Baden-Württemberg

INNENMINISTERIUM

8. März 2012

Stellungnahme der Landesregierung

zum

30. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2010/2011

Dorotheenstraße 6, 70173 Stuttgart, Telefon (0711) 231 - 4, Fax (0711) 231 - 50 00
E-Mail: poststelle@im.bwl.de, Internet: http://www.im.baden-wuerttemberg.de

Stellungnahme der Landesregierung
zum 30. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Die Landesregierung nimmt im Folgenden - entsprechend dem Beschluss des Landtags vom 17. September 1987 (LT-Drucksache 9/4667) - zu Beanstandungen und wesentlichen Ausführungen des Landesbeauftragten für den Datenschutz Stellung, die den Datenschutz im öffentlichen Bereich betreffen. Für den nichtöffentlichen Bereich, den der Landesbeauftragte für den Datenschutz nach der Zusammenlegung der beiden Datenschutzaufsichtsbehörden erstmals in seinem Tätigkeitsbericht darstellt, gibt es keine Vorgaben des Landtags. Da die Landesregierung keine Möglichkeit hat, auf die Einhaltung datenschutzrechtlicher Vorschriften durch nichtöffentliche Stellen hinzuwirken, äußert sie sich zu den Ausführungen des Landesbeauftragten für den Datenschutz in diesem Bereich nur, soweit es um Fragen der Gesetzgebung oder das Verhalten der Landesregierung geht und eine Erwiderung erforderlich ist.

1. Teil: Zur Situation

1. Die Zäsur - Datenschutz aus einer Hand in Baden-Württemberg

1.3 Erste Eindrücke und Probleme

Die Darstellung des Landesbeauftragten für den Datenschutz, das **Innenministerium** habe bei der Zusammenlegung der beiden Aufsichtsbehörden drei hochwertige Stellen für ministerielle und andere Zwecke „zurückbehalten“, ist so nicht richtig:

Das Innenministerium hat bis 31. März 2011 im Referat „Datenschutz, Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich“ nicht nur die Aufgaben der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich, sondern auch die ministeriellen Aufgaben auf dem Gebiet des Datenschutzes wahrgenommen. Auf letztere entfielen, wie das Innenministerium schon in seiner Antwort auf den Antrag der Abgeordneten Andreas Stoch u. a. SPD (LT-Drucksache 14/5333) dargestellt hat, eine Stelle des höheren und des gehobenen Dienstes, insgesamt also 2,0 Stellen. Da die ministeriellen Aufgaben auch nach der Zusammenlegung der beiden Datenschutzaufsichtsbehörden vom Datenschutzreferat des Innenministeriums erledigt werden, verblieben dort die Stelle des Referatsleiters (B3) und eine Stelle des gehobenen Dienstes (A12). Die auf die übergehenden Aufgaben entfallenden Stellen wurden auf den Landesbeauftragten für den Datenschutz übertragen, die diese Aufgaben wahrnehmenden Mitarbeiterinnen und Mitarbeiter wurden zum Landesbeauftragten für den Datenschutz versetzt. Nicht möglich war es, beim Übergang der Aufgaben den vom Landesbeauftragten für den Datenschutz für erforderlich gehaltenen Personalmehrbedarf zu Lasten des Innenministeriums zu decken.

Die vom Landesbeauftragten für den Datenschutz beklagten personellen Veränderungen in der Aufsichtsbehörde vor deren „Umressortierung“ beruhten auf Ereignissen und individuellen Entscheidungen von Mitarbeiterinnen und Mitarbeitern, die von der Personalverwaltung des Innenministeriums nicht beeinflussbar waren.

Die Landesregierung ist ebenso wie der Landesbeauftragte für den Datenschutz der Auffassung, dass weder dem Datenschutz noch den Betroffenen oder den seiner Aufsicht unterliegenden öffentlichen und nichtöffentlichen Stellen damit gedient ist, wenn die Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten für den Datenschutz „auf Dauer“ bei dieser Dienststelle verbleiben. Dies kann dazu führen, dass diese in einer auf die Abwägung unterschiedlicher Interessen angelegten Rechtsmaterie einseitig auf die Belange des Datenschutzes fokussiert sind und reine Datenschutzkarrieren durchlaufen. Die Landesregierung ist deshalb bestrebt, § 26 Absatz 4 Satz 4 des Landesdatenschutzgesetzes in der Praxis Rechnung zu tragen und die Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten für den Datenschutz in den allgemeinen Personalaustausch einzubeziehen und auf diese Weise das datenschutzrechtliche Wissen in der Landesverwaltung auszubauen.
Dies haben die Personalreferentinnen und -referenten der Ministerien dem Landesbeauftragten für den Datenschutz in der von ihm angesprochenen Sitzung versichert und ihm in Einzelfällen wohlwollende Prüfung zugesagt.

Allerdings sind bei derartigen Personalwechseln, worauf das **Staatsministerium** in dem vom Landesbeauftragten für den Datenschutz zitierten Schreiben hingewiesen hat, gesetzliche Vorgaben und die Stellensituation der jeweiligen Dienststellen zu beachten, die auch durch eine schriftliche Vereinbarung zwischen der Landesregierung und dem Landesbeauftragten für den Datenschutz nicht außer Kraft gesetzt werden können. Nach § 11 des Landesbeamtengesetzes sind freie Dienstposten bei den jeweiligen öffentlichen Stellen in der Regel öffentlich auszuschreiben. Auf diese Ausschreibungen können sich stets auch Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten für den Datenschutz bewerben, müssen sich dann aber dem Wettbewerb mit möglichen Konkurrentinnen und Konkurrenten stellen. Nach Artikel 33 Absatz 2 des Grundgesetzes und § 9 des Beamtenstatusgesetzes sind Personalauswahlentscheidungen nach Eignung, Befähigung und fachlicher Leistung zu treffen. Dabei kommt nach ständiger Rechtsprechung dienstlichen Beurteilungen von Beamten, insbesondere in den Auswahlverfahren, die Personalentscheidungen vorbereiten, maßgebliche Bedeutung zu. Stellenbesetzungen sind also im Wesentlichen abhängig von den Beurteilungen der jeweiligen Bewerber. Erfüllen mehrere im Landesdienst tätige Bewerber das Anforderungsprofil einer Ausschreibung, ist der am besten beurteilte Bewerber auszuwählen.
Hinzu kommt, dass die durch die Einsparverpflichtungen bedingte angespannte Stellensituation bei allen Dienststellen dazu führt, dass zunehmend neu zu besetzende Dienstpos-

ten nur innerhalb der jeweiligen Dienststelle ausgeschrieben werden können, weil eine Stellenbesetzung von außen mangels vorhandener Stellen nicht mehr möglich ist. Die Einbeziehung externer Bewerber ist in diesen Fällen nur dann realisierbar, wenn der Wechsel stellenneutral erfolgt, was faktisch bedeutet, dass der Bewerber mit seiner Stelle kommen müsste. Aus diesem Grund sind auch der vom Landesbeauftragten für den Datenschutz vorgeschlagenen (verstärkten) Abordnung von Mitarbeiterinnen und Mitarbeitern, die bereits zwischen der Kultusverwaltung und der Polizei auf der einen und dem Landesbeauftragten für den Datenschutz auf der anderen Seite mit gutem Erfolg praktiziert wird und deswegen auch fortgesetzt werden soll, Grenzen gesetzt.

Diese Gegebenheiten müsste eine etwaige schriftliche Vereinbarung zwischen der Landesregierung und dem Landesbeauftragten für den Datenschutz berücksichtigen. Ihr Inhalt müsste sich daher auf eher formale Absprachen beschränken, die teilweise bereits jetzt praktiziert werden: So geben etwa die Ressorts ihre externen Stellenausschreibungen dem Landesbeauftragten für den Datenschutz zur Kenntnis, sodass sich dessen Mitarbeiterinnen und Mitarbeiter auf diese Stellen bewerben können. Denkbar wäre auch, dass der Landesbeauftragte für den Datenschutz Veränderungswünsche von Mitarbeiterinnen und Mitarbeitern unter Übersendung einer Profilbeschreibung den Ressorts zur Kenntnis bringt, sodass die Ressorts diese Personen bei der Besetzung geeigneter Stellen in ihre Überlegungen einbeziehen können. Ferner kann der Landesbeauftragte für den Datenschutz bei ihm zu besetzende Stellen den Ressorts melden, sodass diese die Ausschreibung geeigneten Personen in ihrem Geschäftsbereich bekannt machen können. Zum Abschluss einer schriftlichen Vereinbarung mit diesem Inhalt ist die Landesregierung bereit, falls der Landesbeauftragte für den Datenschutz dies wünscht.

1.4 Der Wechsel beginnt - auch im Datenschutz?

Die in der Koalitionsvereinbarung vorgesehene Bestimmung des Landesbeauftragten für den Datenschutz zur obersten Landesbehörde, die Übertragung der Bußgeldzuständigkeit für die Verfolgung datenschutzrechtlicher Ordnungswidrigkeiten auf den Landesbeauftragten für den Datenschutz und die Stärkung der Stellung der behördlichen Datenschutzbeauftragten machen Änderungen des Landesdatenschutzgesetzes und weiterer Rechtsvorschriften erforderlich. Nach Auffassung des **Innenministeriums** sollten diese zurückgestellt werden, bis feststeht, wie es mit dem am 25. Januar 2012 von der EU-Kommission vorgelegten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung, BR-Drucksache 52/12) weitergeht. Der Verordnungsentwurf sieht unter anderem Regelungen für die Aufsichtsbehörde, deren Unabhängigkeit, Ausgestaltung als Kollegialorgan, Aufgaben und Befugnisse sowie über die Bestellung behördlicher Datenschutzbeauftragter vor. Die Regelung soll die Richt-

linie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Amtsblatt der EG vom 23. November 1995 Nr. L 281/31) ersetzen, die durch die Mitgliedstaaten in nationales Recht umgesetzt wurde (in Deutschland insbesondere durch das Bundes- und die Landesdatenschutzgesetze). Mit dem Erlass dieser Verordnung würde die Europäische Union für den Datenschutzbereich unmittelbar geltendes Recht setzen, das das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze - zumindest weitgehend - gegenstandslos werden ließe.

