

## **Beschlussempfehlung und Bericht**

### **des Ständigen Ausschusses**

#### **zu der Mitteilung des Landesbeauftragten für den Datenschutz vom 17. Januar 2014 – Drucksache 15/4600**

### **31. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2012/2013**

#### Beschlussempfehlung

Der Landtag wolle beschließen,

von der Mitteilung des Landesbeauftragten für den Datenschutz vom 17. Januar 2014 – Drucksache 15/4600 – und der vom Innenministerium hierzu mit Schreiben vom 16. April 2014 vorgelegten Stellungnahme der Landesregierung (siehe Anlage zum Ausschussbericht) Kenntnis zu nehmen.

05. 06. 2014

Der Berichterstatter:

Sascha Binder

Der Vorsitzende:

Dr. Stefan Scheffold

#### Bericht

Der Ständige Ausschuss beriet die Mitteilung des Landesbeauftragten für den Datenschutz vom 17. Januar 2014, Drucksache 15/4600, in seiner 32. Sitzung am 5. Juni 2014. Zur Beratung lag ferner das Schreiben des Innenministeriums vom 16. April 2014 (*Anlage*) mit der Stellungnahme der Landesregierung zum 31. Tätigkeitsbericht vor.

Der Landesbeauftragte für den Datenschutz legte dar, er bedanke sich für die Gelegenheit, seinen 31. Tätigkeitsbericht auch im Ständigen Ausschuss vorzustellen, sowie für die grafische Gestaltung der Drucksache mit diesem Tätigkeitsbericht.

Ausgegeben: 25.06.2014

*Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: [www.landtag-bw.de/Dokumente](http://www.landtag-bw.de/Dokumente)*

*Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.*

Anschließend führte er aus, seit genau einem Jahr gebe es immer wieder neue Enthüllungen zum Thema NSA, und es dränge sich der Eindruck auf, dass es noch weitere Enthüllungen geben werde. Diese Thematik beschäftige viele Verantwortliche weltweit und natürlich auch die Datenschützer. Vielfach mache sich im Übrigen auch ein Gefühl der Machtlosigkeit und auch der Ratlosigkeit breit. Auch die deutsche Wirtschaft sei in höchstem Maße beunruhigt über die bekannt gewordenen Vorgänge; denn die Erkenntnisse der Geheimdienste würden auch für Zwecke der Wirtschaftsspionage genutzt. Es falle auf, dass sich die Bundesregierung mit dem Umgang mit dieser Problematik relativ schwer tue.

Am Vortag habe der Generalbundesanwalt bekannt gegeben, dass er wegen der Abhörmaßnahmen gegen das Mobiltelefon der Bundeskanzlerin ein Ermittlungsverfahren einzuleiten beabsichtige; in diesem Zusammenhang dränge sich die Frage auf, wie mit Spähangriffen auf andere Mobiltelefone in Deutschland umgegangen werde, die wie jedes Wirtschaftsunternehmen ebenfalls jederzeit zum Zielobjekt einer Überwachungsmaßnahme werden könnten. Die vereinzelt politischen Forderungen, die zwischenzeitlich aufgekommen seien, seien im Sande verlaufen; beispielsweise habe die Europäische Kommission die Evaluierung des Safe-Harbor-Abkommens noch nicht abgeschlossen, und erschwerend komme hinzu, dass nach den Europawahlen die Europäische Kommission neu gebildet werden müsse. Die Einleitung des erwähnten Ermittlungsverfahrens sei jedoch ein wichtiges Signal; denn dies zeige, dass Spionage auch dann kein Kavaliärsdelikt sei, wenn sie sich gegen vermeintliche Freunde richte.

Ein weiterer Abschnitt im vorliegenden Tätigkeitsbericht sei dem Thema „Big Data“ gewidmet. Denn dieses Thema sei sowohl für die Wirtschaft als auch für den Datenschutz wichtig. In diesen Bereich fielen die „Smart-TV“ genannten intelligenten Fernseher, die von den Medien bereits als „Spione im Wohnzimmer“ bezeichnet worden seien. Denn sie seien in der Lage, Informationen zur Senderauswahl und zum sonstigen Verhalten der Nutzer an den Gerätehersteller, an den Sender sowie auch an Dritte wie beispielsweise Werbepartner zu übermitteln. Diese Geräte seien ein Beispiel dafür, dass das Internet in immer mehr technische Geräte, die im Alltag genutzt würden, Einzug halte. Auch immer mehr Stromzähler und Kraftfahrzeuge seien permanent mit dem Internet verbunden. Irgendwann würden auch Kühlschränke selbsttätig Nachschub bestellen, wenn sich herausstelle, dass ein Lebensmittel, welches sich im Normalfall darin befinde, ausgegangen sei.

Zur europäischen Datenschutzreform habe es in den letzten zwei Monaten keine Neuigkeiten mehr gegeben. Die letzte Meldung zu diesem Thema habe gelautet, dass das Europäische Parlament in erster Lesung die Verhandlungslinie des federführenden LIBE-Ausschusses gebilligt habe. Berichterstatter für das große Reformwerk sei der deutsche Abgeordnete Jan Philipp Albrecht von den Grünen. Es bleibe zu hoffen, dass er das Ziel der europäischen Datenschutzreform wie bisher weiterverfolge.

Im Bereich Inneres sei nach wie vor am sogenannten Mitzieheffekt Kritik zu üben; er werde auch weiterhin ein Gegner des Mitzieheffekts bleiben. Dieser Effekt gehe darauf zurück, dass die Polizei nach § 38 des Polizeigesetzes unter bestimmten Voraussetzungen personenbezogene Daten, die ihr im Rahmen von Ermittlungsverfahren bekannt geworden seien, zur vorbeugenden Bekämpfung von Straftaten speichern dürfe, dass jedoch die Prüffristen, ob eine weitere Speicherung erforderlich sei, spätestens mit Ablauf des Jahres begännen, in dem das letzte Ereignis erfasst worden sei, das zur Speicherung der personenbezogenen Daten geführt habe. Deshalb hätten spätere Eintragungen zur Folge, dass zulässigerweise auch gespeicherte Daten aus früheren Ermittlungsverfahren weiterhin gespeichert bleiben dürften, selbst wenn das Aussonderungsprüfdatum früherer Erkenntnisse abgelaufen wäre. Dieser Mitzieheffekt führe vielfach zu einer langen Speicherung von Alt- bis Uraltvorgängen. Bedauerlicherweise sei das Innenministerium nicht bereit, analog zur Vorgehensweise in Niedersachsen feste Löschfristen einzuführen. Aus seiner Sicht stünde es dem Land Baden-Württemberg gut an, eine entsprechende Veränderung herbeizuführen.

Auch hinsichtlich der Durchführungsverordnung zum Polizeigesetz gebe es noch Gesprächsbedarf mit dem Innenministerium; er verweise auf seine Empfehlung, dass zur Vorbeugung gegen unzulässige Datenabfragen jeder Zugriff auf die polizeilichen Auskunftssysteme – statt wie bisher nur jeder 50. Abruf – protokolliert werden solle und die Protokolldaten statt wie bisher nur für ein halbes Jahr bis zu einem Jahr gespeichert bleiben sollten.

Zu Abschnitt 2.1.4 – Der Sinneswandel im Polizeirecht – sei anzumerken, er halte es für unverständlich, dass sich die derzeit Verantwortlichen nicht mehr an alles erinnern könnten, was sie seinerzeit im Zusammenhang mit der Einfügung des § 38 Absatz 2 PolG geäußert hätten. Er halte diese Regelung nach wie vor für ein Argernis. Denn dafür, für die polizeiliche Kriminalstatistik Angaben zu erhalten, müssten nicht alle Einzelfälle personenscharf gespeichert werden, und sei es auch nur für zwei Jahre.

Zum Abschnitt 2.2.4 – Zuverlässigkeitsprüfungen in allen Varianten – sei anzumerken, das Innenministerium sei nach wie vor der Auffassung, dass die Einwilligungslösung für Zuverlässigkeitsprüfungen bei Veranstaltungen, die umfangreiche Sicherheitsmaßnahmen zum Schutz der Verfassungsorgane von Bund und Ländern erforderten, richtig und vertretbar sei. Er plädiere nach wie vor dafür, eine gesetzliche Grundlage für Zuverlässigkeitsprüfungen bei derartigen Veranstaltungen zu schaffen, und er halte es für bemerkenswert, dass das Staatsministerium eine solche Regelung prüfen wolle.

Er habe zur Kenntnis genommen, dass das Innenministerium angedeutet habe, prüfen zu wollen, ob es für die Speicherung der Ergebnisse und Unterlagen der Zuverlässigkeitsüberprüfung von Bewerberinnen und Bewerbern für den Polizeivollzugsdienst ebenfalls einer expliziten Einwilligung oder einer gesetzlichen Änderung bedürfe. Er halte es allerdings für bemerkenswert, dass dies nicht bereits früher geschehen sei.

Zum Thema Waffenrecht werde im Tätigkeitsbericht angekündigt, dass seine Dienststelle in den nächsten Monaten kontrollieren werde, inwieweit die eingerichteten automatisierten Abrufverfahren von den Waffenbehörden in Übereinstimmung mit den gesetzlichen Regelungen genutzt würden. Diese Kontrollen seien bereits angelaufen; bei Bedarf könne er darüber berichten.

Seine Dienststelle habe ferner dazu beigetragen, dass das Interessenbekundungsverfahren im Rahmen der Polizeistrukturreform datenschutzkonform ablaufe. Dabei habe es eine konstruktive Zusammenarbeit gegeben. Seine Dienststelle erwarte im Übrigen von der Einrichtung von Rechts- und Datenschutzreferaten bei den größeren Polizeipräsidien einen gewissen Schub zugunsten des Datenschutzes. Dort sollte mehr und fachlich noch qualifizierter für den Datenschutz gearbeitet werden; den behördlichen Datenschutzbeauftragten werde derzeit bedauerlicherweise vielfach noch zu wenig Zeit für die Erfüllung ihrer Aufgaben eingeräumt, und er hoffe, dass in den neuen Polizeipräsidien die notwendigen personellen Kapazitäten für den Datenschutz zur Verfügung gestellt würden.

Zum Thema Verfassungsschutzgesetz gebe es nach wie vor Meinungsverschiedenheiten zwischen seiner Dienststelle und dem Innenministerium. Aus seiner Sicht sei es schade, dass der Verfassungsminister des Landes einräumen müsse, dass ein Gesetz, das aus seinem Haus stamme, verfassungswidrig sei. Er würde es begrüßen, wenn der bereits seit zehn Jahren bestehende ungute Zustand möglichst bald beendet würde und möglichst noch in der laufenden Legislaturperiode das Gesetz verfassungskonform ausgestaltet würde.

Zum Thema Antiterrordateigesetz verweise er auf seine Ausführungen im Tätigkeitsbericht. Zwischenzeitlich sei der Gesetzentwurf für ein neues Antiterrordateigesetz in den Bundesrat eingebracht worden. Das Bundesverfassungsgericht habe im Übrigen in seiner entsprechenden Entscheidung im vergangenen Jahr eine stärkere Kontrolle der Antiterrordatei angemahnt und eine bestimmte Kontrolldichte eingefordert, was sicher auch für die Rechtsextremismusedatei gelte. Dies sei im derzeitigen Programm jedoch in dieser Form noch nicht vorgesehen; er sei auch dagegen, Aufgaben an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu delegieren und sie zu bitten, im Wege der Amtshilfe tätig zu

werden. Denn dies würde bedeuten, dass Landesbehörden durch Bundesbehörden kontrolliert würden, was nicht gewollt sein könne. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit prüfe das Bundeskriminalamt und versuche, die dortigen Protokolldaten zu prüfen, doch die Auswertung und vor allem die gezielte Nachschau und die Überprüfung des sogenannten Aktenrückhalts sollten in der Zuständigkeit des Landesbeauftragten für den Datenschutz und nicht der Bundesbeauftragten liegen.

Hinsichtlich des nachrichtendienstlichen Informationssystems NADIS liefen derzeit Gespräche mit dem Innenministerium und dem Landesamt für Verfassungsschutz. Seine Dienststelle vertrete im Gegensatz zum Landesamt für Verfassungsschutz die Rechtsauffassung, dass die Dateiführung nicht den Amtshilferegelungen des § 1 Absatz 3 des Bundesverfassungsschutzgesetzes unterliege, sondern dass es sich um eine Auftragsdatenverarbeitung handle.

Zu Kapitel 3 – Justiz – verweise er auf den Tätigkeitsbericht. Seiner Dienststelle liege es fern, sich in Sachen Quellen-TKÜ in die richterliche Unabhängigkeit einzumischen. Die Zusammenarbeit mit dem Justizministerium sei im Berichtszeitraum sehr erfreulich gewesen. Dies habe sich nicht zuletzt daran gezeigt, dass ein sehr fähiger Staatsanwalt an seine Dienststelle abgeordnet worden sei; das Justizministerium habe auch dafür gesorgt, dass die Juristenausbildungs- und Prüfungsordnung in der Weise geändert worden sei, dass in seiner Dienststelle nicht nur die Wahlstation, sondern auch die Verwaltungsstation der Referendare absolviert werden könne.

In letzter Zeit habe es immer wieder Nachfragen mit dem Ziel gegeben, in seiner Dienststelle mitarbeiten zu können; zuletzt sei in seiner Dienststelle ein Student der Hochschule Darmstadt als Praktikant tätig gewesen. Er bedanke sich in diesem Zusammenhang bei dem Beschäftigten seiner Dienststelle, der sich mit der Frage der Ausbildung von Referendaren befasse. Es zeige sich, dass die Themen Datenschutz und Datensicherheit für gute Nachwuchskräfte immer wichtiger würden und auch für den späteren Beruf interessante Betätigungsfelder darstellten.

