaft, Vorkehrungen gegen missbräuchliche Anmeldeversuche unzureichend oder nicht vorhanden und daraus folgend der Online-Zugriff nicht sicher. Bei probeweisen Anmeldeversuchen des LfD konnte in mehreren Fällen auf Kundendaten zugegriffen werden. Bei kaum einer der geprüften Apotheken waren vorhandene Empfehlungen zur sicheren Gestaltung von Online-Zugängen, z.B. des Bundesamtes für Sicherheit in der Informationstechnik, berücksichtigt worden. Nach Ansicht des LfD ist davon auszugehen, dass den Betreibern die bestehenden Defizite vielfach nicht bewusst waren, da für den Betrieb einer Online-Apotheke zumeist auf technische Dienstleister zurückgegriffen wird. Datenschutzrechtlich verantwortlich bleiben auch in diesen Fällen nach § 11 Abs. 1 BDSG jedoch die einzelnen Apotheker.

Nach branchenbezogenen Untersuchungen besuchten 2009 jeder 10. der 40 Millionen Internetnutzer in Deutschland mindestens einmal eine Online-Apotheke. Da hierbei zum Teil sensible Gesundheitsdaten anfallen, bedarf es aus Sicht des LfD dringend einer Überarbeitung der Anmeldeverfahren. Angesichts der Sensibilität der Daten muss eine angemessene Sicherheit gewährleistet sein; der Wettbewerb bei Kundenakquise- und Kundenbindung darf nach Auffassung des LfD nicht auf Kosten des Sicherheitsniveaus ausgetragen werden.

Angesichts des Umfangs der erkannten Schwachstellen hat der LfD zunächst die Apothekenaufsicht und die Landesapothekerkammer unterrichtet und Empfehlungen für eine sichere Gestaltung der Online-Zugänge ausgesprochen. Diese haben die Versandapotheken informiert und auf die notwendige Überarbeitung der Verfahren hingewiesen. Die Apothekenaufsicht wird die Empfehlungen des LfD künftig im Zulassungsverfahren für Versandapotheken berücksichtigen.

Da es sich nach den Erkenntnissen des LfD um ein generell bestehendes Problem handelt – was sich unter anderem daran zeigte, dass ein Großteil der Online-Lösungen auf den selben, bundesweit angebotenen technischen Plattformen fußte –, hat er die Datenschutzaufsichtsbehörden der anderen Bundesländer unterrichtet.

Der LfD wird die Umsetzung der Empfehlungen daher zu gegebener Zeit stichprobenweise überprüfen und bei weiterhin festgestellten Mängeln Maßnahmen nach § 38

Abs. 5 BDSG – Anordnungen, ggf. Zwangsgeldverfahren oder Untersagungen – ergreifen.

Hinweise zur Gestaltung von Online-Zugängen

- Es ist technisch sicherzustellen, dass für die Zugangskennungen und die zughörigen Passwörter von den Benutzern unterschiedliche Zeichenfolgen gewählt werden.
- Durch technische Maßnahmen is zu gewährleisten, dass für die Zugangskennung sowie für das Passwort eine Mindestlänge von fünf Zeichen eingehalten wird.
- Die zulässige Zeichenfolge für ein Passwort sollte aus alphanumerischen Zeichen bestehen und neben Buchstaben mindestens eine Ziffer oder ein Sonderzeichen enthalten.
- Einfachmuster (z.B. 123456, abcdef, aaaaaa) und triviale Angaben (test, service, system, admin) müssen bei der Vergabe von Passwörtern ausgeschlossen werden.
- Durch technische Maßnahmen ist sicher zu stellen, dass ein systemseitig ggf. vergebenes Anfangspasswort nach der erstmaligen Anmeldung vom Benutzer zwingen geändert werden muss.
- Nach einer überschaubaren Zahl erfolgloser Anmeldeversuche muss eine Sperrung des Zugangs erfolgen oder eine erneute Anmeldung nur mit zeitlicher Verzögerung möglich sein.