Unabhängig hiervon wird das Innenministerium Maßnahmen ergreifen, um die Stellung der Datenschutzbeauftragten in den Behörden, das Aus- und Fortbildungsangebot für diesen Personenkreis und die Vernetzung der behördlichen Datenschutzbeauftragten zu verbessern sowie für diese wichtige Informationen bereitzustellen.

Was das Thema „Datenschutz als Bildungsaufgabe“ angeht, legt das **Kultusministerium** Wert darauf, dass der Datenschutz schon jetzt Gegenstand sowohl des Unterrichts in den allgemein bildenden und beruflichen Schulen als auch in der Lehreraus- und -fortbildung ist. Das Bildungsangebot wird derzeit allerdings weiterentwickelt.

In den Bildungsplänen für die weiterführenden allgemein bildenden Schulen in Baden-Württemberg aus dem Jahr 2004 ist das Thema in den Kontext der informationstechnischen Grundbildung (ITG) eingebettet.

Wissen, Problembewusstsein und Handlungskompetenzen im Bereich des Datenschutzes sind unverzichtbare Bestandteile moderner Medienkompetenz. Dementsprechend fordert der Entwurf einer neu gefassten Erklärung der Kultusministerkonferenz „Medien in der Schule“, die im Frühjahr 2012 verabschiedet werden soll, zum Thema „Urheberrecht und Datenschutz“ ausdrücklich eine Sensibilisierung der Schülerinnen und Schüler, Lehrkräfte, Schulleitungen und Eltern auf den Gebieten des Datenschutzes, Jugendschutzes und Persönlichkeitsrechts sowie des Urheber- und Lizenzrechts.

Das Kultusministerium unterstützt die Haltung der Kultusministerkonferenz und beabsichtigt, bei der Neufassung der Bildungspläne für die allgemein bildenden Schulen das Thema Medienbildung umfassend zu berücksichtigen. Neben eigenen, in den Stundentafeln der Schulen fest verankerten curricularen Einheiten zur Medienbildung beispielsweise in der Sekundarstufe I sollen Bildungsstandards für die Leitfächer der Medienbildung (Deutsch, sozialkundliche Fächer, Kunst, Musik, Religionslehre, Ethik, neuerdings auch Fremdsprachen) erarbeitet werden (integrativer Ansatz). Dabei wird auch der Datenschutz - insbesondere auch im Sinne einer Sensibilisierung für den Selbstdatenschutz - in ange-

messener Weise zu berücksichtigen sein. Die Mediennutzung der Kinder und insbesondere der Jugendlichen bietet dazu vielfältige Anhaltspunkte.

Neben der Verankerung im Bildungsplan spielt das Thema „Datenschutz“ auch in landesweiten Programmen und Initiativen zur schulischen Medienbildung eine wichtige Rolle, die unter anderem vom Landesmedienzentrum Baden-Württemberg (LMZ) zusammen mit den 57 Stadt- und Kreismedienzentren durchgeführt werden.

Darüber hinaus bietet das „Schülermedienmentorenprogramm“, mit dem Schülerinnen und Schüler zu Mentoren fortgebildet werden, um ihre Mitschüler beim Erwerb von Medienkompetenzen zu unterstützen, Module zum Datenschutz, Urheberrecht und zum Persönlichkeitsrecht an.

Auch in den beruflichen Schulen haben Medienkompetenz und Datenschutz einen hohen Stellenwert. Differenzierte Unterrichtsinhalte, die durch die Bildungspläne für die Schularten der beruflichen Schulen vorgegeben werden, vertiefen die von den Schülerinnen und Schülern in den zuführenden Schulen erworbene Medien- und Datenschutzkompetenz mit Blick auf die konkrete berufliche Relevanz. So sind in einem Großteil der Ausbildungsberufe, in denen die Bundesrahmenlehrpläne als Landeslehrpläne übernommen wurden, Fragen der Informationstechnologie in die Lernfelder integriert. In den beruflichen Vollzeitschularten ist das Thema Datenschutz ebenfalls in den Unterricht in den Fächern Informatik, Computertechnik beziehungsweise Datenverarbeitung oder vergleichbaren Fächern verankert.

Auch in der Lehreraus- und -fortbildung wird gegenwärtig bereits Medien- und Datenschutzkompetenz vermittelt. Der Landesbeauftragte für den Datenschutz erkennt dies in seinem Bericht auch an. Über die im Bericht aufgeführten Aktivitäten hinaus wurden Fortbildungsangebote zum Datenschutz inzwischen auch auf Fachberaterinnen und Fachberater sowie Lehrkräfte, die keine Funktionsstellen innehaben, erweitert. Das Kultusministerium hat die Landesakademie außerdem beauftragt, ein Konzept für eine Fortbildungsveranstaltung "Medienwelten unserer Kinder" zu entwickeln und dieses ständig zu aktualisieren. Dabei werden besonders Fragen des Datenschutzes behandelt sowie Strategien, die Schülerinnen und Schüler zum verantwortungsvollen Umgang mit eigenen Daten in sozialen Netzwerken und dem Internet allgemein anregen. Die Inhalte der geschilderten Initiativen der Fortbildung finden auch Eingang in die Lehrkräfteausbildungen an den Staatlichen Seminaren für Didaktik und Lehrerbildung.

Die Qualitätsentwicklung aller öffentlichen beruflichen Schulen nach dem Konzept "Operativ Eigenständige Schule" (OES) hält eine Sensibilisierung der Lehrkräfte für den Daten-

schutz für dringend notwendig; in diesem Rahmen ist Datenschutz daher insbesondere Bestandteil der Lehrerfortbildung zu den Themen Selbstevaluation und Feedback.

2. Entwicklung des Datenschutzrechts 2010/2011

2.1 Die Neuregelung der Videoüberwachung durch öffentliche Stellen in § 20a LDSG

Soweit der Landesbeauftragte für den Datenschutz - gestützt auf die Koalitionsvereinbarung - seiner Hoffnung Ausdruck gibt, der am 1. April 2011 in Kraft getretene § 20a des Landesdatenschutzgesetzes werde entsprechend seinen Forderungen im Gesetzgebungsverfahren bald geändert, ist dazu Folgendes zu bemerken:

Nachdem die EU-Kommission - wie bereits oben Nummer 1.4 erwähnt - am 25. Januar 2012 einen Vorschlag für eine Datenschutz-Grundverordnung vorgelegt hat, nach deren Erlass das Landesdatenschutzgesetz und damit auch die Videoüberwachungsvorschrift, soweit die Videoüberwachung in den Anwendungsbereich der Verordnung fällt, gegenstandslos wäre, sollte nach Auffassung des **Innenministeriums** vor etwaigen Änderungen des Landesdatenschutzgesetzes zunächst das weitere Schicksal dieses Verordnungsentwurfs abgewartet werden.

Unabhängig hiervon kann den Ausführungen des Landesbeauftragten für den Datenschutz jedenfalls in einigen Punkten nicht zugestimmt werden:

- Selbstverständlich kann der Gesetzgeber vorsehen, dass eine Videoüberwachungsvorschrift auch für Kameraattrappen gilt. Der Anwendungsbereich des Landesdatenschutzgesetzes würde damit allerdings auf Sachverhalte erweitert, in denen keine personenbezogenen Daten erhoben und verarbeitet werden. Deshalb hat der seinerzeitige Gesetzentwurf hiervon in Übereinstimmung mit der Mehrzahl der Landesdatenschutzgesetze und § 6b des Bundesdatenschutzgesetzes, der eher als die vom Landesbeauftragten für den Datenschutz angeführte Vorschrift im Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes mit § 20a Landesdatenschutzgesetz vergleichbar ist, abgesehen. Eine Schutzlücke entsteht für die Betroffenen dadurch nicht, weil diese sich gegen das Anbringen einer Kameraattrappe notfalls unter Berufung auf das allgemeine Persönlichkeitsrecht zur Wehr setzen können.

- Soweit der Landesbeauftragte für den Datenschutz der Auffassung ist, an „sensiblen Orten“ müsse die Videoüberwachung nicht nur „regelmäßig“, wie es in der seinerzeitigen Gesetzesbegründung heißt, sondern „ausnahmslos“ unzulässig sein, muss ihm aufgrund der langjährigen praktischen Erfahrungen einer Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich widersprochen werden. So kann es - um

nur ein Beispiel zu nennen - in ganz besonders gelagerten Einzelfällen gerechtfertigt sein, zwischen den einzelnen Räumen einer Toilette zu differenzieren und die Videoüberwachung in einem Toilettenvorraum, in dem sich lediglich ein Spiegel und Handwaschbecken befinden, noch als zulässig anzusehen, nicht hingegen in der eigentlichen Toilette. Die im Gesetz vorgesehene Abwägung und die Gesetzesbegründung tragen dem Rechnung und führen zu angemessenen Lösungen.

- Die in der Gesetzesbegründung erwähnte Ausnahme von der Kennzeichnungspflicht von Videoüberwachungsanlagen gibt lediglich die wohl herrschende Meinung in der datenschutzrechtlichen Literatur zum Bundesdatenschutzgesetz wieder. Selbstverständlich kann auf die Kennzeichnung einer Videoüberwachungsanlage nur verzichtet werden, wenn die Tatsache der Überwachung und die dafür verantwortliche Stelle für jedermann vor Betreten des überwachten Raums offenkundig sind. Wenn Streit darüber entstehen kann, ob etwas offenkundig ist, liegen die Voraussetzungen für eine Ausnahme von der Kennzeichnungspflicht nicht vor.