Zu Kapitel 5 – Kommunales – könne konstatiert werden, dass es an vielen Stellen eine gute und konstruktive Zusammenarbeit mit der kommunalen Ebene gebe. Seine Dienststelle habe hierzu Kontakt mit den kommunalen Landesverbänden aufgenommen, kommunale Praktiker einbezogen und beispielsweise eine Handreichung für die Veröffentlichung von Bildern im Internet herausgegeben. Auch die Thematik „Übertragung von Gemeinderatssitzungen im Internet“ sei gemeinsam bearbeitet worden. Dazu habe es in Konstanz und in Seelbach je ein Pilotprojekt gegeben. In Konstanz habe Anfang des Jahres die erste Gemeinderatssitzung mit Internetübertragung stattgefunden, und zwar über eine Podcast-Lösung. Dabei werde die Sitzung aufgezeichnet, und die Aufnahmen würden gegliedert nach Tagesordnungspunkten zum Abruf bereitgestellt, jedoch erst am Folgetag, was die Möglichkeit biete, die einzelnen Beiträge vor der Bereitstellung zu sichten und gegebenenfalls zu bearbeiten, um etwaige datenschutzrechtliche Probleme zu vermeiden.

Seelbach setze auf eine um 90 Sekunden zeitversetzte Übertragung, was den Nachteil habe, dass für eventuell notwendige Eingriffe nur sehr wenig Zeit zur Verfügung stehe.

Gemeinsam mit Kommunen seien auch Fortbildungen geplant; beispielsweise habe sich die Stadtverwaltung von Tübingen dafür interessiert. Im Herbst werde seine Dienststelle in Karlsruhe tätig, und auch eine Fortbildungsveranstaltung in Reutlingen sei im Gespräch. Mit den vorhandenen personellen Kapazitäten könnten jedoch maximal zwei Veranstaltungen pro Jahr bewältigt werden; gleichwohl seien solche Veranstaltungen sinnvoll, um strukturelle Verbesserungen des Datenschutzes zu erreichen, statt im Wesentlichen auf Datenschutzbeschwerden zu reagieren.

Das Innenministerium schließe zwar aus der Tatsache, dass nur vier Beanstandungen ausgesprochen worden seien, von denen drei eher formal und weniger inhaltlich gewesen seien, dass es mit dem Datenschutz in der öffentlichen Verwaltung zum Besten stehe. Doch der Bedarf nach Beratungen in Fragen der IT-Sicherheit sei gerade im kommunalen Bereich groß. Er weise in diesem Zusammenhang da-

rauf hin, dass es immer mehr IT-Verfahren an der Schnittstelle zwischen Verwaltung und Bürger gebe, soziale Netzwerke auch durch öffentliche Stellen immer stärker genutzt würden und immer mehr Geräte sowohl privat als auch für dienstliche Zwecke genutzt würden. Angesichts dieser Entwicklungen seien sowohl die Datenschutzbeauftragten als auch die IT-Sicherheitsbeauftragten in allen Verwaltungen auf das Höchste gefordert. Dies werde sich in nächster Zeit mit Sicherheit nicht ändern, weil das Internet den ganzen Lebensalltag und das ganze Umfeld durchdringe und weil immer mehr Möglichkeiten bestünden, auf das individuelle Verhalten der Menschen zu schließen. Wenn beispielsweise bei Müllgebühren oder Gebühren für die Straßenbenutzung eine möglichst hohe Gerechtigkeit angestrebt werde, werde die Abrechnung meist personenscharf, und dann seien Datenschutzaspekte zu beachten.

Zusammenfassend sei feststellbar, im kommunalen Bereich gebe es keinen Anlass, gewissermaßen Entwarnung zu geben; die Herausforderungen nähmen sogar eher noch zu.

Weiter erklärte er, den Kommunen sei es unbenommen, eine Steuer auf Gästeübernachtungen zu erheben. Dazu müsse jedoch in jedem Einzelfall unterschieden werden, ob sich ein Gast zu beruflichen oder zu privaten Zwecken in der Gemeinde aufhalte, und dieser Aufwand sei unangemessen hoch. Zum Thema Bettensteuer hätten Freiburger Hoteliers im Übrigen ein Musterverfahren vor dem VGH angestrengt; es bleibe abzuwarten, wie es ausgehe. Er gehe davon aus, dass es letztlich auf die Frage hinauslaufe, ob es abgabenrechtlich zulässig sei, Hoteliers zu verpflichten, bei den Gästen abzufragen, ob eine Übernachtung beruflichen Zwecken diene oder nicht.

In diesem Zusammenhang sei anzumerken, dass das neue Bundesmeldegesetz Änderungen bei der Hotelmeldepflicht mit sich bringen werde. Ein Fall in Ulm, bei dem ein Hotelgast ins Visier der Polizei geraten sei, weil er den gleichen Namen und den gleichen Geburtstag wie ein gesuchter Straftäter gehabt habe, habe gezeigt, dass es ganz unterschiedliche Vorgehensweisen des Polizeivollzugsdienstes gebe. Während es Polizeidienststellen gebe, die täglich und möglichst von allen Hotels eine Übermittlung der Hotelmeldescheine verlangten, gebe es andere Polizeidienststellen, die nur gelegentlich oder anlassbezogen Auskunft verlangten, wer in einem Hotel gemeldet sei. Das Bundesmeldegesetz werde sicherlich eine gewisse Vereinheitlichung bewirken.

Ausländische Hotelgäste müssten im Gegensatz zu inländischen im Übrigen immer ein Personaldokument vorlegen. Diese Ungleichbehandlung halte er für eine Diskriminierung, an der sich durch das neue Bundesmeldegesetz auch nichts ändern werde. Er würde sich eine Gleichbehandlung wünschen; denn wenn es aus Sicherheitsgründen wichtig sei, reisende Täter aufzuspüren, dann sollte die Identität im Hotel generell nachgewiesen werden müssen. Wenn es weniger wichtig sei, einen solchen Nachweis zu fordern, sollte auch bei ausländischen Gästen darauf verzichtet werden.

Zum Kapitel 6 – Verkehr – sei im Tätigkeitsbericht im Wesentlichen auf die technische Entwicklung und verschiedene Projekte hingewiesen worden, die seine Dienststelle im Berichtszeitraum beschäftigt hätten.

Zu den Kapiteln 7 und 8 des Tätigkeitsberichts habe es ausweislich der Stellungnahme der Landesregierung zum Tätigkeitsbericht nur relativ wenige Dissenspunkte gegeben. Ihm sei das Thema „Datenschutz an Pflegestützpunkten und Pflegeeinrichtungen“ wichtig, über das seine Dienststelle seit Jahren mit der beim Sozialministerium angesiedelten Landesarbeitsgemeinschaft Pflegestützpunkte e. V. (LAG) im Gespräch sei. Aus seiner Sicht sollte die LAG bzw. das Sozialministerium gegenüber den Trägern der Pflegestützpunkte noch einmal klarstellen, wer verantwortliche Stelle im datenschutzrechtlichen Sinne sei. Darum habe er bereits im vergangenen Jahr gebeten, doch vor Ort erhalte er immer wieder ganz unterschiedliche Antworten auf entsprechende Fragen. In dieser Hinsicht scheine ihm auf der Ebene der Landratsämter und bei den Pflegeeinrichtungen noch eine gewisse Verunsicherung zu bestehen. Auch hinsichtlich der Zusatzvereinbarungen sollte es eine stärkere fachliche Koordination durch das Sozialministerium geben. Er bitte die Vertreter des Innenministeriums, diesen Wunsch an das Sozialministerium weiterzugeben.

Wichtig sei aus seiner Sicht auch die Frage, ob das Sozialamt, wenn es Leistungen auszahlen solle, das Gutachten des medizinischen Dienstes der Krankenkassen, der den Pflegebedarf geprüft habe, benötige. Aus Sicht seiner Dienststelle reiche es aus, wenn sich das Sozialamt mit den Ergebnissen dieses Gutachtens begnüge; gleichwohl beharre das Sozialministerium jedoch nach wie vor auf der Auffassung, das Sozialamt habe grundsätzlich das Recht, das komplette MDK-Gutachten zu bekommen, in dem auch viele andere Angaben enthalten seien, beispielsweise auch zu psychischen Auffälligkeiten. Für die Arbeit werde jedoch nur das Ergebnis benötigt, wie ihm einige Sozialämter sogar bestätigt hätten.

Er weise in diesem Zusammenhang darauf hin, dass in Bayern auf die Übermittlung des kompletten Gutachtens verzichtet werde; dort genüge die Mitteilung des Ergebnisses. Er würde sich vom Sozialministerium etwas mehr Datensparsamkeit wünschen.

Das Kapitel 8 im Tätigkeitsbericht befasse sich mit Datenschutz an Kindertageseinrichtungen und Schulen. Ihm sei die Feststellung wichtig, dass sich die Zusammenarbeit zwischen seiner Dienststelle und dem Ministerium für Kultus, Jugend und Sport gut entwickelt habe. Von „Notstandsgebieten“ würde er zwischenzeitlich nicht mehr sprechen wollen. Diese positive Entwicklung sei auch ein Ergebnis eines gewissen Personalaustauschs; er weise in diesem Zusammenhang darauf hin, dass ein früherer Angehöriger seiner Dienststelle nunmehr im Ministerium für Kultus, Jugend und Sport tätig sei und sich dort u. a. mit datenschutzrechtlichen Fragen befasse. Umgekehrt sei ein Berufsschullehrer aus dem Kultusbereich an seine Dienststelle abgeordnet worden, der im Bereich der Lehrerfortbildung in Datenschutzfragen tätig sei.

Beim Thema „Landeseinheitliche Bildungsnummer“ gebe es noch keinen Konsens zwischen ihm und dem Ministerium für Kultus, Jugend und Sport. Er persönlich sei von der Notwendigkeit einer landeseinheitlichen Bildungsnummer nicht überzeugt; denn der Verweis auf Schulwechsel oder Mehrfachbewerbungen von Schülern reiche ihm als Rechtfertigungsgrundlage für eine solche Nummer nicht aus. Die Skepsis der Datenschützer gegenüber einheitlichen Bildungsnummern gründe sich im Übrigen auf die Rechtsprechung des Bundesverfassungsgerichts, in der ein Verbot der Totalerhebung der Bevölkerung zum Wesenskern der verfassungsrechtlichen Identität des Landes erhoben worden sei. Es gebe bereits genügend Identifikationsnummern, sodass es keiner weiteren bedürfe, die vielleicht dazu benutzt werden könnten, Bildungskarrieren von Kindern vom Kindergarten bis zum Hochschulabschluss und womöglich noch darüber hinaus zu verfolgen. Er würde sich eine politische Festlegung wünschen, ob so etwas gewollt sei, auch wenn es rechtlich und technisch möglich wäre.

Wichtiger als eine Bildungsnummer wäre aus seiner Sicht eine frühzeitige Verankerung der Medienbildung in den Bildungsplänen und im Schulalltag. Vor allem sollte die Medienbildung früher einsetzen, als es derzeit vorgesehen sei. Neulich habe er an einer Sitzung des Beirats zur Bildungsplanreform teilgenommen, und dort sei wieder einmal deutlich geworden, wie darum gekämpft werde, Inhalte in den einzelnen Jahrgangsstufen unterzubringen, doch die Medienbildung sei mittlerweile eine der sogenannten Leitperspektiven. Für besonders eindrucksvoll halte er die Aussage der Vertreterin des Landesschülerbeirats bei dieser Veranstaltung, ihre Medienbildung habe sie praktisch nur zu Hause und im Freundeskreis erhalten, nicht jedoch in der Schule, und nach ihrer Feststellung seien die Lehrerinnen und Lehrer vielfach eher technikfeindlich eingestellt gewesen. Angesichts dessen, dass in den Klassenstufen drei und vier, also mit acht oder neun Jahren, mindestens die Hälfte der Kinder bereits Umgang mit dem Internet habe, komme die Schule mit Medienbildung in der Klassenstufe fünf recht spät. Er wäre dankbar, wenn die Ausschussmitglieder auf die Bildungspolitik im Landtag mit dem Ziel einwirken könnten, dass die Medienbildung an der Schule früher einsetze als in der Klassenstufe fünf, also bereits in der Grundschule.

Weiter führte er aus, für seine Dienststelle sei das Thema „Datenschutz in der Wirtschaft“ außerordentlich wichtig und binde auch entsprechend viele Kapazitäten. Ein wichtiger Aspekt in diesem Zusammenhang sei die Arbeit von Auskunfteien. In Baden-Württemberg, konkret in Baden-Baden, habe die zweitgrößte Auskunftei Deutschlands ihren Sitz. Damit sei aus seiner Dienststelle eine Sachbearbeiterin

fast komplett und ein Referent fast zur Hälfte der Arbeitszeit befasst. Gerade zu den Auskunfteien gebe es immer wieder Beschwerden. Wenn der Bundesgesetzgeber jedoch keine schärferen Regeln einführe, werde sich an der „Kaffeesatzleserei“ der Auskunfteien nichts ändern; rechtlich handle es sich um Meinungsäußerungen, sodass die Einflussmöglichkeiten begrenzt seien.

Das Kapitel 11 – Technik und Medien – im Tätigkeitsbericht befasse sich u. a. mit dem Thema Videoüberwachung. Diese habe sich zwischenzeitlich zu einem Massenphänomen entwickelt, weil für relativ wenig Geld ausgereifte Technik zur Verfügung stehe. Seine Dienststelle erhalte täglich mehrere Beschwerden von Menschen, die sich durch Videoüberwachungsmaßnahmen belästigt fühlten. Überwiegend gehe es dabei um Überwachungseinrichtungen in der Nachbarschaft. Doch auch die Videoüberwachung in Geschäften, Gaststätten und hin und wieder auch am Arbeitsplatz sei vielfach Anlass für eine Beschwerde. Im März 2014 hätten die Datenschutzaufsichtsbehörden der Länder im nicht öffentlichen Bereich, der sogenannte Düsseldorfer Kreis, einen Beschluss zu Dashcams, also Kameras auf dem Armaturenbrett von Kraftfahrzeugen, gefasst. Für diese Dashcams werde mit dem Argument geworben, dass damit etwaige Unfälle dokumentiert werden könnten. Die Datenschutzaufsichtsbehörden hätten jedoch erklärt, diese Kameras seien unzulässig. Es müsse sicher noch vor Gericht ausgetestet werden, wie weit diese Rechtsauffassung trage; in Bayern werde es höchstwahrscheinlich demnächst ein Verfahren vor einem Verwaltungsgericht geben, weil die bayerische Aufsichtsbehörde einen Bescheid gegenüber einem Autofahrer, was den Einsatz einer Dashcam angehe, erlassen habe.