13.7 Research in Motion/Blackberry-Lösungen in der Landesverwaltung

Im Rahmen der vorgesehenen Einführung des Push-Mail-Dienstes der Firma Research in Motion (RIM) im Bereich der Landesregierung wurde der LfD um Stellungnahme gebeten. Dieser wurde unter datenschutzrechtlichen Gesichtspunkten in der Vergangenheit vor allem aufgrund der Tatsache problematisiert, dass die gesamte Kommunikation über zentrale RIM-eigene Mobile Routing Center (MRC) geführt wird. Deren Aufbau, Konzeption und Sicherheitsniveau waren nicht offen gelegt, so dass nicht verlässlich abgeschätzt werden konnte, ob eine ausreichende Vertraulichkeit der Kommunikation gegenüber dem Betreiber sowie gegenüber Dritten gewährleistet ist.

Eine zwischenzeitlich vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) erstellte Sicherheitsanalyse (Certification Report 06-104302, S. 28) kommt in diesem Zusammenhang zu dem Ergebnis, dass mit der geprüften Schlüsselgenerierung und den Schlüsselaustauschprotokollen die Vertraulichkeit und Integrität übermittelter Inhalte gewährleistet ist. Bei der Analyse der Blackberry Enterprise Solution wurden keine Hinweise auf Funktionen gefunden, die es dem Betreiber erlauben würden, E-Mails von Kunden zu lesen. Die zur Verschlüsselung von Nachrichten genutzten Mechanismen könnten mit angemessenem Zeit- und Ressourcenaufwand nicht gebrochen werden, die Kommunikation bleibe damit vertraulich gegenüber Dritten, einschließlich des Betreibers.

Die Untersuchung der Blackberry Enterprise Server-Lösung hatte ergeben, dass keine Funktionen vorhanden sind, die es dem Betreiber erlauben würden, auf Informationen zuzugreifen, die auf dem Enterprise Server oder damit verbundenen Systemen gespeichert sind. Auf der Grundlage der Sicherheitsanalyse wurde vom SIT ein bis Dezember 2010 gültiges Zertifikat erteilt. Eine ähnliche Aussage trifft die Sicherheitsanalyse des österreichischen Zentrums für sichere Informationstechnologie aus dem Jahr 2004 (http://www.a-sit.at/de/technologiebeobachtung/sicherheitsanalysen_und_konzepte/blackberry.php).

Für die kryptografischen Module der Endgeräte-Software sowie der Implementierung im Blackberry Enterprise Server wurden vom US-amerikanischen National Institute of Standards and Technology im Jahr 2005 entsprechende Zertifikate erteilt und 2008/2009 aktualisiert (http://csrc.nist.gov/groups/STM/cmvp/validation.html).

Aus Sicht des LfD wurden damit die Bedenken hinsichtlich eines potentiellen Zugriffs auf die Kommunikation zwischen Enterprise Server und Endgerät durch Dritte einschließlich Research in Motion weitgehend ausgeräumt. Bestehende Vorbehalte des Bundesamts für Sicherheit in der Informationstechnik hinsichtlich der fehlenden Möglichkeit, selbstentwickelte Kryptomechanismen in eine Blackberry-Lösung einzubinden, sind aus Sicht des LfD nachvollziehbar. Sie erstrecken sich allerdings auf den Bereich sicherheitskritischer Anwendungen bzw. den Geheimschutzbereich. Für davon nicht betroffene Anwendungen bietet unter Berücksichtigung der dabei ausgesprochenen Empfehlungen zu Konfiguration und Betrieb die vom SIT zertifizierte Lösung nach Auffassung des LfD eine ausreichende Kommunikationssicherheit.

Hinsichtlich der weiteren Aspekte des Einsatzes mobiler Endgeräte (Schutz vor unbefugter Nutzung, Schutz im Fall des Diebstahls oder bei Verlust, Authentifizierung beim Zugang zum rlp-Netz etc.) ergeben sich für die RIM-Lösung Anforderungen, wie sie vergleichbar auch für bereits jetzt schon eingesetzte Lösungen bestehen und im Rahmen der IT-Standards der Landesverwaltung in der „Landestrategie für den entfernten und mobilen E-Mail-Zugriff“ vorgesehen sind.