- Wenn sich der Landesbeauftragte für den Datenschutz dagegen wendet, dass zur Vermeidung oder Aufklärung von Ordnungswidrigkeiten von erheblicher Bedeutung durch Videoüberwachung erhobene personenbezogene Daten an die Polizei übermittelt werden dürfen, ist dem entgegenzuhalten, dass dadurch der Gleichklang von Erhebungs- und Verwertungsvorschrift hergestellt wird. Hinzu kommt, dass die Vermeidung und Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung auch eine Aufgabe der Polizei ist.

- Dass die in § 20a Landesdatenschutzgesetz enthaltene Verpflichtung zur Freigabe einer Videoüberwachungsanlage auch für Altanlagen gilt, die ohne Rechtsgrundlage betrieben wurden, ist so selbstverständlich, dass es dafür weder einer ausdrücklichen Regelung im Gesetz noch einer entsprechenden Aussage in der Gesetzesbegründung bedurfte. Ebenso selbstverständlich ist, dass die Freigabe einer Videoüberwachungsanlage die verantwortliche Stelle nicht davon entbindet, in der Folge zu prüfen, ob der Einsatz von Videoüberwachungstechnik noch gerechtfertigt ist.

- Nichtöffentliche Stellen, die über keinen behördlichen Datenschutzbeauftragten verfügen, lediglich wegen der beabsichtigten Einrichtung einer Videoüberwachungsanlage zur Bestellung eines solchen zu verpflichten, erschien dem Innenministerium nicht sachgerecht.

2.2. Ein modernes Datenschutzrecht für das 21. Jahrhundert

Das **Innenministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz, dass das deutsche Datenschutzrecht dringend modernisiert werden muss. Das Eckpunktepapier der Datenschutzbeauftragten stellt dafür eine gute Grundlage dar. Ob es noch zu einer Modernisierung des deutschen Datenschutzrechts kommen wird, ist allerdings fraglich, nachdem die EU-Kommission inzwischen den Entwurf einer Datenschutz-Grundverordnung vorgelegt hat, die unmittelbar geltendes Recht schaffen würde.

2.3 Aktivitäten auf Bundesebene im Berichtszeitraum

2.3.2 Die gesetzliche Neuregelung des Beschäftigtendatenschutzes ist überfällig

Das **Innenministerium** hält ebenso wie der Landesbeauftragte für den Datenschutz eine gesetzliche Regelung des Beschäftigtendatenschutzes für dringend erforderlich. Im Hinblick auf Artikel 82 des von der EU-Kommission vorgelegten Entwurfs einer Datenschutz-Grundverordnung wird jedoch genau geprüft werden müssen, welche nationalen Regelungen danach überhaupt noch möglich sind und ob und gegebenenfalls in welchen Punkten der dem Deutschen Bundestag zur Beratung vorliegende Gesetzentwurf geändert werden muss. Dabei muss bedacht werden, dass die EU-Kommission nach dem Verordnungsentwurf ermächtigt werden soll, jederzeit delegierte Rechtsakte zu erlassen, um bestimmte Rahmenbedingungen für die Datenverarbeitung in diesem Bereich festzulegen. Dies spricht dafür, zunächst das weitere Schicksal des Entwurfs der Datenschutz-Grundverordnung abzuwarten.

2.3.3 Bis hierher und nicht weiter: Rote Linien im Internet

Die Vorlage einer Datenschutz-Grundverordnung durch die EU-Kommission stoppt - jedenfalls zunächst - auch alle Pläne, den Datenschutz im Internet auf nationaler Ebene zu regeln.

2.4 Novellierung des europäischen Rechtsrahmens

Die EU-Kommission hat - wie bereits erwähnt - am 25. Januar 2012 den Entwurf einer Datenschutz-Grundverordnung und einer Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (BR-Drucksache 51/12) vorgelegt. Das **Innenministerium** hat den Landtag hierüber unterrichtet. Beide Entwürfe bedürfen noch sorgfältiger Prüfung durch Bund und Länder. Zweifelhaft erscheint, ob die Regelungen im Einklang mit dem Subsidiaritätsgrundsatz stehen. Entsprechende Zweifel hatte der Bundesrat bereits 2010 bei der Vorstellung des Gesamtkonzepts durch die EU-Kommission geäußert (vergleiche hierzu die BR-Drucksache 707/10). Der Bundesrat wird voraussichtlich im März 2012 zu beiden Entwürfen Stellung nehmen.

3. Internationaler Datenverkehr

3.4 Strafverfolgung über die Grenzen - Grenzen für den Datenschutz?

Die Regelungen des Rahmenbeschlusses Schwedische Initiative werden durch den ebenfalls in allen Mitgliedstaaten der Europäischen Union umzusetzenden „Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden“ ergänzt. Dieser regelt, unter welchen Voraussetzungen die übermittelten Daten genutzt und weiterverarbeitet werden dürfen. Das **Innenministerium** beabsichtigt, beide Rahmenbeschlüsse im Zuge der Novellierung des Polizeigesetzes umzusetzen. Hieran hält es - unbeschadet der Absicht der EU-Kommission, den Datenschutz durch den Erlass einer Richtlinie für die straftatenbezogene Datenverarbeitung und eine Datenschutz-Grundverordnung (vergleiche dazu oben Nummer 2.4) neu zu regeln - fest. Beide Rechtsvorschriften sollen nach den Vorstellungen der Kommission zwar bis Ende 2012 in Kraft treten. Angesichts der Zweifel, ob die beiden Vorschriften mit dem Subsidiaritätsgrundsatz vereinbar sind, und angesichts vieler Fragen und Bedenken im Detail ist es jedoch wenig wahrscheinlich, dass dieser Zeitplan eingehalten werden kann. Hinzu kommt, dass der Entwurf der Richtlinie eine zweijährige Frist für ihre Umsetzung in nationales Recht vorsieht.

4. Aktuelle technische Herausforderungen

4.1 Von hölzernen Pferden und Holzwegen - Der „Staats-Trojaner“ im Einsatz

Der Landesbeauftragte für den Datenschutz stellt nicht in Frage, dass die vier die jeweiligen richterlichen Anordnungen umsetzenden Maßnahmen der Quellen-Telekommunikationsüberwachung rechtmäßig waren. Er bezweifelt auch nicht den fachlichen Bedarf, eine Erfassungssoftware einzusetzen. Die Anmerkungen des Landesbeauftragten für den Datenschutz beziehen sich vielmehr auf Softwarefunktionen, aus denen Sicherheitsrisiken erwachsen können sowie diesbezügliche Verbesserungsmöglichkeiten. Das Landeskriminalamt hat die Vorschläge des Landesbeauftragten für den Datenschutz geprüft. Es plant zusätzliche Sicherungen bei der Authentifizierung und Verschlüsselung, der Protokollierung und der vorgeschalteten Testung der Funktionalitäten einschließlich einer Prüfung des Quellcodes. Parallel hierzu unterstützt das **Innenministerium** die Erarbeitung gemeinsamer Standards und Möglichkeiten für eine staatliche Software durch Bund und Länder, die seit Oktober 2011 läuft.

4.6 Das gefällt uns (noch) nicht - Datenschutz in sozialen Netzwerken

Das **Innenministerium** hält - wie die Datenschutzbeauftragten - eine Verbesserung des Datenschutzes bei sozialen Netzwerken in einer Reihe von Punkten für dringend erforderlich. In erster Linie sind die Betreiber solcher Plattformen aufgerufen, die zum Schutz der Nutzenden gebotenen Maßnahmen zu ergreifen, und zwar unabhängig davon, wo die Betreiber ihren Sitz haben und wie die Datenverarbeitung im Einzelnen datenschutzrechtlich zu beurteilen ist, insbesondere wer verantwortliche Stelle ist. Wie schwierig die datenschutzrechtliche Beurteilung dieser Vorgänge ist, zeigt das Gutachten des Wissenschaftlichen Dienstes des Schleswig-Holsteinischen Landtages (Umdruck 17/2988). Angesichts der Verbreitung der sozialen Netzwerke wird man die Lösung der Probleme nicht darin sehen können, dass öffentliche wie nichtöffentliche Stellen künftig keine Social Plugins mehr nutzen oder darauf verzichten, auf Plattformen von Facebook Fanpages einzurichten. Eine gewisse Zurückhaltung öffentlicher Stellen wäre aber gegenwärtig angesichts der aufgezeigten datenschutzrechtlichen Probleme angebracht. Darüber hinaus gilt es, in Gesprächen mit den Netzwerk-Betreibern und mit tatkräftiger Unterstützung der Datenschutzbeauftragten praktikable Lösungen zu finden, die Webseiten- und Fanpage-Betreibern die weitere Nutzung dieser Angebote zweifelsfrei in Einklang mit datenschutzrechtlichen Vorschriften ermöglichen. Da öffentliche Stellen zunehmend über soziale Netzwerke mit ihren Bürgerinnen und Bürgern kommunizieren, werden sich die Datenschutzressorts der Länder aufgrund eines Auftrags der Chefinnen und Chefs der Staats- und Senatskanzleien der Länder vom September 2011 an der Suche nach einer Lösung beteiligen. Sie haben inzwischen eine Arbeitsgruppe eingesetzt.

2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Gesetzgebung

1.2 Vorratsdatenspeicherung

Das **Innenministerium** lehnt das „Quick-Freeze-Verfahren“ in der bislang vom Bundesministerium für Justiz vorgeschlagenen Form ab und kann sich dabei auf den Beschluss der Innenministerkonferenz vom 21./22. Juni 2011 stützen. Ein „Einfrieren“ hat ohne zusätzliche Festlegung, welche Daten nach Umfang und Dauer durch Telekommunikationsdiensteanbieter gespeichert werden müssen, keinen für die Gefahrenabwehr und die Strafverfolgung nutzbaren Anwendungsbereich. Auch das Bundesverfassungsgericht hat in dem vom Landesbeauftragten für den Datenschutz zitierten Urteil festgestellt, dass das „Quick-Freeze-Verfahren“ kein der Vorratsdatenspeicherung vergleichbar effektives Ermittlungsinstrument ist, auf das der Gesetzgeber vor dem Hintergrund des aus dem Verhältnismäßigkeitsgrundsatz folgenden „Gebots der Wahl des am wenigsten einschneidenden Mittels“ verwiesen werden müsste (BVerfGE 125, 260, 318).