Aus seiner Sicht passe es nicht zusammen, immer wieder gegen stationäre Kameras, die an Häusern angebracht seien, einzuschreiten, weil sie auch den öffentlichen Verkehrsraum in der Umgebung erfassten, den Einsatz von Kameras in Fahrzeugen hingegen unkommentiert zu lassen. Deshalb wäre es konsequent, bei Dashcams zu einer ähnlichen Bewertung zu kommen. Ob dies letztlich trage, werde sich zeigen.

Ferner seien Wildkameras erwähnenswert, die auch in der Presse bereits thematisiert worden seien. Auch andere Datenschutzbeauftragte hätten sich zu diesem Thema bereits pointiert geäußert. Seine Dienststelle sei zu dieser Thematik im Gespräch mit dem Ministerium für Ländlichen Raum und Verbraucherschutz und vertrete die Auffassung, dass der Einsatz von Wildkameras durch Förster und Jäger nach Möglichkeit untersagt werden sollte. Er habe Verständnis, wenn Jäger derartige Kameras als praktisch ansähen, um sich einen Überblick über den Wildbestand im Revier zu verschaffen. Doch nicht alles, was praktisch sei, müsse zugelassen werden. Er gehe davon aus, dass Übereinstimmung im Ausschuss darüber bestehe, dass der Wald auch in Zukunft den Menschen ermöglichen sollte, sich unbeobachtet zu erholen. Niemand sollte im Wald Gefahr laufen, unbemerkt abgelichtet zu werden.

Der Innenminister lege dar, der vorliegende 31. Tätigkeitsbericht sei nicht nur hinsichtlich der Darstellung und Aufbereitung anders als die vorangegangenen, sondern er sei auch schlanker und zeige nach Auffassung der Landesregierung und auch nach seiner persönlichen Auffassung positive Entwicklungen auf. Während im Bereich der Wirtschaft und im privaten Bereich zu beobachten sei, dass die Zahl der Datenschutzbeschwerden immer weiter wachse, stelle er fest, dass die Zahl der Datenschutzbeschwerden von Bürgerinnen und Bürgern, was die öffentliche Verwaltung angehe, zurückgehe, und dies sei grundsätzlich positiv. Er schließe daraus allerdings nicht, dass es im öffentlichen Bereich in Datenschutzfragen keine Problem und keinen Handlungsbedarf mehr gäbe. Aus seiner Sicht zeige die Entwicklung jedoch, dass die präventiven Maßnahmen sowohl des Landesbeauftragten für den Datenschutz als auch der öffentlichen Verwaltung und der politischen Entscheidungsträger durchaus Wirkung zeigten und deshalb, auch wenn sie Geld kosteten, sinnvoll seien. Es gebe nach wie vor einen hohen Beratungs- und Informationsbedarf, was sich in vermehrten Anfragen beim Landesbeauftragten für den Datenschutz niederschlage. Es gelinge also offenbar, die Mitarbeiterinnen und Mitarbeiter in der öffentlichen Verwaltung besser als in der Vergangenheit für Datenschutzfragen zu sensibilisieren. Dies sei sehr gut; denn der Mensch spiele in Datenschutzfragen eine große Rolle. Er habe nie die Absicht gehabt, beschwichtigend zu wirken, sehe jedoch, dass die präventiven Maßnahmen offensichtlich Wirkung zeigten.

In diesem Zusammenhang sei darauf hinzuweisen, dass der IT-Planungsrat vor etwa einem Jahr eine für den Bund und für die Länder verbindliche Informationssicherheitsleitlinie beschlossen habe. Derzeit laufe der Umsetzungsprozess, beispielsweise durch die Einrichtung einer Arbeitsgruppe des IT-Planungsrats der Informationssicherheitsbeauftragten des Bundes und der Länder. Ferner gehe es um Fortbildungsmaßnahmen für die Beschäftigten in der öffentlichen Verwaltung und die erhöhte Sensibilisierung der Beschäftigten für den Datenschutz. Baden-Württemberg greife auch aktiv Angebote, die an anderer Stelle gemacht würden, auf; er weise darauf hin, dass die Bundesakademie für öffentliche Verwaltung ein sehr gutes Projekt gestartet habe. In diesem Zusammenhang würden unter dem Titel „Die Hacker kommen“ Informationsveranstaltungen organisiert. Im September des vergangenen Jahres habe in Stuttgart eine solche Veranstaltung stattgefunden, die auf außerordentlich positive Resonanz gestoßen sei. Deshalb sei vorgesehen, im laufenden Jahr mehrere solcher Veranstaltungen im Land durchzuführen, und zwar sowohl auf der Ebene der Ministerien als auch auf der Ebene der Regierungspräsidien, um auch eine Verbreitung in die Fläche hinein zu bewirken.

Es gebe in der Tat noch einiges zu tun, insbesondere auch, was EU-rechtliche Datenschutzregelungen anlange. Im Übrigen habe sich das Europäische Parlament im März in erster Lesung mit der Datenschutzgrundverordnung befasst, die durchaus Positives enthalte. Die Landesregierung habe seinerzeit deutlich gemacht, dass diese EU-rechtlichen Regelungen nicht dazu führen dürften, dass Datenschutzstandards auf der Ebene von Bund und Ländern abgesenkt würden.

Aus den genannten Gründen ziehe er aus dem vorliegenden Tätigkeitsbericht ein insgesamt positives Resümee. Er freue sich, dass der Landesbeauftragte für den Datenschutz in diesem Tätigkeitsbericht auch die Polizeistrukturereform erwähnt habe. Auch im Tätigkeitsbericht werde jedoch deutlich, dass eine so gewaltige Veränderung im Apparat der Polizei zwar große datenschutzrechtliche Problematiken aufgeworfen habe, dass das Innenministerium dieser Verantwortung jedoch gerecht geworden sei. Die Polizeistrukturereform habe im Übrigen den positiven Nebeneffekt gehabt, dass die Grundlagen der Personalstammdaten, die bisher nicht konsistent gewesen seien, aktualisiert worden seien, was auch zu einer verbesserten Datensicherheit beigetragen habe. Er lege auch Wert auf die Feststellung, dass die Themenbereiche Recht und Datenschutz in den Polizeipräsidien auf der Leitungsebene platziert worden seien, um zu unterstreichen, dass das Innenministerium dem Datenschutz und der Datensicherheit auch in den Reihen der Polizei einen hohen Stellenwert einräume.

Abschließend teile er mit, im Landesamt für Verfassungsschutz seien insgesamt rund 340 Beschäftigte tätig, und der dortige behördliche Datenschutzbeauftragte sei zu rund 90 % und damit nahezu vollständig für diese Tätigkeit freigestellt, auch um deutlich zu machen, dass es sich aus Sicht des Innenministeriums um eine wichtige Funktion handle.

Der Landesbeauftragte für den Datenschutz äußerte, zu den neuen Datenschutzbeauftragten der Polizeipräsidien sei noch anzumerken, dass vom 7. bis 9. Juli 2014 in Wertheim ein erstes Treffen dieser Datenschutzbeauftragten stattfinden werde, an dem auch er sowie weitere Beschäftigte seiner Dienststelle teilnahmen. Er sei an weiterhin guten Kontakten interessiert.

Ein Abgeordneter der CDU brachte vor, er bedanke sich beim Landesbeauftragten für den Datenschutz und allen in dessen Dienststelle Beschäftigten für ihre umfassende Tätigkeit. Der Datenschutz sei beim Landesbeauftragten für den Datenschutz in guten Händen. Neben der Kontrolle sei auch die Beratung wichtig; dies gelte insbesondere für den kommunalen Sektor.

Seine Fraktion und auch die Landesregierung stimmten in vielen Punkten mit dem Landesbeauftragten für den Datenschutz überein; ihm falle jedoch auf, dass es zum Innenministerium immer wieder gewisse Differenzen gebe. Dies sei jedoch auch früher so gewesen.

Zum Thema Vorratsdatenspeicherung legte er dar, er sei dem Innenministerium dankbar für seine klare Haltung zu diesem Thema. Seine Fraktion stimme mit dem Innenministerium darin überein, dass die derzeitige ungute Situation verändert werden müsse.



Weiter brachte er vor, insgesamt sei in Datenschutzfragen bereits vieles erreicht worden. Es müsse immer auch gründlich abgewogen werden zwischen den Sicherheitsinteressen des Landes und den Persönlichkeitsrechten der Bürgerinnen und Bürger. Er bedanke sich beim Landesbeauftragten für den Datenschutz für den vorliegenden Tätigkeitsbericht; es sei erfreulich, dass immer wieder ein Dialog mit ihm möglich sei.

Eine Abgeordnete der SPD führte aus, auch sie bedanke sich namens ihrer Fraktion für den vorliegenden Tätigkeitsbericht. Es bleibe abzuwarten, wie das europäische Datenschutzrecht weiterentwickelt werde; denn die Landespolitik könne ohne entsprechende europarechtliche Regelungen keinen umfassenden Datenschutz gewährleisten. Sie habe erfreut zur Kenntnis genommen, dass der Datenschutz auch im Rahmen des Interessenbekundungsverfahrens im Zuge der Polizeistrukturereform beachtet worden sei.

Sie begrüße, dass die Themen Medienkompetenz und Medienbildung in den neuen Bildungsplänen als Leitperspektive anerkannt würden. Dieses unter Präventionsgesichtspunkten wichtige Thema sei außerordentlich begrüßenswert, und es sei gut, dass dieser Bereich in die Landeskompetenz falle. Viele Eltern verfügten zum Teil nur über geringe Medienkompetenz, sodass sie diese auch nicht an ihre Kinder weitergeben könnten. Eine Aufnahme der Themen Medienkompetenz und Medienbildung und die Behandlung dieser Themen in der Schule seien deshalb unverzichtbar, damit Kinder und Jugendliche nicht nur die Chancen vermittelt bekämen, sondern auch mit den damit einhergehenden Risiken vertraut gemacht würden.

Ein Abgeordneter der Grünen äußerte, auch er bedanke sich beim Landesbeauftragten für den Datenschutz für seine Tätigkeit und den grafisch neu gestalteten und größtenteils spannend geschriebenen Tätigkeitsbericht. Aus seiner Sicht müsse dem Datenschutz in der Medienbildung ein höherer Stellenwert und ein größerer Raum gegeben werden, zumal immer mehr Bereiche des täglichen Lebens auch unter Datenschutzgesichtspunkten betrachtet werden müssten.

Zum Thema Smart-TV sei anzumerken, dass sich auch die Landesmedienanstalt und der Rundfunkrat des SWR damit befassen, doch in der Öffentlichkeit sei leider noch nicht genug bekannt, was es bedeute, wenn ein Smart-TV betrieben werde. Es sei nur eine Frage der Zeit, bis die ersten dieser Geräte auch mit eingebauten Kameras ausgestattet würden. Er plädiere dafür, das Thema Smart-TV unter dem Blickwinkel „Persönlichkeitsrechte der Nutzer“ noch weiter in das Blickfeld der Öffentlichkeit zu rücken.

Ein Abgeordneter der FDP/DVP legte dar, auch er schließe sich den lobenden Worten an. Er schätze die klare Sprache des Landesbeauftragten für den Datenschutz. Angesichts dessen, dass in der laufenden Sitzung sowohl der Landesbeauftragte für den Datenschutz als auch der Innenminister anwesend seien, interessiere ihn, ob beabsichtigt sei, das Recht so zu ändern, dass der erwähnte Mitzieheffekt künftig vermieden werde, und welche Konsequenzen aus dem Urteil zum Großen Lauschangriff gezogen würden.

Der Landesbeauftragte für den Datenschutz äußerte, der Landesgesetzgeber könne sowohl das Landespolizeigesetz als auch das Landesverfassungsschutzgesetz ändern. Er habe den Innenminister bisher so verstanden, dass beabsichtigt sei, das Landesverfassungsschutzgesetz bei nächster Gelegenheit zu ändern; diese „nächste Gelegenheit“ habe jedoch bereits mehrfach bestanden, ohne dass sie genutzt worden wäre.

Zum Polizeigesetz des Landes sei anzumerken, dass es durchaus liberalere Polizeigesetze gebe als das baden-württembergische. Zu diesem Thema könne er sich gern auch einmal zusammenfassend im Detail äußern. Er weise in diesem Zusammenhang darauf hin, dass möglichst viele Informationen gesammelt würden, um sehen zu können, ob bestimmte Personen wiederholt auffällig würden, dazu gebe es Dateien, in denen auch völlig legale Verhaltensweisen gespeichert würden, und dies sei im Grunde eine Vorratsdatenspeicherung. Für solche Fälle seien durchaus liberalere gesetzliche Regelungen denkbar, doch ob das geltende Recht entsprechend geändert werde, müsse politisch entschieden werden.

Ein Abgeordneter der CDU äußerte, ihn interessiere, ob beabsichtigt sei, § 6 Absatz 3 des Landesverfassungsschutzgesetzes verfassungskonform zu machen oder angesichts dessen, dass zehn Jahre lang keine Grundrechtseingriffe auf dieser Grundlage vorgenommen worden seien, zu prüfen, ob eine solche Rechtsgrundlage überhaupt noch erforderlich sei.