Die Aussagen des Fraunhofer-Instituts gelten allerdings nur für die zertifizierte Konfiguration der Blackberry Enterprise Solution. Da sowohl die eingesetzten Endgeräte als auch die verwendete Software Änderungen

unterliegen, wurde dem Hersteller eine verbindliche Erklärung abverlangt, ob und ggf. in welchem Umfang im Rahmen der o.g. Zertifizierungen getroffene Aussagen davon berührt sind.

Eine Verarbeitung personenbezogener Daten durch Research in Motion wäre als Auftragsdatenverarbeitung nach § 4 LDSG zu bewerten. Dieser verpflichtet die auftraggebende Stelle sicherzustellen, dass die auftragnehmende Person oder Stelle die Bestimmungen des Landesdatenschutzgesetzes beachtet und sich der Kontrolle des LfD unterwirft. Angesichts der Tatsache, dass es sich bei Research in Motion um ein kanadisches Unternehmen handelt und die relevante IT-Infrastruktur außerhalb Deutschlands liegt, ist es aus Sicht des LfD fraglich, ob, selbst im Fall einer entsprechenden vertraglichen Regelung, bei Bedarf eine zeitnahe und effektive Kontrolle möglich wäre. Die Bedeutung dieser Frage würde sich jedoch relativieren, wenn sichergestellt wäre, dass dem Betreiber der Mobile Routing Center ausschließlich verschlüsselte Informationen zur Kenntnis gelangen. Der LfD hat daher darum gebeten zu klären, welche Informationen im Einzelnen – Nutzdaten, Verkehrsdaten, Stammdaten der Kommunikationsteilnehmer – im Zugriff von Research in Motion stehen, welche davon ausschließlich in verschlüsselter Form und welche im Klartext vorliegen. Nach Lage der Dinge dürften zumindest die Kennungen der Endgeräte im Klartext benötigt werden. Wenn diese von Research in Motion jedoch auf zulässige Weise keinen einzelnen Nutzern zugeordnet werden können, wäre auch hier ein Personenbezug auszuschließen.

Zu den angesprochenen Punkten lag bis Redaktionsschluss noch keine verbindliche Rückäußerung seitens Research in Motion vor.

13.8 Protokollierung tut Not

Angesichts der Komplexität heutiger IT-Verfahren mit ihrer hohen Zahl von Benutzern, verteilten Strukturen und Verantwortlichkeiten bedarf es für eine datenschutzgerechte Gestaltung eines geeigneten Instrumentariums, um die Verarbeitung personenbezogener Daten nachvollziehen zu können. Grundlage einer angemessenen Nachvollziehbarkeit ist eine aussagefähige Protokollierung einschließlich geeigneter Auswertungsmöglichkeiten. Protokolldaten müssen Auskunft darüber geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Ihre Nutzung für Revisions- und Beweiszwecke erfordert, dass sie vollständig und nur Berechtigten zugänglich sind und nicht nachträglich verändert werden können. Zur Wahrung der Vertraulichkeit, Integrität und Authentizität sind nach Möglichkeit geeignete kryptografische Verfahren nach dem Stand der Technik einzusetzen.

Soweit nicht bereichspezifische Rechtsgrundlagen Vorgaben hinsichtlich der Nachvollziehbarkeit formulieren, gründen die entsprechenden Anforderungen auf § 9 BDSG bzw. § 9 LDSG. Danach sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften über den Datenschutz zu gewährleisten. Die Notwendigkeit einer Protokollierung ergibt sich dabei aus Nr. 4 und Nr. 5 der Anlage zu § 9 BDSG sowie als vorbeugende Maßnahme der Zugangs- und Zugriffskontrolle bzw. aus § 9 Abs. 2 Nr. 10 LDSG (Verarbeitungskontrolle).