1.4 Rechtsgrundlagen für die Tätigkeit des Bundeskriminalamts

Das **Innenministerium** weist noch einmal darauf hin, dass die Rechtsverordnung nach § 7 Absatz 6 des Bundeskriminalamtsgesetzes nach überwiegender Auffassung nicht Voraussetzung für die Führung der Dateien beim Bundeskriminalamt war (vergleiche dazu auch die Stellungnahme der Landesregierung zum 29. Tätigkeitsbericht, LT-Drucksache 14/6131, Seite 13).

1.5 Verfassungsschutz - verfassungswidrige Maßnahmen zum Schutz der Verfassung?

Die Feststellung des Landesbeauftragten für den Datenschutz, dass die Regelung in § 6 Absatz 3 des Landesverfassungsschutzgesetzes - ebenso wie die vergleichbare Regelung im Bundesverfassungsschutzgesetz - noch nicht an die Rechtsprechung des Bundesverfassungsgerichts angepasst wurde, trifft zu. Das **Innenministerium** wird den Landesbeauftragten für den Datenschutz zu gegebener Zeit an der Erarbeitung der Neuregelung beteiligen.

2. Datenverarbeitung durch Sicherheitsbehörden

2.1 1. Mai 2009 - Tag der Arbeit - mit Folgen für viele

Die Darstellung des Vorgehens der Polizei trifft weitgehend zu. Die Löschung eines Großteils der Datensätze geht jedoch nicht vorrangig auf die Kontrolle des Landesbeauftragten für den Datenschutz, sondern auf die Überprüfungen durch die betroffene Polizeidirektion und das Landeskriminalamt zurück. Diese waren durch den schrittweisen Abschluss der Strafverfahren notwendigerweise zeitversetzt. Lediglich eine Löschung erfolgte erst nach zweimaligem Schriftwechsel mit dem Landesbeauftragten für den Datenschutz. Der Gesamtvorgang wurde eingehend mit dem Landesbeauftragten für den Datenschutz erörtert. Daraus resultierten einzelne Verbesserungen bei der Vor- und Nachbereitung der Verarbeitung personenbezogener Daten im Zusammenhang mit Großveranstaltungen. Die betroffene Polizeidirektion hat ihr gewonnenes Erfahrungswissen inzwischen an andere Dienststellen weitergegeben.

Das Vorgehen der Stadtverwaltung wird vom Landesbeauftragten für den Datenschutz zutreffend dargestellt. Auch teilen sowohl das **Innenministerium** als auch die Stadtverwaltung die rechtliche Beurteilung des Landesbeauftragten für den Datenschutz. Die Stadtverwaltung hat sich aufgrund der vom Landesbeauftragten für den Datenschutz ausgesprochenen Beanstandung eingehend mit dem Thema Datenschutz auseinandergesetzt und Maßnahmen ergriffen, um künftig die Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten. Insbesondere sollen einzelne Mitarbeiterinnen und Mitarbeiter, die sich vermehrt mit Datenschutzfragen befassen, intensiv geschult und regelmäßig fortgebildet werden.

2.2 Dienstanweisung POLAS-BW - ein Weg zu mehr Datenqualität

Der Landesbeauftragte für den Datenschutz hat das Engagement des Landeskriminalamts bei der Erarbeitung der Dienstanweisung hervorgehoben. Die Polizei wird - so das **Innenministerium** - ihre Bemühungen um die Datenqualität und eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter fortführen. Zu den vom Landesbeauftragten für den Datenschutz beispielhaft beschriebenen Fehlern im „Massengeschäft“ sind keine Anmerkungen erforderlich; deren Bereinigung ist überwiegend unstrittig.

2.3 Die Prüffallregelung nach § 38 Absatz 2 des Polizeigesetzes auf dem datenschutzrechtlichen Prüfstand

Auf die verfassungsrechtlichen Bedenken des Landesbeauftragten für den Datenschutz ist das **Innenministerium** bereits in seiner Stellungnahme zum 29. Tätigkeitsbericht eingegangen (vergleiche dazu LT-Drucksache 14/6131, Seite 21). Die Vorgängerregelung im Polizeigesetz, die für die Datenspeicherung zwingend eine Wiederholungsprognose voraussetzte, hatte zu keinem befriedigenden Ausgleich zwischen dem öffentlichen Interesse an der Verfügbarkeit der Daten zur Kriminalitätsbekämpfung (Erkennung als Mehrfachtäter) und den Interessen der von der Speicherung Betroffenen geführt.
Die Praxis der Polizeidienststellen im Umgang mit der sogenannten Prüffallregelung hat sich seit deren Einführung Ende 2008 verstetigt und durch ergänzende Hinweise des Landeskriminalamts, die dieses im Zusammenhang mit der Überarbeitung der Dienstanweisung POLAS-BW Mitte 2011 gegeben hat, und des Landesbeauftragten für den Datenschutz verbessert. Die vom Landesbeauftragten für den Datenschutz unterbreiteten Vorschläge spiegeln mehrere Aspekte des laufenden Qualitätsverbesserungsprozesses der Polizei wider. Die Zweifel des Landesbeauftragten für den Datenschutz an der Umsetzung des Aus- und Fortbildungskonzepts teilt das Innenministerium nicht. Gleichwohl werden die Lehrgänge beständig fortentwickelt und optimiert.

2.4 Videoüberwachung bei der Polizei - wofür ist sie wirklich geeignet?

- Stuttgart 21 - Was kann und was darf wo und warum aufgenommen werden?

Eine Kennzeichnung des Bereichs, der am Hauptbahnhof Stuttgart von Videoaufnahmen betroffen ist, fand Anfang Januar 2012 in Abstimmung mit dem Landesbeauftragten für den Datenschutz statt. Das **Innenministerium** weist darauf hin, dass noch ein Datenschutz- und Sicherheitskonzept erstellt wird.

2.5 Die „Sport-Dateien“ der Polizei im Land und das Problem mit der Verbunddatei

Nach Auffassung des **Innenministeriums** bedingen die unterschiedlichen Zweckbestimmungen der Dateien „Gewalttäter Sport“ und „Arbeitsdatei für szenekundige Beamte“ (SKB-Datenbank), dass gewaltgeneigte Sportfans oft in beiden Dateien gespeichert sind. Über die bundesweite Datei „Gewalttäter Sport“ hinaus unterstützt die „SKB-Datenbank“ auf Landesebene die Dokumentation von problemfantypischen Verhaltensweisen zur Verbesserung der Gefahrenabwehr und Straftatenvorsorge.

Die nur wenigen Polizeibeamten eingeräumte Befugnis zur Kenntnisnahme von Daten anderer Dienststellen - abgesichert durch eine hundertprozentige Zugriffsprotokollierung -

unterstützt dabei, unnötige Mehrfachspeicherungen von Personen zu verhindern und den Erkenntnisaustausch zu verbessern.

2.6 Was gibt es Neues zur Arbeitsdatei „Politisch motivierte Kriminalität“?

Die seit 2005 durchgeführten Überprüfungen der in der Arbeitsdatei „Politisch Motivierte Kriminalität“ gespeicherten Daten, datenschutzrechtliche Fortbildungen und andere Maßnahmen haben auch aus Sicht des **Innenministeriums** zur Erhöhung der Kompetenz und Handlungssicherheit der Staatsschutz-Sachbearbeiterinnen und -Sachbearbeiter im Umgang mit personenbezogenen Daten und zur Verbesserung der Qualität der Arbeitsdatei geführt.

2.7 Verdeckte Ermittlungen in Heidelberg und beim NATO-Gipfel 2009

Aus Sicht des **Innenministeriums** ist entscheidend, dass der Landesbeauftragte für den Datenschutz keine Zweifel an der grundsätzlichen Möglichkeit äußert, einen ausländischen Polizeibeamten einzusetzen. Seine dazu noch offenen Detailfragen hat das Landeskriminalamt im Dezember 2011 beantwortet.

2.8 „Zuverlässigkeitsüberprüfungen“ bei Großveranstaltungen weiterhin ohne gesetzliche Grundlage

Das **Innenministerium** hält weiterhin an der in den Stellungnahmen zum 27. und 28. Tätigkeitsbericht (LT-Drucksache 14/1269, Seite 16 und LT-Drucksache 14/2366, Seite 22) vertretenen Rechtsauffassung fest, dass Zuverlässigkeitsüberprüfungen auf der Grundlage sogenannter „informierter“ Einwilligungen der Betroffenen (das heißt die Betroffenen werden darüber informiert, was mit ihren Daten geschieht beziehungsweise geschehen kann) zulässig sind. Durch sicherheitsbehördliche Beratung der Veranstalter, überarbeitete Informationen für die Einwilligungsentscheidung sowie zentrale Widerspruchs- und Datenauskunftsstellen werden die Betroffenenrechte zusätzlich geschützt. Den fachlichen Bedarf für Überprüfungen von Personen in einzelnen sicherheitsempfindlichen Bereichen stellt auch der Landesbeauftragte für den Datenschutz nicht in Frage.
Die Zuverlässigkeitsüberprüfung ist keine polizeiliche Aufgabe. Die Polizei wirkt daran lediglich mit. Veranlasser der Überprüfung ist der jeweilige Veranstalter, also beispielsweise der Deutsche Fußballbund bei der Fußball-Weltmeisterschaft. Daher ist eine gesetzliche Regelung der Zuverlässigkeitsüberprüfung ausschließlich im Polizeigesetz als systematisch verfehlt abzulehnen und im Rahmen der Novellierung des Polizeigesetzes nicht vorgesehen. Eine gesetzliche Regelung müsste vielmehr - lässt man an dieser Stelle die von der EU-Kommission geplante Datenschutz-Grundverordnung außer Betracht - hinsichtlich privater Veranstalter im Bundesdatenschutzgesetz getroffen werden. Ob es dann noch

ergänzender Regelungen im Polizeigesetz für die Mitwirkung der Polizei bedarf, wäre zu prüfen, wenn der Wortlaut der Vorschrift im Bundesdatenschutzgesetz feststeht.