Der Innenminister legte dar, der Landesbeauftragte für den Datenschutz habe in seiner Kritik hinsichtlich des Landesverfassungsschutzgesetzes in der Tat recht. Auch er fühle sich angesichts der derzeitigen Situation zunehmend unwohl. Er habe bisher immer argumentiert, vor einer Änderung des Landesverfassungsschutzgesetzes anstehende Änderungen des Bundesverfassungsschutzgesetzes abzuwarten, doch dies dauere ihm mittlerweile zu lange. Deshalb müsse das Landesverfassungsschutzgesetz, weil es in Teilen nicht verfassungskonform sei, geändert werden. In welche der vom CDU-Abgeordneten aufgezeigten Richtungen, sei jedoch noch offen; dies müsse sehr sachlich und objektiv diskutiert werden. Es spreche zwar viel dafür, eine Vorschrift, die nicht die seinerzeit erhofften Erfolge mit sich gebracht habe und sich als nicht erforderlich erwiesen habe, nach einer gewissen Zeit wieder zu streichen; andererseits sei nicht ausgeschlossen, dass einmal eine Situation eintrete, in der es hilfreich sei, eine solche Vorschrift zur Verfügung zu haben. Er plädiere für eine sorgsame Abwägung, in der auch berücksichtigt werde, dass sich die Schwerpunkte der öffentlichen Wahrnehmung immer wieder veränderten. Auch er könne sich im Übrigen daran erinnern, was er vor einigen Jahren gesagt habe, doch es sollte auch möglich sein, seine Meinung im Laufe der Zeit zu ändern. Es sei im Übrigen nicht ausgeschlossen, dass es zwischen ihm und dem Landesbeauftragten für den Datenschutz hinsichtlich der §§ 22 und 38 des Polizeigesetzes durchaus auch Meinungsunterschiede gebe.

Abschließend stellte er unter Bezugnahme auf das Landesverfassungsschutzgesetz klar, das Land handle nicht rechtswidrig; denn von der theoretisch bestehenden Möglichkeit der Wohnraumüberwachung werde kein Gebrauch gemacht.

Ein Abgeordneter der CDU warf ein, damit bleibe der Innenminister in der Kontinuität seines Amtsvorgängers.

Ein weiterer Abgeordneter der CDU führte aus, die NSA-Affäre habe dem Datenschutz einen zusätzlichen Schub verliehen. Erschreckend sei jedoch, dass sich in Umfragen ein großer Teil der befragten Personen in der Weise äußere, es sei ihnen egal, ob jemand mithöre oder mitlese, und erkläre, es werde lediglich erwogen, vielleicht irgendwann einmal Verschlüsselungstechnik einzusetzen. Die NSA-Affäre sei von vielen Personen also zwar registriert worden, sei jedoch noch nicht als gravierend genug angesehen worden, um eine Verhaltensänderung auszulösen. Deshalb sei zu befürchten, dass, wenn die NSA-Affäre einmal aus dem öffentlichen Bewusstsein verschwunden sein werde, dem Datenschutz und dem Schutz der Persönlichkeitsrechte wieder weniger Aufmerksamkeit gewidmet werde als derzeit.

Der Landesbeauftragte für den Datenschutz äußerte, ein großer Teil der Datenschutzbeschwerden von Bürgern hätten eher geringe Eingriffe in die Persönlichkeitsrechte zum Thema wie beispielsweise Videoüberwachungsanlagen in der Nachbarschaft oder der Erhalt von unerwünschten Werbemails, und es sei etwas frustrierend, dass es eine Totalüberwachung gebe, deren Ausmaß weder technisch noch finanziell eingeschränkt werde, diese Tatsache jedoch weitgehend hingenommen werde. Dieses Problem könne nur durch entschlossenes politisches Handeln gelöst werden; dem setze jedoch die aus außenpolitischen Gründen gebotene Rücksichtnahme Grenzen.

Hoffnungsfroh stimme ihn, dass auch die amerikanische Industrie unter der Überwachung durch die NSA leide; denn es seien massive Vertrauensverluste feststellbar. Wenn sich große europäische Anwender von amerikanischen Anbietern wie beispielsweise Microsoft abwendeten und sich dafür entschieden, keine Daten mehr in Clouds abzulegen, sondern ihre Daten in Europa oder sogar in Deutschland zu speichern, habe dies auch wirtschaftliche Auswirkungen auf amerikanische Firmen. Im Übrigen zeige das Urteil betreffend Google, dass Europa durchaus gewillt sei, eine andere Rechtsordnung entgegenzusetzen. Ob es möglich sei, sich erfolgreich gegen internationale Spionage zu wehren, hänge vom Mut der Akteure

ab, Geheimdiensten Grenzen aufzuzeigen, was sich auch auf die Praxis des Bundesnachrichtendienstes auswirken könne. Es sei unstrittig, dass hinsichtlich der Überwachung eine erhöhte Sensibilität geboten sei.

Der Ausschuss beschloss ohne förmliche Abstimmung dem Plenum zu empfehlen, von der Mitteilung des Landesbeauftragten für den Datenschutz vom 17. Januar 2014, Drucksache 15/4600, und der vom Innenministerium hierzu mit Schreiben vom 16. April 2014 vorgelegten Stellungnahme der Landesregierung (*Anlage*) Kenntnis zu nehmen.

24. 06. 2014

Sascha Binder



Baden-Württemberg

INNENMINISTERIUM  
DER MINISTER

Anlage

Innenministerium Baden-Württemberg • Pf. 10 34 65 • 70029 Stuttgart

Datum 16. April 2014  
Durchwahl 0711 231-3250  
Aktenzeichen 2-0557.6/6  
(Bitte bei Antwort angeben)

An den  
Präsidenten des Landtags  
von Baden-Württemberg  
Herrn Guido Wolf MdL  
Haus des Landtags  
Konrad-Adenauer-Str. 3  
70173 Stuttgart

☞ Stellungnahme der Landesregierung zum 31. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (LT-Drs. 15/4600)

Anlagen  
Stellungnahme der Landesregierung  
Synopsis

Sehr geehrter Herr Landtagspräsident,

die Landesregierung hat in der Kabinettsitzung vom 1. April 2014 die Stellungnahme zum 31. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz beschlossen.

Ich darf Ihnen diese Stellungnahme und eine Synopse\*) in der Anlage zuleiten.

Je 35 Mehrfertigungen der Stellungnahme und der Synopse werden der Landtagsverwaltung für die Beratung im Ständigen Ausschuss mit besonderer Post zugeleitet.

Mit freundlichen Grüßen

  
Reinhold Gahr MdL

\*) Die oben genannte Synopse kann beim Informationsdienst des Landtags eingesehen werden.



**Baden-Württemberg**

INNENMINISTERIUM

15. April 2014

**Stellungnahme der Landesregierung**

**zum**

**31. Tätigkeitsbericht  
des Landesbeauftragten für den Datenschutz  
in Baden-Württemberg (LT-Drs. 15/4600)**

## 2

Die Landesregierung nimmt im Folgenden – entsprechend dem Beschluss des Landtags vom 17. September 1987 (LT-Drs. 9/4667) – zu den wesentlichen Ausführungen des Landesbeauftragten für den Datenschutz Stellung, die den Datenschutz im öffentlichen Bereich betreffen.

Für die Stellungnahme zum nichtöffentlichen Bereich, für den der Landesbeauftragte für den Datenschutz seit dem 1. April 2011 zuständig ist, 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. Dasselbe gilt für sonstige Bereiche des Datenschutzes, soweit das Land Baden-Württemberg nicht zuständig ist.

Förmliche Beanstandungen im Sinne des Landesdatenschutzgesetzes (LDSG) – die „schärfste“ Reaktionsmöglichkeit des Landesbeauftragten – sind nicht im aktuellen Bericht genannt.

## 1. Zur Situation

### 1.3 Europäischer und internationaler Datenschutz

#### 1.3.1 Die EU-Datenschutz-Grundverordnung – eine schwere Geburt

Das **Innenministerium** begrüßt grundsätzlich die Einführung eines Datenschutzrechtes, welches für die EU einheitlich gelten soll. Der Vorschlag der Europäischen Kommission wird neben Einzelfragen im Detail allerdings insbesondere hinsichtlich der Einbeziehung des öffentlichen Bereichs in eine EU-Datenschutz-Grundverordnung kritisch bewertet. Dadurch könnte das Landesdatenschutzrecht weitgehend obsolet werden. In diesem Zusammenhang ist ergänzend zu den Ausführungen des Landesbeauftragten für den Datenschutz darauf hinzuweisen, dass der Bundesrat am 30. März 2012 (BR-Drs. 52/12 [Beschluss]) Subsidiaritätsrüge gegen den Vorschlag erhoben hat.

#### 1.3.2 Die Europäische Datenschutzrichtlinie für Polizei und Justiz

Aus Sicht des **Innenministeriums** ist die Forderung des Landesbeauftragten für den Datenschutz zu begrüßen, dass durch die Richtlinie nur das Mindestmaß des Datenschutzes festgesetzt wird. Deutschland hatte im Oktober 2013 zu allen Artikeln der Datenschutz-

richtlinie eine zwischen dem federführenden Bundesministerium des Innern, dem damaligen Bundesministerium der Justiz und den Ländern abgestimmte Stellungnahme mit konkreten Änderungsvorschlägen für den Richtlinienentwurf an die EU übermittelt. Diese betreffen insbesondere folgende Punkte:

- Klarstellung, dass die Datenschutzrichtlinie nur rechtliche Mindeststandards setzt;
- Anpassung des Anwendungsbereichs der Datenschutzrichtlinie zur Erstreckung auf die gesamte polizeiliche Tätigkeit inklusive der nicht-straftatenbezogenen Gefahrenabwehr;
- Beschränkung der sehr weitgehenden polizeilichen Informationspflichten an Betroffene;
- Infragestellung des Mehrwerts gegenüber dem Rahmenbeschluss 2008/977/JI und Kritik an der kompetenzwidrigen Beeinflussung des nationalen Polizei- und Strafprozessrechts.

Inwieweit diese Position in das laufende Rechtsetzungsverfahren Eingang findet, bleibt abzuwarten.

#### 1.4 Datenschutz auf Bundesebene

##### 1.4.1 Die Weiterentwicklung des Bundesdatenschutzgesetzes (BDSG): Still ruht der See – auch im Bereich des Beschäftigtendatenschutzes

Das **Innenministerium** hält ebenso wie der Landesbeauftragte für den Datenschutz eine gesetzliche Regelung des Beschäftigtendatenschutzes für erforderlich. Aus diesem Grund hat Baden-Württemberg unter Federführung des Innenministeriums eine Bundesratsinitiative erarbeitet, die am 5. Juli 2013 in den Bundesrat eingebracht und beraten wurde (BR-Drs. 552/13). In dieser Entschließung wurde u. a. zum Ausdruck gebracht, dass im Hinblick auf Artikel 82 des von der EU-Kommission vorgelegten Entwurfs einer EU-Datenschutz-Grundverordnung zunächst zu prüfen sein wird, welcher Spielraum für nationale Regelungen verbleibt. Insbesondere ist zu berücksichtigen, dass die EU-Kommission zur Festlegung bestimmter Rahmenbedingungen für die Datenverarbeitung zum Erlass delegierter Rechtsakte ermächtigt werden soll. Dies spricht dafür, zunächst den weiteren Fortgang des Verfahrens hinsichtlich der EU-Datenschutz-Grundverordnung abzuwarten.

##### 1.4.2 Das E-Government-Gesetz des Bundes

Die Landesregierung wird die Ausführungen und Bewertungen des Landesbeauftragten für den Datenschutz in die weitere Arbeit an einem E-Government-Gesetz des Landes Ba-

den-Württemberg einbeziehen. Das federführende **Innenministerium** wird im Rahmen des weiteren Verfahrens den Landesbeauftragten für den Datenschutz auch schon in einem frühen Stadium und fortlaufend beteiligen und damit seine Verpflichtung aus § 31 Absatz 4 LDSG umsetzen. Die Arbeit für ein solches Gesetz steht noch am Anfang. Die Landesregierung ist sich bewusst, dass eine Förderung der elektronischen Verwaltung nur dann erfolgreich sein wird, wenn ein gutes und sicheres Datenschutzniveau gewährleistet ist, wie dies auch in der Stellungnahme des Landesbeauftragten für den Datenschutz gefordert wird.

#### 1.4.4 Die Bundesstiftung Datenschutz nimmt ihre Arbeit auf – ohne die Datenschützer

Die Einwirkungsmöglichkeiten der Landesregierung auf die Stiftung Datenschutz sind nach Ansicht des **Innenministeriums** begrenzt: Nach § 1 Absatz 2 Satz 1 der Satzung der Stiftung Datenschutz werden von den 25 Mitgliedern des Beirates ein Mitglied auf Vorschlag der Innenministerkonferenz der Länder und ein Mitglied auf Vorschlag der Kultusministerkonferenz der Länder bestellt.

#### 1.4.6 Aussichten für den Datenschutz in der 18. Legislaturperiode des Deutschen Bundestags – Erwartungen an die Politik

Das **Innenministerium** teilt im Wesentlichen die Ansichten des Landesbeauftragten für den Datenschutz hinsichtlich der Aussichten für den Datenschutz in der 18. Legislaturperiode des Deutschen Bundestages. Ob es noch zu einer Modernisierung des deutschen Datenschutzrechts kommen wird, ist allerdings fraglich, nachdem die EU-Kommission inzwischen den Entwurf einer EU-Datenschutz-Grundverordnung vorgelegt hat, die unmittelbar geltendes Recht schaffen würde.

### 1.5 Aus der Dienststelle

Die beiden vom Landesbeauftragten für den Datenschutz angeführten Gründe für die Schwierigkeiten bei Abordnungen zu seiner Dienststelle können für das **Innenministerium** und die Innenverwaltung nicht bestätigt werden. Bei Bewerbungen auf eine Tätigkeit beim Landesbeauftragten für den Datenschutz wird der verträgliche Zeitpunkt für einen Wechsel zwischen den personalverwaltenden Stellen verhandelt und in der Innenverwaltung wird die Station beim Landesbeauftragten für den Datenschutz als für die Personalentwicklung förderlich bewertet. Umgekehrt haben geeignete Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten für den Datenschutz bei entsprechenden Ausschreibungen in der Innenverwaltung bei Erfüllung von Anforderungsprofil und entsprechender Eignung,



Befähigung und fachlicher Leistung die Möglichkeit zum Wechsel, wenn nicht aus Stellengründen eine Beschränkung des Bewerberfeldes erfolgen muss.