Nach Auffassung des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder ist eine Protokollierung lesender Zugriffe aus Gründen der datenschutzrechtlichen Revisionssicherheit grundsätzlich erforderlich. Es sind Mechanismen zu schaffen, mit denen lesende Zugriffe orientiert an der Art der Daten bzw. der genutzten Funktionen differenziert protokolliert werden können. Der Umfang der Protokollierung korrespondiert dabei mit den bestehenden Zugriffsregelungen. Bei hinreichend fein differenziertem Zugriffsschutz kann eine Protokollierung reduziert werden; umgekehrt steigt ihre Bedeutung in den Bereichen mit weit gefassten (Abfrage-) Berechtigungen. Erkenntnisse aus der Kontrollpraxis zeigen, dass trotz entgegenstehender Regelungen in Informationssystemen bestehende Recherche- und Auswertungsmöglichkeiten auch für Abfragen genutzt werden, bei denen das Vorliegen eines sachlichen Grundes zweifelhaft ist. Neben einem stringenten Berechtigungskonzept kann dem nur mit einer Protokollierung lesender Zugriffe begegnet werden. Einem oftmals nur geringen Entdeckungsrisiko missbräuchlicher Zugriffe müssen geeignete Aufklärungsmöglichkeiten – auch mit Blick auf deren präventive Wirkung – gegenüberstehen.

Eine angemessene Nachvollziehbarkeit ist im Allgemeinen bei der Erfassung folgender Angaben sichergestellt:

- Authentifizierung und Autorisierung (Login/Logout),
- Zeitpunkt eines Zugriffs,
- Kennung des jeweiligen Benutzers,
- Kennung der jeweiligen Arbeitsstation,
- aufgerufene Transaktion (Anzeige-/Abfragefunktion, Reportname, Maskenbezeichnung),
- verwendete Such- bzw. Abfragekriterien (z.B. Name, Geburtsdatum, Wohnort, Vorgangsnummernummer etc.),
- Ergebnis der Abfrage (z.B. Zahl der Trefferfälle, Fallnummern, Kennung der angezeigten Bildschirmmaske),

- etwaige Folgeaktionen bzw. Navigationsschritte (z.B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport).

Protokolldaten unterliegen als personenbezogene Daten ihrerseits datenschutzrechtlichen Vorschriften sowie einer strikten Zweckbindung (z. B. § 31 BDSG, § 13 Abs. 6 LDSG). Sie dürfen insbesondere nicht für eine automatisierte allgemeine Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden. Eine stichprobenweise oder anlassbezogene Auswertung von Protokolldaten im Rahmen der Datenschutzkontrolle ist keine derartige allgemeine Verhaltens- und Leistungskontrolle. Sie ist weiterhin keine Vorratsdatenspeicherung; diese setzt eine Speicherung zu unbestimmten Zwecken voraus, ein solcher (Datenschutzkontrolle) ist für die Protokolldaten jedoch ausdrücklich normiert.

Die Datenschutzbeauftragten des Bundes und der Länder haben die zentralen Empfehlungen zur Protokollierung in informationstechnischen Systemen in einer allgemeinen Orientierungshilfe zusammengefasst.

Orientierungshilfe „Protokollierung“ des Arbeitskreises Technik
(http://www.datenschutz.rlp.de/downloads/oh/ak_oh_protokollierung.pdf)

13.9 Biometrische Authentisierung

Die Authentisierung von Personen anhand bestimmter körperlicher Merkmale wie z.B. Fingerabdrücken, Gesichtsgeometrie oder Irismuster kommt zunehmend ergänzend oder alternativ zu bisherigen Authentisierungsverfahren wie Benutzerkennung/Passwort oder Tokenlösungen zum Einsatz.

Im Gegensatz zu Benutzerkennung und Passwort und zu Verfahren von Besitz und Wissen sind biometrische Daten potenziell lebenslang und eindeutig mit den Betroffenen verbunden. Deshalb sind für biometrische Authentisierungsverfahren – unabhängig vom im Einzelfall verwendeten Verfahren – besondere Vorkehrungen zu treffen:

- Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.
- Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens von grundlegender Bedeutung. Dabei sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z.B. auf einer Chipkarte, realisiert werden.
- Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptografischer Verfahren.

Mit Blick auf die besonderen Gegebenheiten und Anforderungen bei der Verarbeitung biometrischer Merkmale haben die Datenschutzbeauftagten des Bundes und der Länder eine Orientierungshilfe zum Einsatz biometrischer Authentifizierungsverfahren herausgegeben.