2.9 NADIS - das nachrichtendienstliche Informationssystem des Verfassungsschutzes in neuem Gewand

Das Bundesministerium des Innern beteiligt den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an der Entwicklung des Projekts. Diesem ist es unbenommen, seinerseits die Landesbeauftragten für den Datenschutz einzubinden.

Im Übrigen werden das **Innenministerium** und das Landesamt für Verfassungsschutz auch in Zukunft alles in ihrer Macht Stehende tun, damit der Landesbeauftragte für den Datenschutz seine Vor-Ort-Kontrollen effektiv durchführen kann.

2. Abschnitt: Justiz

1. Gesetzgebung

1.1 Schuldner bald im Internet? Das bundesweite Vollstreckungsportal

Das **Justizministerium** stellt voran, dass es sich bei dem „Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung“ sowie den vorgesehenen Verordnungsentwürfen zur konkreten Umsetzung um Bundesrecht handelt, auf dessen Ausgestaltung die Landesregierung nur begrenzten Einfluss hatte und hat. Vertreter des baden-württembergischen Justizministeriums wirken allerdings in einer bundesweiten Arbeitsgruppe „Vollstreckungsportal“ mit, in der Regelungen für die administrative und insbesondere technische Umsetzung erarbeitet beziehungsweise Vorschläge für die rechtliche Ausgestaltung formuliert werden. Auf den Ergebnissen dieser Arbeitsgruppe basieren im Wesentlichen die folgenden Darlegungen zu den aufgeworfenen Fragen:

- Nach dem Verordnungsentwurf des Bundesministeriums der Justiz sollen die Schuldnerdaten sowohl in den Ländern als auch im Vollstreckungsportal gespeichert werden; es liegt also eine redundante Speicherung vor. Eine Speicherung nur bei den zentralen Vollstreckungsgerichten der Länder hätte zur Folge, dass sechzehn bidirektionale Datenverbindungen in die Länder realisiert werden müssten, also Datenverbindungen, die eine Datenübertragung in beide Richtungen zulassen. Eine solche technische Umsetzung erscheint weder wirtschaftlich sinnvoll, da sie mit erheblichen Mehrkosten verbunden wäre, noch wäre ein stabiler, störungsfreier Betrieb gesichert. Die Abfrage der Schuldnerdaten würde mit einer erheblichen zeitlichen Verzögerung vonstatten gehen. In datenschutzrechtlicher Hinsicht wäre hiermit kein entscheidender Sicherheitsgewinn

verbunden, da es zusätzlich zur Übertragung von Abfragedatensätzen vom Vollstreckungsportal an das jeweilige Vollstreckungsgericht des Landes kommen würde. Des Weiteren kann die aus Datenschutzgründen erforderliche Protokollierung jedes Zugriffes auf die Schuldnerdaten nur gewährleistet werden, wenn die Schuldnerdaten auch im Vollstreckungsportal gespeichert werden. Andernfalls könnten die im Vollstreckungsportal gespeicherten Abrufprotokolle nicht zugeordnet werden.
Damit nicht synchrone Datenbestände zwischen den Ländern und dem Vollstreckungsportal erkannt und gegebenenfalls notwendige Gegenmaßnahmen ergriffen werden können, sollen im Vollstreckungsportal Kontrollmaßnahmen umgesetzt werden. So wird der Erfolg der Übertragung der Datensätze an das Vollstreckungsportal durch ein Quittierungsverfahren abgesichert. Auf der Grundlage dieses Quittierungsverfahrens wird in den Länderschuldnerverzeichnissen anschließend vermerkt, ob die Übertragung erfolgreich war. Diese Information wird regelmäßig automatisch überprüft; gegebenenfalls wird eine erneute Übertragung automatisch veranlasst. Somit ist gewährleistet, dass im Vollstreckungsportal immer die aktuellsten Daten verfügbar und abrufbar sind. Im Zweifelsfall wird dem Einsichtnehmenden angezeigt, dass der Datenbestand eines zentralen Vollstreckungsgerichts des Landes nicht auf dem neuesten Stand sein könnte. Zusätzlich haben alle sechzehn Länder über eine administrative Funktion die Möglichkeit, aktuelle Informationen zu ihren Datenbeständen ins Vollstreckungsportal einzustellen.

Eine Verlagerung der datenschutzrechtlichen Verantwortlichkeit ist mit der Einrichtung des Vollstreckungsportals nicht verbunden. Für die Überprüfung der eingelieferten Daten sind die jeweiligen zentralen Vollstreckungsgerichte der Länder als verantwortliche Stelle zuständig, eine zusätzliche Prüfung im Vollstreckungsportal ist nicht vorgesehen.

- Die Einsichtnahme in das Schuldnerverzeichnis ist nur zu bestimmten Zwecken gestattet; die Prüfung dieser Einsichtsberechtigung soll automatisiert erfolgen. Die Anregung des Landesbeauftragten für den Datenschutz, ein Freitextfeld “Verwendungszweck“ einzuführen, um eine effektive nachträgliche Kontrolle der Einsichtsberechtigung zu ermöglichen, hat die Arbeitsgruppe bereits aufgegriffen und die Umsetzung im Rahmen der abschließenden rechtlichen und technischen Ausgestaltung angeregt.

- Auch die Arbeitsgruppe hält eine sechsmonatige Aufbewahrungsfrist der Abrufprotokolle für zu kurz und hat darauf hingewiesen, dass dies mit dem Anspruch des Schuldners kollidiert, zu wissen, wer wann und aus welchem Grund den Eintrag in das Schuldnerverzeichnis eingesehen hat. Daher spricht sich die Arbeitsgruppe dafür aus, die Protokolldaten solange zu speichern, wie auch der Schuldnerdatensatz Bestand hat. Ein Vorhalten der Protokolldaten über die Löschung des Datensatzes hinaus wird dagegen nicht befürwortet, da der Schuldner nach der Löschung seines Datensatzes so gestellt werden muss, als sei er nie in das Schuldnerverzeichnis eingetragen gewesen. Deshalb

wäre eine Zuordnung der Abrufprotokolle zu den entsprechenden Schuldnerdaten dann nicht mehr möglich.

- Die im Verordnungsentwurf des Bundesministeriums der Justiz vorgesehene Registrierungsmöglichkeit mittels Kreditkarte wird auch von der Arbeitsgruppe Vollstreckungsportal aus datenschutzrechtlichen Gründen abgelehnt. Eine Identifikation anhand der Kreditkartendaten ist nicht denkbar, da die Kreditkartenprovider keine Daten über den Kreditkarteninhaber zurückliefern, sodass die dem Schuldner zu gewährende Möglichkeit der Einsichtnahme in die Abrufprotokolle aus technischen Gründen nicht realisierbar wäre. Folglich hat die Arbeitsgruppe dem Bundesministerium der Justiz vorgeschlagen, die entsprechende Vorschrift in der Schuldnerverzeichnisführungsverordnung zu streichen.

Was die Suche nach Schuldnern im Schuldnerverzeichnis anbelangt, wird seitens der Arbeitsgruppe „Vollstreckungsportal“ eine Suche nach Vor- und Nachname sowie einem weiteren Attribut wie Geburtsdatum oder Geburtsort als Mindestanforderung angesehen. Zudem sollte eine Übermittlung der Daten an den Anfragenden erst dann erfolgen, wenn die Eingabe der Suchdaten so präzise ist, dass das Suchergebnis auf einen übereinstimmenden Datensatz eingegrenzt werden konnte. Nur so kann sichergestellt werden, dass “Ausforschungsansätze“ vermieden werden.

Zwischenzeitlich liegt der Arbeitsgruppe ein erster Verordnungsentwurf vor, der die Suche im Vollstreckungsportal nach dem Vorbild des Portals für Insolvenzbekanntmachungen zum Inhalt hat. Demnach wäre bei der Suche die Angabe des Zentralen Vollstreckungsgerichts verpflichtend. Auch diese Vorgehensweise würde aber bei Personen mit gängigen Namen noch keine eindeutige Identifizierung ermöglichen. Die Arbeitsgruppe hat das Bundesministerium der Justiz bereits auf diese Problematik hingewiesen.

1.3 Der virtuelle Überwachungsraum - Funkzellenabfrage

Das **Justizministerium** ist der Auffassung, dass bei einer Funkzellenabfrage zwar zwangsläufig auf Daten unbeteiligter Personen zugegriffen wird. Dies begründet aber keine Eingriffstiefe, die mit der auf Kommunikationsinhalte abzielenden Telekommunikationsüberwachung vergleichbar wäre. Erhoben und an die Ermittlungsbehörden übermittelt werden bestimmte Verkehrsdaten der im Abfragezeitpunkt in einer Funkzelle eingebuchten Mobiltelefone. Neben der Kennung der Funkzelle handelt es sich um die Kennung der genutzten SIM-Karte, die Gerätekennung des genutzten Mobiltelefons (sogenannte IMSI- und die IMEI-Nummer) sowie einige Grunddaten der Kommunikation, nämlich Beginn und Ende des Kommunikationsvorgangs nach Datum und Uhrzeit sowie die Partnerrufnummer. Voraussetzung ist stets, dass Kommunikation stattgefunden hat. Bei bloßer Anwe-

senheit in einer abgefragten Funkzelle werden keine Daten gespeichert, so dass auch keine Daten an die Strafverfolgungsbehörden übermittelt werden können.
Ziel der Maßnahme ist die Ermittlung eines noch unbekannten Täters, von dem nur bekannt ist, dass er sich an einem bestimmten Tatort - auf den sich die Funkzellenabfrage beziehen muss - aufgehalten und dort kommuniziert hat. Hierzu werden gegebenenfalls die Ergebnisse verschiedener Tatortfunkzellenabfragen miteinander verglichen, um Übereinstimmungen (wiederkehrende IMEI- oder IMSI-Nummern) festzustellen. Abgeklärt werden nur die Kennungen, die mehrmals auftauchen oder aus anderen Gründen auffallen. In diesen Fällen ist dann vom Vorliegen eines Anfangsverdachts auszugehen. Er rechtfertigt die Abklärungen. Die Betroffenheit einer möglichen Vielzahl Unbeteiligter beschränkt sich daher auf die Erhebung der oben dargestellten Daten, ohne dass sich bei der überwiegenden Mehrzahl der hiervon Betroffenen weitere Ermittlungsmaßnahmen anschließen.