Das Innenministerium weist darauf hin, dass für den Personalaustausch zwischen dem Innenministerium oder anderen Dienststellen der Innenverwaltung und dem Landesbeauftragten für den Datenschutz keine Besonderheiten im Vergleich zum Personalaustausch innerhalb der Landesverwaltung zwischen den Ressorts gelten. Das heißt, dass bei entsprechenden Stellenausschreibungen und Auswahlentscheidungen Versetzungen innerhalb der Landesverwaltung oder, wenn nicht sogleich entsprechende Planstellen in Anspruch genommen werden können oder sollen, vorgeschaltete oder von Anfang an befristete Abordnungen möglich sind. Dies gilt sowohl für einen Wechsel von Mitarbeiterinnen und Mitarbeitern des Landesbeauftragten für den Datenschutz in die Innenverwaltung wie auch umgekehrt. Über den konkreten Wechselzeitpunkt und ggf. die Bedingungen verständigen sich die beteiligten Personalverwaltungen.

Vorübergehende Verwendungen von Mitarbeiterinnen und Mitarbeitern der Innenverwaltung beim Landesbeauftragten für den Datenschutz werden vom Innenministerium im Rahmen der Personalentwicklung als weitere fachliche Verwendungen stets positiv bewertet; ebenso ein Wechsel von Mitarbeiterinnen oder Mitarbeitern des Landesbeauftragten für den Datenschutz in die Innenverwaltung. Bei diesen Personalwechseln werden, soweit vom Landesbeauftragten für den Datenschutz als Anforderungsprofil entsprechend mitgeteilt, bei den Bewerberinnen und Bewerbern auch besondere Fähigkeiten wie zum Beispiel englische Fremdsprachenkenntnisse berücksichtigt.

Eine vom Landesbeauftragten für den Datenschutz angestrebte schriftliche Vereinbarung mit der Landesregierung für einen regelmäßigen Personalaustausch muss neben der durch die Landesverfassung gewährleisteten Ressorthoheit auch die gesetzlichen dienstrechtlichen Rahmenbedingungen beachten. Eine detaillierte Bewertung kann erst nach Kenntnis der diesbezüglichen Vorstellungen des Landesbeauftragten für den Datenschutz erfolgen.

Außerdem stellt der Landesbeauftragte für den Datenschutz dar, dass im Berichtszeitraum 2012/2013 im Vergleich zu den Zahlen für 2010 die Anzahl von Eingaben der Bürgerinnen und Bürger bei ihm hinsichtlich des öffentlichen Bereichs um fast 60 % gesunken sind. Dies deutet – bei steigender Anzahl von Eingaben zum nichtöffentlichen Bereich – nach Ansicht des Innenministeriums darauf hin, dass die Bürgerinnen und Bürger zufriedener mit dem Umgang ihrer Daten durch die Verwaltung sind.

## 2. Innere Sicherheit

### 2.1 Notwendige, freiwillige und unterlassene Änderungen des Polizeirechts

#### 2.1.1 Gesetz zur Änderung des Polizeigesetzes und des Gesetzes zur Ausführung des Personenstandsgesetzes vom 20. November 2012 (LT-Drs. 15/2675)

Aus Sicht des **Innenministeriums** ist die Regelung in § 38 Absatz 5 des Polizeigesetzes (PolG) über die Fristen für die Speicherung von personenbezogenen Daten, die im Rahmen von Ermittlungsverfahren bekanntgeworden sind, aus Klarstellungsgründen vor dem Hintergrund verschiedener verwaltungsgerichtlicher Entscheidungen aus anderen Bundesländern erforderlich (z. B. Bayerischer Verwaltungsgerichtshof, Bayerische Verwaltungsblätter [BayVBl] 1998, 115; Hessischer Verwaltungsgerichtshof, Neue Zeitschrift für Verwaltungsrecht [NVwZ] 2006, 110). Das bereits im Rahmen der Anhörung zum Gesetzgebungsverfahren geäußerte Anliegen des Landesbeauftragten für den Datenschutz, etwaige Unklarheiten beim Vollzug der Vorschrift zu beseitigen, wurde aufgegriffen. Die Dienststellen wurden noch einmal an die bestehenden Vollzugshinweise (Dienstanweisung POLAS Nr. 13.2) erinnert. Eine Ergänzung der gesetzlichen Regelung ist aus Sicht des Innenministeriums nicht angezeigt.

#### 2.1.2 Änderungen durch das Gesetz zur Umsetzung der Polizeistrukturereform vom 23. Juli 2013 (LT-Drs. 15/2675)

Das **Innenministerium** bleibt bei der Zusage, dass bei der nächsten Änderung der Durchführungsverordnung zum Polizeigesetz (DVO PolG) eine Prüfung der Vorschläge des Landesbeauftragten für den Datenschutz zur Protokollierung der Zugriffe auf die polizeilichen Auskunftssysteme erfolgen wird.

#### 2.1.3 Geplante Änderungen im Polizeigesetz und im Landesverfassungsschutzgesetz

Aus Sicht des **Innenministeriums** ist zur Identifizierung von Gefahr verursachenden Nutzern der Telemedien die Erhebung bestimmter Nutzungsdaten nach dem Telemediengesetz erforderlich. Die Polizei benötigt im Interesse einer wirksamen Gefahrenabwehr diese den Anbietern vorliegenden Daten, um die Betroffenen und ihre möglichen Aufenthaltsorte rasch und verlässlich ermitteln zu können.

Überwiegend stehen Telemediendienste kostenlos zur Verfügung. Dies hat nach den polizeilichen Erfahrungen zur Folge, dass bei den Betreibern häufig Fantasiepersonalien als Bestandsdaten vorliegen. Eine Identifikation des Nutzers ist – wenn überhaupt – vielfach

nur über die genutzte IP-Adresse möglich. Betroffen sind Internetdienste wie Chats oder Videoportale.

Die Aufgabenstellungen der Polizei und des Verfassungsschutzes unterscheiden sich grundlegend. Die Datenerhebung nach § 5 b des Landesverfassungsschutzgesetzes (LVSG) ist nicht zur Abwehr von konkreten Gefahren für hochrangige Rechtsgüter erforderlich, sondern um Beteiligte von Kommunikationsvorgängen zu identifizieren und das Erkenntnisbild extremistischer Personen zu vervollständigen.

Der Landtag hat die Notwendigkeit dieser Regelungen bestätigt und am 19. Februar 2014 das am 1. März 2014 in Kraft getretene Gesetz zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes vom 25. Februar 2014 (GBl. S. 77) beschlossen.

#### 2.1.4 Der Sinneswandel im Polizeirecht

Aus Sicht des **Innenministeriums** besteht vor dem Hintergrund der nach wie vor beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerde (1 BvR 2795/09) zum Einsatz automatischer Kennzeichenlesesysteme nach § 22 a PolG kein Anlass, die Regelung aufzuheben.

Anzumerken ist, dass die aktuelle Fassung des § 22 a PolG bereits frühere Entscheidungen des Bundesverfassungsgerichts zum Einsatz automatischer Kennzeichenlesesysteme berücksichtigt. So wurden im Zuge der Änderung des Polizeigesetzes im Jahre 2008 insbesondere folgende Forderungen des Bundesverfassungsgerichts erfüllt:

- gesetzliche Definition des Fahndungsbestands, mit dem die erhobenen Kennzeichen abgeglichen werden, und
- sofortiger Abgleich der erfassten Kennzeichen und sofortige spurlose Löschung im Nichttrefferfall.

Ferner ist zu unterstreichen, dass in Baden-Württemberg derzeit keine Erfassungsgeräte im Einsatz sind und damit von der Regelung des § 22 a PolG kein Gebrauch gemacht wird.

Das Innenministerium hält hinsichtlich der verfassungsrechtlichen Bewertung von § 38 Absatz 2 PolG an seiner zum 29. Tätigkeitsbericht abgegebenen Stellungnahme (LT-Drs. 14/6131, Seite 17) fest. Die Vorgängerregelung im Polizeigesetz, die für die Datenspeicherung zwingend eine Wiederholungsprognose vorausgesetzt hatte, hatte zu keinem optimalen 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 (insbesondere im Zusammenhang mit der Überarbeitung der Dienstweisung POLAS-BW Mitte 2011) wie auch des Landesbeauftragten für den Datenschutz verbessert. Die vom Landesbeauftragten für den Datenschutz benannten Vorschläge spiegeln mehrere Aspekte des laufenden Qualitätsverbesserungsprozesses der Polizei wider. Die Zweifel an der Umsetzung des Aus- und Fortbildungskonzepts teilt das Innenministerium nicht. Gleichwohl werden die Lehrgänge beständig fortentwickelt und optimiert.

## 2.2 Datenverarbeitung durch Sicherheits- und Ordnungsbehörden

### 2.2.1 Der Polizeivollzugsdienst und seine Dateien

Das **Innenministerium** stimmt mit dem Landesbeauftragten für den Datenschutz darin überein, dass durch die Speicherung eines Hinweises auf eine Suizidgefahr der Suizid nicht generell verhindert werden kann. Genauso wenig kann die Polizei davon ausgehen, dass eine Person, zu der kein Hinweis vorliegt, nicht tatsächlich suizidgefährdet ist.

Bei der Durchführung polizeilicher Maßnahmen – insbesondere bei der Aufnahme von Personen in polizeilichen Gewahrsamseinrichtungen, bei Fahndungen, aber auch beispielsweise beim Einschreiten wegen häuslicher Gewalt – kann die Kenntnis einer möglichen Suizidgefahr jedoch dazu beitragen, durch ein entsprechendes taktisches Vorgehen dem Betroffenen angemessen zu begegnen. Insofern dient der Hinweis dem Schutz des Betroffenen und ggf. seines persönlichen Umfeldes einschließlich der Eigensicherung der einschreitenden Polizeibeamten.

Indem Datensätze mit dem Hinweis „Freitodgefahr“ nur für die Dauer von zwei Jahren gespeichert werden können, handelt es sich um einen temporären Eingriff in die Rechte des Betroffenen. Die Löschung ist sichergestellt, sofern nicht neuere Erkenntnisse zu einer erneuten Vergabe des personengebundenen Hinweises (PHW) führen.

Aus Sicht des Innenministeriums sind die Bedenken des Landesbeauftragten für den Datenschutz hinsichtlich der Terminologie „Freitodgefahr“ nachvollziehbar. Schließlich liegt einer Selbsttötung selten ein wirklich freier Willensentschluss zugrunde. Allerdings knüpft die Wortwahl an jene des vom Bundeskriminalamt im August 2011 erarbeiteten Leitfadens

PHW an. Dort ist der PHW-Begriff „FREI“ für Freitodgefahr geregelt. Der Leitfaden wurde, nachdem er beschlossen war, im August 2011 dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Kenntnisnahme übermittelt und nach unserem Kenntnisstand von dieser Seite nicht beanstandet. Vor diesem Hintergrund war der vom Innenministerium befürwortete Vorstoß auf Bundesebene für die Verwendung einer anderen Begrifflichkeit bislang ohne Ergebnis. Dies erklärt auch, weshalb die Stellungnahme des Landesbeauftragten für den Datenschutz inhaltlich noch nicht beantwortet werden konnte.

Außerdem wird das Innenministerium prüfen, wie dem Anliegen des Landesbeauftragten für den Datenschutz entsprochen werden kann, dass die Löschungen der Daten in der INPOL-Zentraldatei und dem Auskunftssystem POLAS-BW erfolgen.

#### 2.2.4 Zuverlässigkeitsprüfungen in allen Varianten

Das **Innenministerium** hält grundsätzlich weiterhin an der in den Stellungnahmen zum 27., 28. und 30. Tätigkeitsbericht (LT-Drs. 14/1269, Seiten 16–17, LT-Drs. 14/2366, Seiten 22–23 bzw. LT-Drs. 15/1500 Seiten 24–25) vertretenen Rechtsauffassung fest, dass Zuverlässigkeitsprüfungen auf der Grundlage sogenannter „informierter“ Einwilligungen der Betroffenen (das heißt die Betroffenen werden darüber informiert, was mit ihren Daten geschieht oder 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 der Landesbeauftragte für den Datenschutz nicht in Frage.

Zuverlässigkeitsprüfungen sind häufig bereichsspezifisch (z. B. § 12b des Atomgesetzes, § 19 des Hafensicherheitsgesetzes, § 7 des Luftsicherheitsgesetzes oder § 9 der Bewachungsverordnung) geregelt. In welchen anderen Bereichen weitere gesetzliche Regelungen notwendig und wo diese ggf. zu treffen sind, bedarf intensiver Überprüfung. Insbesondere sieht das **Staatsministerium** die Bedenken des Landesbeauftragten für den Datenschutz im Hinblick auf die angesprochenen Großveranstaltungen und den Bedarf zu prüfen, für welche Sachverhaltskonstellationen und ggf. wie eine gesetzliche Grundlage zu schaffen ist.

Im Hinblick auf die Überprüfung der Bewerberinnen und Bewerber für den Polizeivollzugsdienst führt das **Innenministerium** aus, dass nach der geltenden Rechtslage die Sicherheitsüberprüfung grundsätzlich auf die informierte Einwilligung gestützt werden kann. Hierzu wird ein ausführliches Belehrungsformular ausgehändigt. Bezüglich der Einzelfall-

prüfung gilt, dass nicht ausschließlich das von der Bewerberin oder dem Bewerber verwirklichte Delikt, sondern das Alter zur Tatzeit, die Tatzeit bzw. der Zeitraum zwischen Tat und Bewerbung sowie insbesondere das gezeigte Verhalten vor, während und nach der Tat für eine Bewertung der charakterlichen Eignung maßgeblich sind. Die Ergebnisse und Unterlagen der Zuverlässigkeitsüberprüfung verbleiben in der Bewerberakte und werden bei der HfPol BW (Institutsbereich Personalgewinnung) derzeit für fünf Jahre archiviert. Sie finden somit keinen Eingang in die Personalakte. Aufgrund des Schreibens des Landesbeauftragten für den Datenschutz an das Innenministerium vom 10. Februar 2014 erfolgt derzeit eine umfassende Prüfung, ob es für diese Speicherdauer ebenfalls einer expliziten Einwilligung oder einer gesetzlichen Änderung bedarf.