Orientierungshilfe „Biometrische Authentisierung“ des Arbeitskreises Technik
(http://www.datenschutz.rlp.de/downloads/oh/ak_oh_biometrie.pdf)

13.10 Verfahrenstests mit Echtdaten

Im Berichtszeitraum wurde wiederum mehrfach die Frage an den LfD herangetragen, in welchem Umfang Echtdaten für den Test von IT-Verfahren genutzt werden können (vgl. auch 21. Tb., Tz. 21.2.2). Angesichts der Tatsache, dass mit der Entwicklung heutiger IT-Verfahren in der Regel Softwareunternehmen beauftragt werden und Testdaten damit häufig außerhalb der datenverarbeitenden Stelle genutzt werden, kommt diesem Punkt grundsätzliche Bedeutung zu. Aus datenschutzrechtlicher Sicht kommt die Verwendung von Echtdaten nur insoweit in Betracht, als die zu testenden Sachverhalte mit den Testdaten nicht hinreichend verlässlich erfasst werden oder der Aufwand zu deren Erzeugung in erforderlichem Umfang und Ausprägung außer Verhältnis steht. Weiterhin sind folgende Punkte zu berücksichtigen:

- Verfahrenstests mit Echtdaten stellen einer Datenverarbeitung im Auftrag nach § 4 LDSG dar. Die bereitgestellten Daten dürfen ausschließlich für Testzwecke verwendet werden. Diese sind inhaltlich festzulegen und zeitlich zu beschränken. Eine darüber hinausgehende Nutzung muss vertraglich ausgeschlossen werden.
- Die an den Verfahrenstests beteiligten Personen sind zuvor nach § 8 LDSG auf die Wahrung des Datengeheimnisses zu verpflichten. Werden die Daten an nicht-öffentliche Stellen abgegeben, sind die betroffenen Mitarbeiter des Auftragnehmers nach dem Verpflichtungsgesetz zu verpflichten, um eine Anwendbarkeit strafrechtlicher Bestimmungen wie bei Amtsträgern zu gewährleisten (§ 203 StGB).
- Die für Testzwecke zur Verfügung gestellten Daten sind nach Abschluss der Verfahrenstests zu löschen, Datenträger zu vernichten. Die Löschung bzw. die Vernichtung ist durch den Auftragnehmer zu bestätigen.

Aufgrund der allgemeinen Bedeutung der Frage haben die Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zum Projekt- und Produktivbetrieb von IT-Verfahren herausgegeben:

Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“
(http://www.datenschutz.rlp.de/downloads/oh/ak_oh_projekt_produktivbetrieb.pdf)

13.11 Identitätsmanagement

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren ist vielfach bereits vorhanden. So hat beispielsweise jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 TMG).

Bisher werden anonyme oder pseudonyme Nutzungsmöglichkeiten allerdings nur selten angeboten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in einer Entschließung vom 3./4. April 2008 gefordert, den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollten die Einführung solcher datenschutzfördernder Systeme unterstützen.

Die Gesichtspunkte, die aus Datenschutzsicht an geeignete Identitätsmanagementverfahren zu stellen sind, hat der Arbeitskreis Technik der Datenschutzbeauftragten in einem Arbeitspapier formuliert.

Arbeitspapier „Identitätsmanagement“ des Arbeitskreises Technik
(http://www.datenschutz.rlp.de/downloads/oh/ak_oh_id-management.pdf)

14. Aus der Dienststelle

14.1 Personalsituation

Beim LfD waren im Berichtszeitraum zunächst 12 Mitarbeiter beschäftigt. Zur Wahrnehmung der neuen Aufgaben im nicht-öffentlichen Bereich (s.a. Tz. 2.3.1) wurden dem LfD eine A16-, zwei A11-Stellen und eine Stelle im Sekretariatsbereich bewilligt. Die Stellen konnten – mit einer Ausnahme – zeitnah besetzt werden. Am Ende des Berichtszeitraums sind in der Geschäftsstelle nunmehr 15 Mitarbeiter beschäftigt, vier von ihnen sind Teilzeitkräfte.