Vor diesem Hintergrund trifft es nicht zu, dass anhand dieser Daten die gezielte Abbildung von Freundschafts- und Beziehungsnetzwerken, die Erstellung von Bewegungsprofilen oder die Identifizierung von Interessen und politischer Einstellung möglich ist.

Nicht gerechtfertigt erscheint dem Justizministerium auch die Kritik am Rechtsbegriff der „Straftat von erheblicher Bedeutung“, bei deren Vorliegen eine Funkzellenabfrage rechtlich möglich ist und der nur schwer zu bestimmen sein soll. Der Rechtsbegriff findet in einer Vielzahl von anderen, zum Teil eingriffsintensiveren Eingriffsgrundlagen Verwendung, beispielsweise in §§ 81g, 98a, 100h, 100i, 110a, 163e sowie § 163f der Strafprozessordnung (StPO) - letzterer regelt etwa die längerfristige Observation eines Beschuldigten. Der Rechtsbegriff hat zudem durch die jahrzehntelange - auch verfassungsgerichtliche - Rechtsprechung ausreichend Konturen gewonnen. Auslegungsschwierigkeiten in der gerichtlichen Praxis - die Funkzellenabfrage steht wie jede verdeckte Ermittlungsmaßnahme unter ermittlungsrichterlichem Anordnungsvorbehalt - sind nicht bekannt.

Soweit bemängelt wird, die Strafprozessordnung enthalte keine Vorgaben, wie mit den erlangten Daten umzugehen sei, weist das Justizministerium auf die Vorschriften der § 101 Absatz 3 bis 8 StPO sowie § 477 Absatz 2 Satz 2 StPO hin. Darin finden sich detaillierte Regelungen, wie mit Daten weiter zu verfahren ist, die im Zuge der Ermittlungsmaßnahmen gewonnen worden sind.

3. Eine Strafanzeige kommt selten allein - aber warum müssen Anzeigeerstatter über andere Anzeigeerstatter informiert werden?

Das **Justizministerium** bestätigt die Sachverhaltsdarstellung des Landesbeauftragten für den Datenschutz.

Auf die im Tätigkeitsbericht geäußerte Kritik hin hat zwischenzeitlich der Generalstaatsanwalt in Stuttgart dem Landesbeauftragten für den Datenschutz schriftlich mitgeteilt, dass § 171 Satz 1 StPO grundsätzlich eine Rechtsgrundlage auch für die Mitteilung personenbezogener Daten ist. Im konkreten Einzelfall teilt die Generalstaatsanwaltschaft aber die Ansicht, dass die Namensnennung nicht zwingend war und daher hätte unterbleiben sollen.

Auch in vergleichbaren Fallgestaltungen, in denen dem Namen eines einzelnen Anzeigeerstatters für die jeweiligen Mitanzeigeerstatter keine – beispielsweise unter Rechtsschutz- beziehungsweise Rechtsverfolgungsaspekten – rechtlich relevante Bedeutung zukommt, wird künftig darauf geachtet werden, dass sich die Namen der Anzeigeerstatter aus der Verfügung nicht entnehmen lassen. Der Generalstaatsanwalt in Stuttgart hat sich hierzu mit dem Generalstaatsanwalt in Karlsruhe abgestimmt. Die staatsanwaltschaftliche Praxis wurde um entsprechende Beachtung gebeten.

3. Teil: Bildung und Forschung

1. Datenschutz an Schulen

1.2 Sparsamkeit am falschen Platz: Datenschutz an einer Gesamtschule

Das **Kultusministerium** sieht die Darstellung im Tätigkeitsbericht als zutreffend an und teilt auch die Rechtsauffassung des Landesbeauftragten für den Datenschutz.

Um der Beanstandung des Landesbeauftragten für den Datenschutz Rechnung zu tragen, hat das zuständige Regierungspräsidium den Schulleiter inzwischen auf die Belange des Datenschutzes hingewiesen. Die Schulleitung hat daraufhin schriftlich angeordnet, dass Schriftstücke, die personenbezogene Daten enthalten, in einem Aktenvernichter zu vernichten sind. Zusätzlich zu den bereits bestehenden Aktenvernichtern wurde ein weiteres Gerät angeschafft und im Kopierraum der Schule mit einer Bedienungsanweisung und einem Hinweis auf die Vernichtung datenschutzrelevanter Dokumente aufgestellt. Ferner wurden alle Beschäftigten der Schule über den Umgang mit personenbezogenen Daten aufgeklärt. Sie mussten hierzu durch Unterschrift bestätigen, dass sie die Bestimmungen der Verwaltungsvorschrift des Kultusministeriums „Datenschutz an öffentlichen Schulen“ vom 25. November 2009 gelesen haben und künftig beachten werden.

4. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

2. Datenschutz im Krankenhaus

2.1 Kontrollbesuch in einem Klinikum

Der Landesbeauftragte für den Datenschutz stellt den Sachverhalt zutreffend dar. Gegen dessen datenschutzrechtliche Beurteilung hat das **Sozialministerium** nichts einzuwenden.

Mangels konkreter Aufsichtsbefugnisse beschränken sich die Einwirkungsmöglichkeiten des Sozialministeriums jedoch auf allgemeine Hinweise gegenüber den Krankenhausträgern. Das Sozialministerium hat die baden-württembergische Krankenhausgesellschaft inzwischen schriftlich darum gebeten, ihre Mitgliedskrankenhäuser auf den Tätigkeitsbericht des Landesbeauftragten für den Datenschutz hinzuweisen und an die Einhaltung des Datenschutzes im Krankenhaus zu erinnern. Insbesondere sollen die Einrichtungen ihre Archivordnungen überprüfen und gegebenenfalls nachbessern sowie ihre Mitarbeiter auf datenschutzrechtliche Bestimmungen aufmerksam machen und regelmäßig schulen.

6. Aufzeichnung von Anrufen bei Integrierten Leitstellen

Um eine den Anforderungen des Datenschutzes genügende Praxis sicherzustellen, hat das **Innenministerium** die Träger der Leitstellen durch ein umfassendes, den Ausführungen des Landesbeauftragten für den Datenschutz entsprechendes Rundschreiben über die Rechtslage informiert und um Beachtung der datenschutzrechtlichen Vorgaben gebeten.

7. Wie geht es weiter mit der Einschulungsuntersuchung?

Auf die Frage der Rechtsgrundlage für die Einschulungsuntersuchung ist das **Sozialministerium** bereits in der Stellungnahme zum 29. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (LT-Drucksache 14/6131, Seite 29 ff) eingegangen.

Seit 2011 ist eine Projektgruppe des Sozialministeriums mit der Novellierung des Gesundheitsdienstgesetzes befasst. Es ist vorgesehen, auch in das novellierte Gesetz eine Rechtsgrundlage für die Erhebung personenbezogener Daten durch die Gesundheitsämter im Rahmen der Einschulungsuntersuchung aufzunehmen.

Auch zur Erforderlichkeit einzelner im Elternfragebogen abgefragter Daten hat sich das Sozialministerium bereits in der Stellungnahme zum 29. Tätigkeitsbericht geäußert. Alle Angaben des Elternfragebogens werden auf freiwilliger Basis erhoben. Sie dienen primär der Vorbereitung der Elternberatung und der Erarbeitung eines auf das Kind und seine

Familie individuell abgestimmten Förderplans. Nur ausgewählte Angaben werden gruppenstatistisch ausgewertet.

Wie vom Landesbeauftragten für den Datenschutz im Bericht angekündigt, werden die von ihm bislang als besonders kritisch eingeschätzten Fragen, wie die zur Geburt des Kindes (normale Geburt/Frühgeburt/Mehrlingsgeburt/Komplikationen) und zu Stärken und Schwächen des Kindes, nicht mehr im Fragebogen für sorgeberechtigte Personen enthalten sein.

Dass sich aus der Beantwortung der Frage, ob sich Eltern Sorgen um die Entwicklung ihres Kindes machen, Erkenntnisse für die Beurteilung von dessen Schulfähigkeit und Förderbedürftigkeit gewinnen lassen, wird vom Landesbeauftragten für den Datenschutz bezweifelt. Dem ist Folgendes entgegenzuhalten:

Die sozial-emotionalen Kompetenzen sind von erheblicher Bedeutung für den Schulerfolg. Die Antwort auf die genannte Frage trägt zusammen mit anderen Informationen zur Entscheidungsfindung bei, ob es beispielsweise sinnvoll ist, die sorgeberechtigten Personen zu bitten, den Fragebogen zu Stärken und Schwierigkeiten des Kindes auszufüllen und ob eine persönliche Kontaktaufnahme des Schularztes mit den Sorgeberechtigten zur Beurteilung der sozial-emotionalen Kompetenzen des Kindes erforderlich ist. Ziel ist, gegebenenfalls geeignete Maßnahmen zur Förderung der sozial-emotionalen Kompetenz des Kindes zu empfehlen. Die Erhebung von Daten ist somit auf den notwendigen Umfang beschränkt und weitere Fragen werden nur gestellt, wenn feststeht, dass die Beantwortung für Zwecke der Einschulungsuntersuchung benötigt wird.

Angaben zum Medienverhalten des Kindes sind weiter vorgesehen, da ein vernünftiger Medienkonsum für die Sprachfähigkeit eines Kindes von hoher Bedeutung ist und diese Angaben beispielsweise bei der Beratung der Eltern helfen. Auf die Bedeutung des Medienverhaltens für die Sprachfähigkeit hat unter anderem auch die Bundeszentrale für gesundheitliche Aufklärung mit entsprechenden Empfehlungen hingewiesen.