Hinsichtlich der Überprüfung der Mitarbeiter von Sicherheitsdiensten durch Gaststättenbehörden wird die rechtliche Bewertung des Landesbeauftragten für den Datenschutz Baden-Württemberg geteilt. Weder das Gaststättenrecht noch das Gewerberecht enthalten eine Rechtsgrundlage für die Durchführung einer Zuverlässigkeitsüberprüfung bei Mitarbeitern einer Sicherheitsfirma vor jedem konkreten Einsatz bei einer Festlichkeit oder einer Veranstaltung.

Da es im Gewerberecht bereits allgemeine Regelungen zur Durchführung von Zuverlässigkeitsüberprüfungen von Gewerbetreibenden im Sicherheitsgewerbe sowie deren Mitarbeiter gibt (vgl. hierzu § 34a GewO), hält das Innenministerium die Schaffung einer weiteren Ermächtigungsgrundlage zur Überprüfung der Mitarbeiter vor jedem Einsatz für unverhältnismäßig.

### 2.3 Die Polizeistrukturreform – auch eine Herausforderung für den Datenschutz

#### 2.3.2 Profitiert der Datenschutz von der Strukturreform?

Beim derzeitigen Sachstand ist dem **Innenministerium** eine belastbare Aussage hinsichtlich des vom Landesbeauftragten für den Datenschutz erwarteten Mehraufwandes durch die geänderte Aufgabenverteilung nicht möglich. Gleichwohl kann nicht ausgeschlossen werden, dass die geänderte Rechtslage zu einem Mehraufwand führt, wenn im Zusammenhang mit der polizeilichen Datenverarbeitung mehrere Dienststellen im Rahmen ihrer Zuständigkeiten tangiert sind.

Insbesondere bei landesweiten Dateien wird regelmäßig die technische Betreuung der Verfahren beim Präsidium Technik, Logistik, Service der Polizei (PTLS Pol) liegen, die fachliche Verantwortung hingegen bei den zuständigen Dienststellen (Landeskriminalamt, Präsidium Einsatz, Regionalpräsidien). Allerdings wird das PTLS Pol hier regelmäßig als

Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung nach § 7 LDSG tätig, außerdem werden Fragestellungen zur IT-Sicherheit sowie zur technischen Umsetzung der Verfahren eine Beteiligung des PTLs Pol erforderlich machen.

Die erforderliche Vereinbarung zur Auftragsdatenverarbeitung wurde im Dezember 2013 erarbeitet. Die Zeichnung der Vereinbarung wurde im Januar 2014 durch das PTLs Pol in Gang gesetzt. Das Landeskriminalamt hat die Vereinbarung zur Auftragsdatenverarbeitung bereits unterzeichnet.

Erfolgt die Datenübermittlung an das PTLs Pol nicht im Rahmen der Auftragsdatenverarbeitung, werden die gesetzlichen Vorschriften zur Datenübermittlung beachtet.

## 2.4 Der Verfassungsschutz in schwerer See

### 2.4.1 Verfassungswidrige Zustände im Verfassungsschutzrecht noch immer nicht behoben

Das **Innenministerium** teilt die Auffassung, dass § 6 Absatz 3 LVSG aufgrund fehlender Regeln zum Schutz des Kernbereichs privater Lebensführung seit dem vom Landesbeauftragten für den Datenschutz zitierten Urteil des Bundesverfassungsgerichts nicht mehr den Anforderungen des Verfassungsrechts entspricht. Allerdings handelt das Landesamt für Verfassungsschutz nicht rechtswidrig, denn es werden keine Maßnahmen der Wohnraumüberwachung durchgeführt. Folglich finden keine Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung statt, so dass die Verfassungswidrigkeit der Norm im Ergebnis unschädlich ist. Die Vorschrift wird Gegenstand einer zukünftigen Gesetzesnovellierung sein, an der der Landesbeauftragte für den Datenschutz beteiligt wird.

Mit dem vom Innenministerium im Entwurf erarbeiteten, vom Landtag am 19. Februar 2014 beschlossenen und am 1. März 2014 in Kraft getretenen Gesetz zur Änderung des Polizeigesetzes und des Landesverfassungsschutzgesetzes (LT-Drs. 15/4812) wird die Abfrage von Bestandsdaten auf eine verfassungsrechtlich einwandfreie Grundlage gestellt. Das Bundesverfassungsgericht hatte in seinem Beschluss vom 24. Januar 2012 (BVerfGE 130, 151 ff.) unter anderem angemahnt, dass die Bestandsdatenauskunft einer qualifizierten Rechtsgrundlage zugunsten der abfragenden Behörde bedürfe.

Die meisten Forderungen, die der Landesbeauftragte für den Datenschutz im Anhörungsverfahren erhoben hat, wurden bereits im Gesetzesentwurf umgesetzt. Das vom Landtag ohne Änderungen des Entwurfs beschlossene Gesetz enthält nun Regeln zur Dokumentationspflicht bei Bestandsdatenabfragen, die sich auf Zugangssicherungs-codes beziehen

oder anhand dynamischer IP-Adressen erfolgen. Für diese Fälle ist auch eine Pflicht zur Benachrichtigung des Betroffenen aufgenommen worden. Schließlich wurde auch eine Evaluationspflicht geregelt.

Nicht geändert wurde die systematische Stellung der neuen Norm zur Bestandsdatenauskunft (§ 8 b LVSG). Diese ist aus Sicht des Innenministeriums gut vertretbar. Sie findet sich auch im Bundes- und in anderen Landesverfassungsschutzgesetzen an der entsprechenden Stelle.

Ebenfalls nicht aufgenommen wurde die Bezugnahme auf eine konkrete Gefahr bei der Abfrage von Bestandsdaten anhand einer IP-Adresse. Dies widerspräche dem Wesen des Verfassungsschutzes. Zu dessen Aufgaben hat das Bundesverfassungsgericht in seinem Urteil zur Antiterrordatei (24. April 2013 – 1 BvR 1215/07) ausgeführt, er habe „Aufklärung bereits im Vorfeld von Gefährdungslagen zu betreiben“ sowie „mannigfaltige Bestrebungen auf ihr Gefahrenpotenzial hin allgemein zu beobachten und sie gerade auch unabhängig von konkreten Gefahren in den Blick zu nehmen“. Dieses Urteil ist gegenüber dem vom Landesbeauftragten für den Datenschutz zitierten die jüngere einschlägige Entscheidung des Bundesverfassungsgerichts.

Die neu in das Gesetz aufgenommenen Regelungen genügen daher insgesamt dem Grundrechtsschutz und tragen darüber hinaus Transparenzanforderungen und Kontrollbedürfnissen Rechnung.

#### 2.4.2 Terrorismusabwehr im Spannungsfeld von kollektivem Sicherheitsdenken und individuellen Freiheitsrechten

Das **Innenministerium** weist darauf hin, dass die Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei, insbesondere bezüglich der Speicherung der Daten von Kontaktpersonen, im Landesamt für Verfassungsschutz umgehend umgesetzt wurden. Außerdem wurde von Seiten des Bundes zugesagt, die vom Gericht an den Bundesgesetzgeber gerichtete Forderung, die Kontrollmöglichkeiten der Datenschutzbeauftragten des Bundes und der Länder zu verbessern, im Zuge der Novellierung des Antiterrordateigesetzes umzusetzen.

#### 2.4.3 Die Neustrukturierung des nachrichtendienstlichen Informationssystems NADIS

Nach der Rechtsauffassung des Bundes und des Verfassungsschutzverbands handelt es sich bei dem nachrichtendienstlichen Informationssystem als Wissensnetz (NADIS-WN) um eine Dienstleistung des Bundesamts für Verfassungsschutz zur Erfüllung der



Zusammenarbeitspflicht des Bundes und der Länder nach Artikel 73 Nr. 10 Buchstaben b und c des Grundgesetzes und § 1 Absatz 3 des Bundesverfassungsschutzgesetzes. Das **Innenministerium** folgt dieser Rechtsauffassung.

Die Kontrollmöglichkeiten des Landesbeauftragten für den Datenschutz – Einsichtnahme in die NADIS-Protokolldaten vor Ort im Landesamt für Verfassungsschutz – waren bisher aufgrund technischer Hindernisse eingeschränkt. In der aktuellen Software-Version sind diese beseitigt, so dass die technischen Voraussetzungen für die Einsichtnahme in die Protokolldaten gegeben sind. Der Landesbeauftragte für den Datenschutz wurde vom Landesamt für Verfassungsschutz hierüber unterrichtet.

#### 2.4.4 Auskunft nach dem Landesverfassungsschutzgesetz

Soweit der Landesbeauftragte für den Datenschutz feststellt, die Ablehnung einer Auskunft enthalte „häufig“ den Hinweis, der Betroffene könne sich an den Landesbeauftragten für den Datenschutz wenden, wird vom **Innenministerium** darauf hingewiesen, dass das Landesamt für Verfassungsschutz diesen Hinweis, der von der einschlägigen gesetzlichen Regelung (§ 13 Absatz 3 Satz 3 LVSG) ausdrücklich gefordert wird, ernst nimmt und bei einer Auskunftsverweigerung stets erteilt.

In dem vom Landesbeauftragten für den Datenschutz angesprochenen Einzelfall, in dem die Daten dem Betroffenen erst im Gerichtsverfahren mitgeteilt wurden, wurde § 99 Absatz 1 Satz 1 der Verwaltungsgerichtsordnung Rechnung getragen. Aufgrund der dort verankerten Auskunfts- und Vorlagepflicht gegenüber dem Gericht wurden die Daten offengelegt.

### 3. Justiz

#### 3.3 Quellen-Telekommunikationsüberwachung im Ermittlungsverfahren – Kontrollbesuch bei einer Staatsanwaltschaft

Die staatsanwaltschaftlichen Anträge auf Erlass eines richterlichen Beschlusses zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) wurden, worauf das **Justizministerium** hinweist und was auch der Landesbeauftragte für den Datenschutz nicht beanstandet, auf §§ 100a, 100b StPO gestützt. Die Anträge entsprachen im beschriebenen Einzelfall auch den von der Rechtsprechung aufgestellten Anforderungen.

Im Hinblick auf die Empfehlung des Landesbeauftragten, die Programme oder Programmsysteme, die ausgeleitet werden sollen, in den Beschlussanträgen explizit zu nennen, ist zu erinnern, dass diese Programme in der Praxis oftmals zum Zeitpunkt der Beantragung der Maßnahme nicht oder nur unvollständig bekannt sind. Im Falle der expliziten Nennung bedürfte es im Falle der Nutzung anderer Systeme jeweils eines Ergänzungsbeschlusses.

Es trifft zu, dass es im Rahmen der Quellen-TKÜ im beschriebenen Einzelfall auch zu Ausleitungen von Telekommunikation beim Einsatz des Endgerätes im Ausland gekommen ist. Soweit der Landesbeauftragte für den Datenschutz die Auffassung vertritt, diese sei ohne Rechtsgrundlage erfolgt und hätte ab dem Zeitpunkt der Ausreise des Beschuldigten bis zur Wiedereinreise eingestellt werden müssen, ist auf § 2 Absatz 3 Satz 2 LDSG hinzuweisen, wonach die Zuständigkeit des Landesbeauftragten für den Datenschutz für die Gerichte nur gilt, soweit sie in Verwaltungsangelegenheiten tätig werden.

Ungeachtet dessen sind die sich in diesem Zusammenhang stellenden Fragen rechtshilfrechtlicher Natur und berühren lediglich die Verwertbarkeit der erlangten Daten. Diese Fragen im Streitfall zu entscheiden, ist ureigenste Aufgabe der Strafgerichte.

Im Übrigen ist auch nicht ersichtlich, warum sich die Eingriffsqualität in datenschutzrechtlicher Hinsicht ändern soll, wenn sich ein Beschuldigter ins Ausland begibt. Ferner ist es – entgegen der Ausführungen im Tätigkeitsbericht – rein technisch nicht ohne weiteres möglich zu erkennen, ob ein Gespräch der Internettelefonie vom Ausland aus geführt wird.

Insgesamt stellen die §§ 100a, 100b StPO – zumal wie im beschriebenen Einzelfall unter Beachtung der Anforderungen der Rechtsprechung – eine auch datenschutzrechtlich eindeutige Grundlage für die Quellen-TKÜ dar.

#### 3.4 Teilprivatisierung im Justizvollzug

Die vom Landesbeauftragten für den Datenschutz zum automatisierten Übermittlungs- und Abrufverfahren nach § 52 des Justizvollzugsgesetzbuches – Buch 1 (JVollzGB I) dargestellte Auffassung wird vom **Justizministerium** geteilt. Bedauerlicherweise wurde es im Rahmen der Umsetzung der Teilprivatisierung der Justizvollzugsanstalt Offenburg versäumt, den Dienstleister gemäß § 52 Absatz 2 Satz 3 JVollzGB I durch Verordnung als weiteren Beteiligten am automatisierten Übermittlungs- und Abrufverfahren zu benennen. Vom Erlass einer entsprechenden Verordnung wird im Hinblick auf die Beendigung des teilprivatisierten Betriebs der Justizvollzugsanstalt Offenburg zum 31. Mai 2014 abgesehen. Es ist jedoch beabsichtigt, im Rahmen der nächsten Änderung des Justizvollzugs-

gesetzbuchs die mit der Übertragung von Vollzugsaufgaben beauftragten Stellen (§ 54 JVollzGB I) in den Katalog des § 52 Absatz 2 Satz 1 JVollzGB I aufzunehmen.

### 3.5 Adressangaben von Zeugen in der Anklageschrift

Das **Justizministerium** weist darauf hin, dass der Leitende Oberstaatsanwalt in Stuttgart die im Tätigkeitsbericht des Landesbeauftragten für den Datenschutz anhand eines Einzelfalls der Staatsanwaltschaft Stuttgart geäußerte Kritik aufgegriffen hat. Er hat durch entsprechende innerdienstliche Maßnahmen dafür Sorge getragen, dass künftig grundsätzlich weder in Anklageschriften noch in Anträgen auf Erlass eines Strafbefehls die vollständige Anschrift von Zeugen, sondern lediglich deren Wohn- bzw. Aufenthaltsort angeführt werden. Die Generalstaatsanwälte in Karlsruhe und Stuttgart werden die vom Landesbeauftragten für den Datenschutz angesprochene Problematik im Übrigen im Rahmen der jeweiligen Dienstbesprechungen mit den Behördenleitern ihres Bezirks erörtern.