14.2 Zulassung als Ausbildungsstelle für Referendare

Zu Beginn des Berichtszeitraums hat das Ministerium des Innern und für Sport den LfD als Ausbildungsstelle für Referendare in der Verwaltungspflichtstation zugelassen. Inzwischen konnten acht Referendare ihre Verwaltungs- bzw. Wahlstation absolvieren. Darüber hinaus nahmen im Berichtszeitraum drei Rechtsstudenten ihr juristisches und drei Schüler ihr Schülerpraktikum war.

14.3 Unterbringung der Dienststelle des LfD

Mit der Übertragung der Zuständigkeit für den Datenschutz im privaten Bereich und der damit verbundenen Erhöhung des Personalbestandes war es notwendig, zusätzlichen Büroraum anzumieten. Dies gelang in dem Mietobjekt, in dem die Dienststelle untergebracht ist. Die Erweiterung wurde zum Anlass für eine Renovierung genommen. Außerdem wurden die technischen Einrichtungen auf den neuesten Stand gebracht.

14.4 Kommentar zum Landesdatenschutzgesetz

Im Kommunal- und Schul-Verlag ist im Juli 2009 eine aktualisierte Fassung des Kommentars zum Landesdatenschutzgesetz Rheinland-Pfalz erschienen. Er wurde von Mitarbeitern des LfD erstellt und bietet die Gewähr für eine gelungene Verbindung von Recht und Praxis (s.a. Tz. 3.5.3).

Abkürzungsverzeichnis

Gesetze und Verordnungen

AGG	Allgemeines Gleichbehandlungsgesetz
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BZRG	Bundeszentralregistergesetz
EuWO	Europawahlordnung
GDIG-E	Entwurf eines Landesgesetzes über die Geodateninfrastruktur
GemO	Gemeindeordnung
GerOrgG	Gerichtsorganisationsgesetz
GG	Grundgesetz
InsO	Insolvenzordnung
KWO	Kommunalwahlordnung
LArchG	Landesarchivgesetz
LDSG	Landesdatenschutzgesetz
LDÜJG	Landesgesetz über Dolmetscherinnen und Dolmetscher und Übersetzerinnen und Übersetzer in der Justiz
LGVerm	Landesgesetz über das amtliche Vermessungswesen
LKindSchuG	Landeskinderschutzgesetz
LKO	Landkreisordnung
LMG	Landesmediengesetz
MG	Meldegesetz
MRRG	Melderechtsrahmengesetz

PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis – Personalausweisgesetz –
POG	Polizei- und Ordnungsbehördengesetz
SchulG	Schulgesetz
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB II	Sozialgesetzbuch – Zweites Buch –
SGB IV	Sozialgesetzbuch – Viertes Buch –
SGB V	Sozialgesetzbuch – Fünftes Buch –
SGB X	Sozialgesetzbuch – Zehntes Buch –
SGB XII	Sozialgesetzbuch – Zwölftes Buch –
StGB	Strafgesetzbuch
StVollzG	Strafvollzugsgesetz
TMG	Telemediengesetz
UIG	Umweltinformationsgesetz
VVG	Versicherungsvertragsgesetz
ZVG	Zwangsversteigerungsgesetz

sonstige Abkürzungen

a.F.	alte Fassung
Art.	Artikel
BGBl.	Bundesgesetzblatt
BT-Drs.	Bundestagsdrucksache
i.V.m.	in Verbindung mit
JVA	Justizvollzugsanstalt
LfD	Landesbeauftragter für den Datenschutz Rheinland-Pfalz
LT-Drs.	Landtagsdrucksache
MinBl.	Ministerialblatt
m.w.N.	mit weiteren Nachweisen
n.F.	neue Fassung
NJW	Neue Juristische Wochenschrift
RFID	Radio Frequency Identification
SWIFT	Society for Worldwide Interbank Financial Telecommunication
Tb.	Tätigkeitsbericht
TKÜ	Telekommunikationsüberwachung
Tz.	Textziffer