Die vom Landesbeauftragten für den Datenschutz geforderte Löschung soziodemografischer Angaben zu den Bezugspersonen des Kindes unmittelbar nach Übermittlung der pseudonymisierten Daten an das Landesgesundheitsamt soll durch entsprechende Vorgaben in den Arbeitsrichtlinien für die Einschulungsuntersuchung sichergestellt werden.

8. Pflegestützpunkte mit datenschutzrechtlichen Startproblemen

Die von der Landesarbeitsgemeinschaft Pflegestützpunkte Baden-Württemberg e.V. und vom **Sozialministerium** erbetene schriftliche Bestätigung des Landesbeauftragten für den Datenschutz, dass in diesen Fällen entgegen der Gesetzesbegründung eine Einwilli-

gungserklärung nicht erforderlich sei, liegt seit kurzem vor. Die Landesarbeitsgemeinschaft wird daher das Merkblatt überarbeiten und anschließend allen Pflegestützpunkten mitteilen, dass auf das Einholen einer Einwilligungserklärung bei den Hilfesuchenden verzichtet werden kann. Vor diesem Hintergrund erübrigt sich eine inhaltliche Stellungnahme des Sozialministeriums.

2. Abschnitt: Soziales

3. Einzelfälle

3.3 Verstoß gegen die Unterstützungspflicht öffentlicher Stellen

Gegen die Darstellung des Sachverhalts und die vom Landesbeauftragten für den Datenschutz ausgesprochene Beanstandung hat das **Sozialministerium** nichts einzuwenden. Das Landratsamt war sich nach eigenen Angaben jedoch nicht bewusst, gegenüber dem Landesbeauftragten für den Datenschutz unwahre Angaben zu machen. Vielmehr habe es für die Anfrage beim ehemaligen Arbeitgeber einen nicht auf den Einzelfall angepassten Vordruck verwendet. Auch habe es in der Folgezeit übersehen, dass die Anfrage unzulässig war. Nach eigenen Angaben hat das Landratsamt sein Formular inzwischen dahingehend geändert, dass nicht mehr nach dem Kündigungsgrund gefragt wird.

5. Teil: Datenschutz in anderen Verwaltungsbereichen

1. Kommunales

1.1 Fertigung von Luftbildaufnahmen zur Ermittlung von kommunalen Abwassergebühren

Zwischen dem **Innenministerium** und dem Landesbeauftragten für den Datenschutz gab es in dieser Sache einen umfangreichen Schriftwechsel und diverse Besprechungen, die jedoch nicht zu einer einvernehmlichen Beurteilung der Rechtslage führten.

Im Gegensatz zum Landesbeauftragten für den Datenschutz hält das Innenministerium die Herstellung und Verwendung von Luftbildern zum Zwecke der Ermittlung der versiegelten Flächen zur Feststellung der Grundlagen für die Gebührensatzungen und zur Erhebung von kommunalen Abwassergebühren nach dem Landesdatenschutzgesetz, aber auch nach den Vorschriften der Abgabenordnung für zulässig. Soweit der Landesbeauftragte für den Datenschutz davon ausgeht, dass die Zulässigkeit der Datenerhebung nach § 3 Absatz 1 Nummer 3a des Kommunalabgabengesetzes in Verbindung mit § 93 Absatz 1 der Abgabenordnung (AO) nicht gegeben ist, da die Daten in jedem Fall zunächst beim Gebührenschuldner zu erheben seien, kann dem nicht gefolgt werden. Vom Grundsatz des § 93 Absatz 1 Satz 3 AO darf nach Auffassung des Innenministeriums abgewichen und „andere Personen“ dürfen zur Auskunft angehalten werden, da es sich um einen atypischen Sachverhalt handelt, der sich von einem normalen Steuersachverhalt unterscheidet.

Hervorzuheben ist, dass es nicht allein um die Aufklärung eines Abgabensachverhalts beim Abgabenschuldner geht, sondern darum, im Vorfeld zunächst einmal die Grundlagen für eine rechtswirksame Abgabensatzung zu ermitteln. Zur Ermittlung des Gebührensatzes ist die Erhebung der versiegelten Fläche einer Gemeinde in ihrer Gesamtheit erforderlich. Im Übrigen dienen die Luftbilder der Vorbereitung des vom Landesbeauftragten für den Datenschutz geforderten Selbstauskunftsverfahrens. Die Beteiligung des Bürgers wird nicht etwa ersetzt, sondern die aufbereiteten Luftbilder erleichtern es den Grundstückseigentümern, die notwendigen Angaben zu machen.

Wenn der Landesbeauftragte für den Datenschutz darauf hinweist, dass es Gemeinden gibt, die die versiegelten Flächen auch ohne Luftbildaufnahmen ermittelt haben, so stellt dies die Zulässigkeit der Luftbildaufnahmen zu den genannten Zwecken nicht generell in Frage. Es ist bekannt, dass es mehrere Vorgehensweisen zur Ermittlung der versiegelten Flächen gibt. In der Regel sind dies vorbereitete Selbstauskunftsverfahren, bei denen die Grundlagen dem Liegenschaftskataster oder bereits vorhandenen oder bei speziellen Befliegungen aufgenommenen Luftbildern beziehungsweise Orthophotos entnommen und

durch Fachbüros aufbereitet werden. Es bleibt der einzelnen Gemeinde vorbehalten, das jeweils geeignete Verfahren zu wählen. Dabei ist die Ausgangssituation der einzelnen Kommune zu berücksichtigen, zum Beispiel die Größe der Gemeinde, die unterschiedlichen Siedlungsverhältnisse und -strukturen sowie die jeweils vorhandene Datenbasis.

1.3 Kommunale Veröffentlichungen im Internet

1.3.1 Die Übertragung von Gemeinderatssitzungen im Internet

Das **Innenministerium** stimmt mit dem Landesbeauftragten für den Datenschutz darin überein, dass Übertragungen von Gemeinderatsdebatten im Internet nur unter besonderen Einschränkungen und Vorgaben möglich sind.

Nach Mitteilung der betroffenen Stadt wird das Vorhaben, Gemeinderatssitzungen im Internet zu übertragen, derzeit nicht weiterverfolgt. Aktuell wird dort ein „Live Ticker“ eingerichtet, um interessierte Bürger - zeitnah - beispielsweise über Abstimmungsergebnisse im Gemeinderat zu informieren.

1.3.2 Die Veröffentlichung von Alters- und Ehejubiläen im Internet

Die Rechtsauffassung des Landesbeauftragten für den Datenschutz wird geteilt. § 34 Absatz 2 des Meldegesetzes lässt die Übermittlung von Jubiläumsdaten nur an Presse und Rundfunk zu. Damit ist die Übermittlung an andere Empfänger ausgeschlossen. Der Begriff der Presse umfasst nach dem Landespressegesetz die Herstellung von periodischen und sonstigen Druckwerken. Der Begriff des Rundfunks schließt Hörfunk und Fernsehen, nicht aber sonstige Medien ein. Eine Veröffentlichung der Daten im Internet ist daher mangels Rechtsgrundlage nicht zulässig. Das **Innenministerium** wird die Kommunen nochmals hierauf hinweisen.

1.3.4 Videoaufnahmen von Kindergartenkindern im Internet

Die Darstellung des Landesbeauftragten für den Datenschutz ist zutreffend, die rechtliche Beurteilung wird vom **Innenministerium** und der betroffenen Stadt geteilt. Letztere hat auf Veranlassung der Rechtsaufsichtsbehörde die Aufnahmen aus dem Internet entfernt.

Die Stadt merkt allerdings an, dass sie dem Landesbeauftragten für den Datenschutz im Zusammenhang mit der Beanstandung mehrere Formulierungsvorschläge für eine Einwilligungserklärung vorgelegt habe, die dieser wohl nicht als ausreichend angesehen habe. Auch habe der Landesbeauftragte für den Datenschutz leider ihrer Bitte nicht entsprochen,

die Stadt zu beraten und ihr eine datenschutzkonforme Einwilligungserklärung zukommen zu lassen.

1.5 Meldewesen - Fehler im Meldeverfahren MeldIT

Das **Innenministerium** teilt die Rechtsauffassung des Landesbeauftragten für den Datenschutz.

Die programmseitigen Fehler bei dem als Fall 1 geschilderten Sachverhalt wurden inzwischen behoben.

Die Probleme in den Fällen 2 und 3 liegen zum Teil in der Formulierung des § 29a Absatz 3 Nummer 3 des baden-württembergischen Meldegesetzes begründet. Danach ist der Abruf der Daten zulässig, wenn die beantragende Stelle den Betroffenen mindestens mit Vor- und Familiennamen sowie mit dessen früherer, gegenwärtiger oder künftiger Anschrift bezeichnet hat. Das Geburtsdatum ist als Identifizierungsmerkmal in dieser Vorschrift nicht genannt. Es ist deshalb systemseitig auch kein zwingendes Suchkriterium. Der dem Deutschen Bundestag zur Beratung vorliegende Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens sieht demgegenüber vor, dass die Erteilung einer einfachen Melderegisterauskunft nur zulässig ist, wenn die Identität der Person, über die eine Auskunft begehrt wird, aufgrund der in der Anfrage mitgeteilten Angaben über den Familiennamen, den früheren Namen, die Vornamen, das Geburtsdatum, das Geschlecht oder eine Anschrift eindeutig festgestellt werden kann. Hier wird die Notwendigkeit einer eindeutigen Identifizierung nochmals hervorgehoben und das Suchkriterium „Geburtsdatum“ ausdrücklich genannt. Zwar geht aus der Gesetzesbegründung hervor, dass eine Mindestanzahl anzugebender Suchkriterien nicht festgelegt werden soll, aber es wird unterstrichen, dass die Person durch die gemachten Angaben eindeutig identifiziert werden muss.