## 4. Steuern und Statistik

### 4.1 Die Elektronischen LohnsteuerAbzugsMerkmale (ELStAM)

Die Ausführungen des Landesbeauftragten für den Datenschutz sind nach Angaben des **Ministeriums für Finanzen und Wirtschaft** inhaltlich korrekt. Das Ministerium hat die Anfrage des Landesbeauftragten für den Datenschutz mit Schreiben vom 10. Januar 2014 umfassend beantwortet und verschiedene Unklarheiten im Zusammenhang mit dem Verfahren ELStAM ausgeräumt.

Aus Sicht des Ministeriums für Finanzen und Wirtschaft ist folgende Klarstellung von Bedeutung: Das Verfahren ELStAM steht als Aufgabe nach § 5 Absatz 1 Nr. 30 Finanzverwaltungsgesetz in der Betriebsverantwortung des Bundeszentralamts für Steuern. Die Fachlichkeit und deren Umsetzung in der ELStAM-Datenbank liegt im Rahmen der KONSSENS-Regularien in der Verantwortung des auftragnehmenden Landes Nordrhein-Westfalen. Die baden-württembergischen Finanzämter sind daher keine verantwortlichen Stellen im Sinne des § 3 Absatz 3 LDSG. Verantwortliche Stellen nach dem Verzeichnisse für die Elektronische Lohnsteuerkarte sind vielmehr die zentrale Produktions- und Servicestelle ELSTER und das Rechenzentrum der Finanzverwaltung des Landes Nordrhein-Westfalen.

#### 4.2 Zensus und Haushaltsstatistiken

Im angesprochenen Eckpunktepapier des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit aus dem Mai 2013 wurden für das mit Blick auf den Zensus 2021 einzuleitende Gesetzgebungsverfahren Hinweise übermittelt. Nach Ansicht des **Ministeriums für Finanzen und Wirtschaft** bleibt aber abzuwarten, wie sich die von kommunaler Seite bundesweit bereits angestregten Gerichtsverfahren (mit weiteren Klageverfahren in Baden-Württemberg ist zu rechnen) entwickeln werden. Nicht auszuschließen ist, dass sich die höchsten deutschen Gerichte mit dem Zensus 2011 befassen werden.

Nach Angaben des Ministeriums für Finanzen und Wirtschaft hat das Statistische Landesamt den Landesbeauftragten für den Datenschutz im August 2013 umfassend über das Projekt „Weiterentwicklung des Systems der Haushaltsstatistiken“ informiert. Im 31. Tätigkeitsbericht sind die wichtigsten Eckpunkte des Projekts korrekt dargestellt. Zutreffend ist auch die Einschätzung des Landesbeauftragten für den Datenschutz, dass die Umsetzung des neuen Systems der Haushaltsstatistiken datenschutzrechtliche Fragen aufwerfen wird. Die Verantwortlichen im Statistischen Landesamt haben mit dem Landesbeauftragten für den Datenschutz vereinbart, ihn zu informieren, sobald neue Informationen über datenschutzrelevante Sachverhalte vorliegen.

#### 4.3 Zentrale Informations- und Annahmestellen bei Finanzämtern

Wie bereits aus dem Tätigkeitsbericht des Landesbeauftragten für den Datenschutz – worauf das **Ministerium für Finanzen und Wirtschaft** hinweist – hervorgeht, handelte es sich bei dem dargestellten Sachverhalt um eine Sondersituation während einer Umbauphase. Bei diesem Finanzamt wurde im Februar 2012 die neugestaltete Zentrale Informations- und Annahmestelle (ZIA) in Betrieb genommen.

Die Finanzämter wurden angewiesen, bei der Einrichtung einer ZIA unter anderem die im Tätigkeitsbericht aufgeführten baulichen und organisatorischen Anforderungen zu beachten. Auch künftig werden die Optimierungsempfehlungen des Landesbeauftragten für den Datenschutz bei anstehenden (Um-) Baumaßnahmen vollumfänglich berücksichtigt.

## 5. Kommunales

### 5.1 Kontrolle und Beratung – beides ist wichtig

Das Engagement des Landesbeauftragten für den Datenschutz in der Beratung und Schulung von Kommunen wird vom **Innenministerium** als oberste Kommunalaufsichtsbehörde begrüßt. Angesichts der Vielzahl der zu erfüllenden Aufgaben der Rechtsaufsicht und der kontinuierlichen Einsparungen im Personalbereich ist den Aufsichtsbehörden die Übernahme zusätzlicher Aufgaben nicht möglich. Konkrete datenschutzrechtliche Einzelfragen können – wie bisher – im Rahmen der Rechtsaufsicht geprüft werden.

### 5.2 Gespräche mit den Kommunalen Landesverbänden und kommunalen Praktikern über Veröffentlichungen durch Kommunen

Das **Innenministerium** als oberste Kommunalaufsichtsbehörde begrüßt, dass der Landesbeauftragte für den Datenschutz die Möglichkeiten der Übertragung von Gemeinderatssitzungen im geltenden Rechtsrahmen in Pilotprojekten mit den Kommunen erprobt. Wie schon der 30. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, in dem die Voraussetzungen für solche Übertragungen genannt wurden, zeigen auch diese Pilotprojekte, dass das geltende Recht Übertragungen nicht ausschließt und eine Gesetzesänderung nicht zwingend ist.

### 5.3 Die Bettensteuer und der Datenschutz

Zu den Anfragen einer Stadt bei Agenturen bzw. Internetplattformen weist das **Ministerium für Finanzen und Wirtschaft** auf Folgendes hin:

§ 3 Absatz 1 Nr. 3 Buchstabe a) Kommunalabgabengesetz (KAG) verweist hinsichtlich der Verfahrensvorschriften u. a. auf § 93 Abgabenordnung (AO). Zur Einholung von Auskünften sind die Steuerbehörden nach § 93 Absatz 1 Satz 1 und 3 AO gehalten, sich mit Anfragen oder Auskunftersuchen zunächst an den jeweiligen Steuerpflichtigen (Beherbergungsbetrieb) zu wenden. Die Einholung von Auskünften bei anderen Personen (z. B. Vermittlungsagenturen oder Betreiber von Internetplattformen) soll erst dann erfolgen, wenn das Auskunftersuchen bei dem jeweiligen Steuerpflichtigen selbst zu keinem Erfolg geführt hat oder keinen Erfolg verspricht. Diese Regelung kann allerdings nur dann angewandt werden, wenn der jeweilige Steuerpflichtige (Beherbergungsbetrieb) bekannt ist. Zur Feststellung von bisher unbekanntem Steuerpflichtigen kann sich die Steuerbehörde demnach unmittelbar an Agenturen oder Betreiber von Internetplattformen wenden.

Zur Empfehlung des Landesbeauftragten für den Datenschutz zum Verzicht auf die Erhebung der Bettensteuer gilt nach Ansicht des Ministeriums für Finanzen und Wirtschaft Folgendes:

Den Kommunen in Deutschland steht ein sogenanntes Steuerfindungsrecht zu. Artikel 105 Absatz 2a des Grundgesetzes regelt, dass die Länder die Befugnis zur Gesetzgebung über die örtlichen Verbrauch- und Aufwandsteuern haben, solange sie nicht bundesgesetzlich geregelten Steuern gleichartig sind.

In § 9 Absatz 4 des baden-württembergischen KAG hat der Landesgesetzgeber die Kommunen ermächtigt, von dem Steuerfindungsrecht Gebrauch zu machen. Die örtlichen Verbrauch- und Aufwandsteuern werden von den Kommunen durch Satzung geregelt.

Sofern der Charakter einer Aufwandsteuer gewahrt wird, ist damit im Grundsatz eine Besteuerung von privat veranlassenen Übernachtungen gegen Entgelt (z. B. in Hotels) durch die Gemeinden möglich. Es ist Sache der Kommunen, im Falle der Erhebung der Bettensteuer für eine Ausgestaltung Sorge zu tragen, die sowohl den Vorgaben des Abgabenrechts als auch des Datenschutzrechts entspricht.

Die Gemeinden haben im Rahmen ihrer Selbstverwaltungsgarantie darüber zu befinden, ob sie im Hinblick auf die örtlichen Gegebenheiten Übernachtungen gegen Entgelt besteuern. Es ist Sache der Gemeinden, Vor- und Nachteile einer solchen Steuer abzuwägen und dabei auch die Auswirkungen zu beurteilen, die sich bei der Einführung einer solchen Steuer ergeben (z. B. Übernachtungspreise, Entwicklung des Fremdenverkehrs, wirtschaftliche Lage und Konkurrenzsituation des örtlichen Beherbergungsgewerbes, Akzeptanz, Ausweichreaktionen). Außerdem obliegt es den Gemeinden zu prüfen, in welchem Verhältnis das zu erwartende Steueraufkommen und der mit der Erhebung der Steuer verbundene Verwaltungsaufwand zueinander stehen würden.

#### 5.4 Die Neuregelung des Bundesmeldegesetzes – kaum verabschiedet, schon wieder repariert

Das **Innenministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz, dass nach dem neuen Bundesmeldegesetz (BMG), welches am 1. Mai 2015 in Kraft treten wird, keine Verpflichtung für Beherbergungsstätten mehr besteht, Meldescheine an Polizeidienststellen zu übermitteln. Nach dem Wortlaut des § 30 Absatz 4 Satz 2 BMG werden die Hotelmeldescheine den Sicherheitsbehörden nur noch zur Einsichtnahme vorgelegt. Aus der Gesetzesbegründung folgt zudem, dass die Herausgabe der Hotelmeldescheine

an Sicherheitsbehörden erst nach deren vorheriger Beschlagnahme oder Sicherstellung rechtlich zulässig ist.

Hingegen sieht der Wortlaut des noch geltenden Meldegesetzes des Landes in § 24 Absatz 3 Satz 1 als gleichberechtigte Handlungsalternativen sowohl die Befugnis zur Einsichtnahme von Hotelmeldescheinen durch Sicherheitsbehörden als auch deren Übermittlung auf Verlangen an den Polizeivollzugsdienst vor.

Unter den Begriff der „Übermittlung“ fallen beispielsweise der postalische Versand oder die Übermittlung der Hotelmeldescheine per Fax. Nach Auffassung des Innenministeriums ist hiervon auch die elektronische Datenübermittlung erfasst, sofern dabei die dem Stand der Technik entsprechenden Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden.

Dies wird aus dem systematischen Zusammenhang mit anderen Vorschriften des Landesmeldegesetzes ersichtlich. So stellt zum Beispiel § 29 Absatz 1 oder 4 Landesmeldegesetz ebenfalls auf „Datenübermittlungen“ ab. Damit sind insbesondere (auch) elektronische Datenübermittlungen, wie sie sich aus der geltenden Meldeverordnung des Landes oder der Zweiten Bundesmeldedatenübermittlungsverordnung ergeben, gemeint.

## 7. **Gesundheit und Soziales**

### 7.5 **Datenschutz im Krankenhaus**

Der 7. Abschnitt des Landeskrankenhausgesetzes Baden-Württemberg enthält umfassende Bestimmungen zum Datenschutz im Krankenhaus.

Nach Ansicht des **Sozialministeriums** handelt es sich bei den beanstandeten Vorfällen jeweils um Einzelfälle, die zudem – zumindest im ersten Fall „Der Verlust von Patientendaten“ – im Nachhinein dazu geführt haben, dass das betreffende Krankenhaus unverzüglich Maßnahmen eingeleitet und die Datenschutzvorkehrungen im Haus nachgebessert hat. Das Sozialministerium hält es dennoch für geboten, auch andere Kliniken im Land erneut an den sensiblen Umgang mit Patientendaten zu erinnern.

Das Ministerium hat daher die Baden-Württembergische Krankenhausgesellschaft angeschrieben und darum gebeten, dass diese ihre Mitgliedskrankenhäuser auf den Tätigkeitsbericht des Landesbeauftragten für den Datenschutz aufmerksam macht und auf die Einhaltung des Datenschutzes im Krankenhaus hinweist. Dabei sollen die Einrichtungen ins-

besondere mit dem Einsatz externer Dienstleister im Zusammenhang mit der Datenverarbeitung und -vernichtung zurückhaltend umgehen und, sofern Externe einbezogen werden, sicherstellen, dass datenschutzrechtliche Bestimmungen eingehalten werden.

#### 7.5.1 Der Verlust von Patientendaten

Es ist aus Sicht des **Innenministeriums** als oberste Kommunalaufsichtsbehörde ausdrücklich zu begrüßen, dass die Trägerin des Kreiskrankenhauses bereits vor dem Verlust von Patientendaten Maßnahmen zur Datensicherheit ergriffen und nach Bekanntwerden des Vorfalls umgehend die weiteren, erforderlichen Maßnahmen getroffen hat. Es ist davon auszugehen, dass auf der Grundlage der nun getroffenen Maßnahmen zumindest ab der Implementierung des neuen Datensicherungskonzepts eine Wiederholung des Vorfalls nach menschlichem Ermessen ausgeschlossen ist.

Das Innenministerium weist darauf hin, dass das Regierungspräsidium Karlsruhe von Amts wegen die Einleitung eines Ermittlungsverfahrens gegen den Träger des Kreiskrankenhauses und den handelnden Mitarbeiter geprüft und von der Einleitung eines Bußgeldverfahrens abgesehen hat. Die Durchführung von Bußgeldverfahren war aus spezialpräventiven Gesichtspunkten nicht geboten.