Um die eindeutige Identifizierung der über MeldIT abgefragten Personen sicherzustellen, wird das Innenministerium an den Softwareentwickler herantreten und gemeinsam mit den Meldebehörden nach einer Lösung für das geschilderte Problem suchen.

2. Steuerverwaltung

2.1 Datenschutzpanne beim elektronischen Lastschriftverfahren für die Kfz-Steuer

Die Ausführungen des Landesbeauftragten für den Datenschutz sind nur insofern zu korrigieren, als es sich nicht um 283.000, sondern um rund 250.000 fehlerhafte Buchungsinformationen handelte.

Richtig ist, dass den Datenempfängern Steuerdaten Dritter zur Kenntnis gebracht wurden. Das **Ministerium für Finanzen und Wirtschaft** weist jedoch darauf hin, dass die Empfänger nicht in der Lage waren, allein anhand der Steuernummer die dahinter stehende natürliche oder juristische Person zu erkennen.

2.2 Auch Steuerpflichtige haben ein Recht auf Auskunft!

Die Forderung des Landesbeauftragten für den Datenschutz, das Auskunftsrecht der Steuerpflichtigen im Besteuerungsverfahren in der Abgabenordnung zu verankern, ist berechtigt. Das **Ministerium für Finanzen und Wirtschaft** setzt sich daher auf Bundesebene für eine entsprechende Regelung ein.

Bereits unmittelbar nach dem Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03) zum Auskunftsanspruch wurde eine Regelung in der Abgabenordnung in Angriff genommen. Anfangs waren allerdings aus Sicht der Länder viele fachliche Punkte streitig. Im Vorgriff auf die gesetzliche Regelung erging daher in 2008 zunächst ein Schreiben des Bundesministeriums der Finanzen. Der Forderung des Landesbeauftragten für den Datenschutz, die baden-württembergischen Finanzämter vorab abweichend von diesem Schreiben anzuweisen, konnte nicht entsprochen werden. Eine Verwaltungsanweisung des Bundes auf dem Gebiet der Bundesauftragsverwaltung bindet die Länder faktisch. Auch hat das Bundesministerium der Finanzen die Länder unter Hinweis auf die Verpflichtung zur Bundestreue ausdrücklich darum gebeten, in diesem Punkt keine abweichenden Verwaltungsentscheidungen zu treffen.

Zwischenzeitlich liegt ein zwischen den Ländern und dem Bundesministerium der Finanzen abgestimmter Gesetzentwurf vor. Dieser wurde an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit der Bitte um Mitteilung etwaiger Ergänzungs- oder Änderungswünsche übersandt. Sobald dessen Rückmeldung vorliegt, wird das Verfahren fortgesetzt. Aufgrund des nunmehr erreichten Verfahrensstands ist jedoch in Kürze mit einer Regelung des Auskunftsanspruchs in der Abgabenordnung zu rechnen.

3. Volkszählung Zensus 2011: Ohne wesentliche Datenschutzmängel

Die Darstellung im Tätigkeitsbericht des Landesbeauftragten für den Datenschutz ist zutreffend, jedoch weist das **Ministerium für Finanzen und Wirtschaft** ergänzend auf Folgendes hin:

Die vom Landesbeauftragten für den Datenschutz geschilderten Probleme traten hauptsächlich in einer Versandtranche eines einzigen Arbeitstages auf. Diese enthielt in begrenztem Umfang Sendungen, die nicht nur einen für den Adressaten bestimmten Frage-

bogen, sondern einen weiteren Fragebogen für ein Objekt eines anderen Eigentümers enthielten.

Die Verantwortlichen im Statistischen Landesamt haben den Fehler selbst erkannt und behoben. Der Grund für den Fehler konnte unmittelbar nach Bekanntwerden und nach kurzer Recherche des beauftragten Druck- und Versanddienstleisters ermittelt werden. Der Dienstleister traf umgehend technische Vorkehrungen, um einen Wiederholungsfall auszuschließen. Zudem wurde auf Anregung der handelnden Personen die Häufigkeit der manuellen Stichproben bei der maschinellen Kuvertierung erhöht. Die gewonnenen Erkenntnisse und angeordneten Maßnahmen werden künftig - bei Vorliegen eines entsprechenden Sachverhalts - selbstverständlich auch auf andere Versandverfahren des Statistischen Landesamts übertragen.

Der Landesbeauftragte für den Datenschutz erwähnt in seinem Bericht auch das Unverständnis einiger Bürgerinnen und Bürger, die sowohl im Rahmen des Zensus 2011 als auch des Mikrozensus auskunftspflichtig waren. Hierzu ist zu sagen, dass beide Befragungen unterschiedliche Ziele verfolgen. Der Mikrozensus liefert seit 1957 mit einem umfassenden Erhebungsprogramm und einem Befragungsumfang von 1 % der Haushalte wichtige Informationen zu den jährlichen Veränderungen der wirtschaftlichen und sozialen Lage der Bevölkerung, auf die auch im Zensusjahr 2011 nicht verzichtet werden konnte. Das gesetzlich vorgegebene Erhebungsprogramm geht dabei weit über den für den Zensus 2011 vorgesehenen Fragenkatalog hinaus. Zudem wird der Mikrozensus in Deutschland gemeinsam mit der Arbeitskräftestichprobe der Europäischen Union durchgeführt. Bei einer Aussetzung des Mikrozensus hätten die vergleichsweise detaillierten Lieferverpflichtungen an die Europäische Union nicht erfüllt werden können. Im Übrigen haben sich nach den im Statistischen Landesamt vorliegenden Informationen kaum Haushalte über ihre Berichtspflichten zu beiden Erhebungen beschwert.

6. Teil: Datenschutz in der Arbeitswelt

1. Abschnitt: Gesundheitsdaten im Arbeitsverhältnis

5. Mehr Datenschutz beim Voranerkennungsverfahren für die Beihilfefähigkeit einer ambulanten psychotherapeutischen Behandlung

Die Abweichung von den Vorgaben der Verwaltungsvorschrift zur Bundesbeihilfeordnung hat das Landesamt für Besoldung und Versorgung damit begründet, dass verschiedene Gutachter bei alleiniger Angabe des Alters Zuordnungsprobleme bei späteren Folgeanträgen befürchtet und deshalb sogar ihre Gutachtertätigkeit in Frage gestellt hätten. Da sich jedoch nur wenige Gutachter so geäußert haben, hat das **Ministerium für Finanzen und Wirtschaft** das Landesamt für Besoldung und Versorgung gebeten, zukünftig nur noch das Alter der zu behandelnden Person zu nennen. Der Bitte des Landesbeauftragten für den Datenschutz ist damit Rechnung getragen.

6. Verwaltungsvorschrift zur Beihilfeverordnung - Beihilfe für berücksichtigungsfähige Angehörige

Voranzustellen ist, dass der Beihilfeanspruch originär in der Person des Beihilfeberechtigten begründet ist, basierend auf dem Dienstverhältnis eines Beamten zu seinem Dienstherrn und der hieraus resultierenden Alimentations- und Fürsorgeverpflichtung des Dienstherrn. Dies gilt sowohl für die aktive Dienstzeit des Beamten als auch für die Zeit des Ruhestandes. Aus diesem Grund kann auch die Forderung, dass berücksichtigungsfähige Angehörige über einen eigenen Beihilfeanspruch vor demjenigen geschützt werden sollen, dem sie ihren Krankenversicherungsschutz zu verdanken haben, rechtlich nicht nachvollzogen werden.

Die Bundesregelung, auf die der Landesbeauftragte für den Datenschutz verweist, räumt den Angehörigen lediglich bei Vorliegen bestimmter Voraussetzungen eine Antragsbefugnis ein, nicht jedoch einen eigenen Beihilfeanspruch (§ 51 Absatz 6 der Bundesbeihilfeverordnung). Selbst in den dort angeführten Ausnahmetatbeständen bedarf es aber der vorherigen Anhörung durch die Beihilfestelle. Überdies bedeutet die Bundesregelung nach Auffassung des **Ministeriums für Finanzen und Wirtschaft** eine erhebliche Einschränkung des dem Beihilfeberechtigten garantierten höchstpersönlichen Rechtsanspruchs (vergleiche dazu § 78 des Landesbeamtengesetzes in Verbindung mit § 1 Absatz 3 der Beihilfeverordnung). Zugleich können Konflikte um die Finanzierung und/oder Begleichung von Krankheitsaufwendungen auf diese Weise Sache der Beihilfestelle werden, obwohl diese Probleme ausschließlich dem Kreis der familienrechtlichen Beziehungen zuzurech-

nen sind und daher gegebenenfalls nach unterhaltsrechtlichen Gesichtspunkten und vor den Zivilgerichten zu lösen sind.

Das Ministerium für Finanzen und Wirtschaft hat seine Auffassung dem Landesbeauftragten für den Datenschutz inzwischen eingehend schriftlich dargelegt.

9. Teil: Technik und Medien

3. Abschied von der GEZ? Der 15. Rundfunkänderungsstaatsvertrag

Die Vorbereitungen für die Evaluierung des 15. Rundfunkänderungsstaatsvertrags sind im Länderkreis bereits angelaufen. Das **Staatsministerium** setzt sich in diesem Zusammenhang dafür ein, dass in die Evaluierung ausdrücklich auch Aspekte des Datenschutzes einbezogen werden. Auch hat es sich bereits zu Beginn des Jahres 2012 in einem Appell im Sinne der vom Landesbeauftragten für den Datenschutz angesprochenen Entschließung des Landtags (LT-Drucksache 15/671, Nummer 1) an die öffentlich-rechtlichen Rundfunkanstalten gewandt.

Im Übrigen wird das Staatsministerium dem Landtag bis spätestens 12. April 2012 darüber berichten, welche Maßnahmen im Bemühen um die in der Entschließung angesprochenen Aspekte zur Stärkung des Datenschutzes bei der Erhebung der Rundfunkbeiträge bis dahin ergriffen wurden und welcher Fortgang sich abzeichnet.