#### 7.5.2 Die Entsorgung von Patientenakten durch einen externen Dienstleister

Das **Innenministerium** weist darauf hin, dass das Regierungspräsidium Karlsruhe gegen den Krankenhausträger als Nebenbeteiligten im selbständigen Verfahren nach § 30 Absatz 4 i. V. m. §§ 87, 88 des Gesetzes über Ordnungswidrigkeiten einen Bußgeldbescheid wegen unbefugter Datenverarbeitung nach § 43 Absatz 2 Nr. 1 BDSG erlassen hat. Die nicht datenschutzgerechte Entsorgung der Patientenakten stellt eine unzulässige Datenübermittlung dar. Der Bußgeldbescheid ist nach Ablauf der Einspruchsfrist rechtskräftig geworden. Da sich das Verfahren des Landesbeauftragten für den Datenschutz allein gegen die Klinik gerichtet hat und auch in der Öffentlichkeit die Klinik als Verantwortliche dargestellt und wahrgenommen wurde, wurde von einem Verfahren gegen Beschäftigte der Klinik abgesehen.

#### 7.14 Benötigt das Sozialamt MDK-Gutachten?

Das **Sozialministerium** ist – mit der überwiegenden Ansicht in der Literatur – der Auffassung, dass eine Differenzierung in zu schwärzende (also für den Sozialhilfeträger nicht relevante) und nicht zu schwärzende (weil für die konkrete Leistungsgewährung von Sozialhilfe relevante) Bestandteile eines medizinischen Gutachtens praktisch schlechthin un-



durchführbar wäre (vgl. hierzu ausführlich Rasmussen, Neue Zeitschrift für Sozialrecht [NZS] 1998, 67 [71, 72]). Hierfür sprechen folgende Gründe (vgl. Rasmussen a. a. O., jeweils m. w. N.):

Selbst Mediziner wären nicht in der Lage, eindeutig zu beurteilen, welche medizinischen Daten begutachtungsrelevant sind und welche nicht. § 69 SGB X gewährleistet einen unbeschränkten Datenfluss zwischen den Sozialverwaltungsträgern, soweit die Aufgabenerfüllung eine entsprechende Datenübermittlung erfordert.

Der Ausnahmeregelung des § 76 Absatz 2 Nr. 1 SGB X liegt zugrunde, dass die im Zusammenhang mit einer Begutachtung für die Feststellung leistungserheblicher Voraussetzungen zugänglich gemachten Daten ohnehin schon das Arzt-Patienten-Verhältnis verlassen haben und es unter Datenschutzgesichtspunkten keinen Unterschied machen sollte, ob ein ärztliches Gutachten z. B. von einer Krankenkasse oder einer Berufsgenossenschaft zur Feststellung ihrer Leistungsvoraussetzungen bewertet wird.

Zum anderen sollen Doppeluntersuchungen vermieden werden. Ferner fordert § 96 Absatz 1 Satz 1 SGB X ausdrücklich, dass von einem Sozialleistungsträger veranlasste ärztliche oder psychologische Untersuchungen so vorgenommen und dokumentiert werden sollen, dass sie auch bei der Prüfung der Voraussetzungen anderer Sozialleistungen verwendet werden können.

## **8. Datenschutz in Kindertageseinrichtungen und Schulen**

### **8.2 Datenschutz an Schulen**

#### **8.2.2 Verfahrensverzeichnis**

Das **Kultusministerium** sieht im Verfahrensverzeichnis eine wichtige Möglichkeit der datenschutzrechtlichen Selbstkontrolle durch die Schulen. Deswegen schult es fortlaufend sowohl Schulleiter als auch behördliche Datenschutzbeauftragte zu diesem Thema. Um den Schulen die Führung der Verfahrensverzeichnisse weiter zu erleichtern, hat das Kultusministerium seit Sommer 2012 zudem ein webbasiertes System „Verfahrensverzeichnis-Online-BW“ (VV-Online-BW) zur Verfügung gestellt, das von jeder Schule genutzt werden kann. In diesem Verfahren stehen ausführliche Hilfetexte und „Leitfragen“ bereit. Zudem werden Mustervorlagen für zentral vorgegebene oder häufig eingesetzte automatisierte Verfahren wie z. B. „Amtliche Schulverwaltung Baden-Württemberg“ (ASV-BW),

„Landeseinheitlichen Schulverwaltungsprogramm Baden-Württemberg“ (SVP-BW) usw. zur Verfügung gestellt. Dieser Service wird ausgebaut.

### 8.2.3 Schulverwaltungsprogramm

Die im SVP-BW gesperrten Datensätze können nach Auskunft des **Kultusministeriums** nicht weiter bearbeitet werden. Eine Löschung der Daten von der Benutzeroberfläche aus ist zwar nicht vorgesehen, da das SVP-BW nur als Interimslösung gedacht ist. Jedoch können die gesperrten Datensätze auf der Ebene der Datenbank gelöscht werden.

Mit der Einführung von ASV-BW, das derzeit bereits an ca. 150 Schulen als Pilotprojekt läuft, wird eine datenschutzkonforme Löschung von Schülerdaten realisiert. ASV-BW beinhaltet darüber hinaus ein Berechtigungskonzept, das „passgenaue“ Zugriffsberechtigungen gewährleistet. ASV-BW wurde dem Landesbeauftragten bereits vorgestellt.

### 8.2.4 Datenverarbeitung im Auftrag

Das **Kultusministerium** stellt im Kultusintranet unter dem Stichwort „Datenschutz an Schulen“ drei mit dem Landesbeauftragten für den Datenschutz abgestimmte Formulare zur Auftragsdatenverarbeitung bereit. Dabei handelt es sich um einen Mustervertrag zur Auftragsdatenverarbeitung, eine Information zu den Pflichten des Auftragnehmers und der Schule sowie eine Ausfüllhilfe zu den beiden Formularen der Auftragsdatenverarbeitung. Das Kultusministerium beabsichtigt, den Mustervertrag unter Berücksichtigung der gewonnenen Erfahrungen kontinuierlich weiterzuentwickeln und wird den Landesbeauftragten für den Datenschutz hierbei beteiligen.

Für die Schulen wäre es von Vorteil, wenn die Kontrolle des Auftragnehmers mit dem Nachweis eines geeigneten Zertifikats (Modul „IT-Grundschutz“ des Bundesamts für Sicherheit in der Informationstechnik) durch den Dienstleister erfüllt werden könnte. Das Kultusministerium regt daher an, bei der nächsten Novellierung des LDSG § 7 entsprechend anzupassen.

### 8.2.5 Umgang mit Fehlzeiten

Die Fehlzeiten der Schülerinnen und Schüler sind nach den Vorgaben der Verwaltungsvorschrift Führen von Klassen- und Kurstagebüchern vom 10. Februar 1999, zuletzt geändert durch Verwaltungsvorschrift vom 14. Juni 2001, in das Klassenbuch einzutragen. Die schriftlichen Entschuldigungen sind hiervon getrennt aufzubewahren.

Das **Kultusministerium** teilt die Einschätzung, dass Lehrer, die den abwesenden Schüler nicht unterrichten, oder gar Mitschüler kein Einsichtsrecht in die schriftlichen Entschuldigungen oder die Fehlzeiten im Klassenbuch haben. In diesem Sinne bestimmt Nr. 5 dieser Verwaltungsvorschrift auch die Verpflichtung der Schulleitung, durch geeignete Maßnahmen sicherzustellen, dass Unbefugte keinen Zugriff auf die Klassen- und Kurstagebücher erhalten.

Das Verlangen, die Entschuldigung per unverschlüsselter E-Mail zu übermitteln, ist auch nach Einschätzung des Kultusministeriums ein Verstoß gegen die Vorgaben des LDSG.

Soweit schriftliche Entschuldigungen aufbewahrt oder elektronisch übermittelte Entschuldigungen gespeichert werden, sollte die Löschung ein Jahr nach der Bekanntgabe des Zeugnisses erfolgen, denn diese werden nicht mit einer Rechtsbehelfsbelehrung versehen, so dass auch erst nach dieser Zeit die Bestandskraft eintritt.

#### 8.2.7 Soziale Netzwerke im Schulbetrieb

Das **Kultusministerium** teilt die Einschätzung des Landesbeauftragten für den Datenschutz, dass der Dienstherr die Nutzung des Sozialen Netzwerks Facebook durch Lehrpersonal zu privaten Zwecken kaum unterbinden kann. Die Handreichung des Kultusministeriums beschränkt sich daher darauf zu untersagen, dass Facebook von Lehrkräften für schulische und damit für dienstliche Aufgaben eingesetzt wird.

Mit der Lernplattform Moodle steht den Schulen in Baden-Württemberg auch eine datenschutzgerechte Alternative zur Verfügung. Darüber hinaus wird sich das Kultusministerium darum bemühen, weitere Soziale Netzwerke zu prüfen, um den Schulen datenschutzkonforme Alternativen zu Facebook empfehlen zu können.

#### 8.2.8 Einführung einer landeseinheitlichen Bildungsnummer

Die Einführung der landeseinheitlichen Bildungsnummer (LBN) ist nach Auskunft des **Kultusministeriums** Teil des Projekts ASV-BW und im Rahmen der gesetzlichen Vorgaben des § 115 des Schulgesetzes für Baden-Württemberg (SchG) zulässig. Vorgesehen sind eine operative Datenbank und eine Auswertedatenbank, also zwei Datenbanken. In der operativen Datenbank pflegen die jeweiligen Schulen die Daten der Schüler und sind somit verantwortliche Stelle im Sinne des LDSG.

Es ist je Schüler ein Datensatz zu führen. Dadurch ergibt sich die Erforderlichkeit für das Zusammenführen der Daten eines Schülers, wenn dieser im Verlauf seiner Schullaufbahn

verschiedene Schulen besucht. Zur Vermeidung von Doppelerfassungen ist daher eine zentrale Generierung einer Identifikationsnummer aus Name, Geburtsdatum und Geburtsort vorgesehen. In der Auswertedatenbank wird die amtliche Schulstatistik mittels pseudonymisierter Schülerdaten geführt, um für Planungszwecke u. a. statistische Bildungshistorien erstellen zu können.

Die LBN ist erforderlich, um die gesetzlichen Anforderungen, insbesondere bei schulübergreifenden Verwaltungsprozessen, umzusetzen (Übertragung der Daten eines Schülers bei Schulwechsel, zuverlässige Erkennung von Mehrfachbewerbung) und bei der Erstellung von Bildungsstatistiken. Voraussetzung hierfür ist die in der Begründung zu § 115 SchG benannte eindeutige Identifizierung von Schülerdaten mittels LBN.

Das Kultusministerium legt im Projekt ASV-BW und insbesondere bei der Einführung der LBN größten Wert auf den Datenschutz und hat daher die Konzepte in enger Abstimmung mit dem Landesbeauftragten für den Datenschutz erarbeitet. Der Landesbeauftragte macht zu Recht darauf aufmerksam, dass aus datenschutzrechtlicher Sicht zu beachten ist, dass eine Schule nur die für ihre eigenen Aufgaben erforderlichen Daten bekommt. Diese Anforderung wird durch die im automatisierten Verfahren realisierten technischen und organisatorischen Maßnahmen nach § 9 Absatz 3 LDSG umgesetzt. Insbesondere ist eine „passgenaue“ Zugriffsberechtigungsstruktur vorgesehen, bei der ein Zugriff auf personenbezogene Daten von Schülern nur derjenigen Schule möglich ist, die deren Stammschule ist.

Der Datenzugriff wird vom Schüler selbst durch das Mitteilen der LBN gesteuert. Ferner gewährleisten engmaschige automatische Protokollierungen, dass festgestellt werden kann, welche Schule für einen Schüler als Stammschule zugeordnet wurde. Zudem wird protokolliert, welcher Bedienstete einer Schule auf Schülerdaten zugegriffen hat. Jede Dateneingabe, -veränderung oder -löschung wird ebenfalls protokolliert. Die Protokolldateien werden entsprechend den datenschutzrechtlichen Bestimmungen regelmäßig gelöscht.

Die im Rahmen des Projektes vorgesehene Überarbeitung der Rechtsverordnung des Kultusministeriums über die Datenverarbeitung für statistische Erhebungen und schulübergreifende Verwaltungszwecke an Schulen (SchulStatDVV) wird unter Beteiligung des Landesbeauftragten erfolgen.

### 8.3 Datenschutz als Unterrichtsthema

#### 8.3.1 Datenschutz macht Schule

Medienbildung wird vom Kultusministerium als eines von fünf Leitprinzipien in den neuen Bildungsplänen curricular verankert. Hierbei werden die Anforderungen der am 8. März 2012 von der Kultusministerkonferenz verabschiedeten Empfehlung „Medienbildung in der Schule“ umgesetzt.

Datenschutz spielt in dem vom Landesmedienzentrum (LMZ) erarbeiteten Mediencurriculum, das eine Verankerung von aufeinander bezogenen Inhalten der Medienbildung in allen Fächern zum Ziel hat (spiralcurricularer Ansatz), eine wesentliche Rolle. Bei der Erarbeitung des Mediencurriculums wurde der Landesbeauftragte für den Datenschutz beteiligt. Seine Anregungen wurden in das Curriculum übernommen.

Das LMZ führt außerdem zum Thema pädagogischer Jugendmedienschutz, soziale Netzwerke und Datenschutz jährlich über 1.200 Veranstaltungen mit etwa 30.000 Teilnehmern (Eltern, Schüler und Lehrkräfte) durch. Beispielhaft können folgende Themen genannt werden:

- Soziale Netzwerke (Facebook etc.),
- Handy und Smartphones,
- Datenschutz und Persönlichkeitsrechte,
- Cyber-Mobbing,
- Jugendsexualität und Internetpornographie,
- Einkaufen, Bestellen, Downloaden im Internet,
- Aktive Medienarbeit,
- Inszenierte Wirklichkeiten im TV und
- Computerspiele.

In diesen Veranstaltungen spielt gerade auch die ethisch-moralische Orientierung eine besondere Rolle, in denen insbesondere auch Fragen des persönlichen Umgangs miteinander im Internet und Sozialen Netzwerken im Zentrum stehen.

Das LMZ hat ferner unter anderem ein Jugendmedienschutzcurriculum erarbeitet, das Schulen konkrete Hilfestellung gibt, wie und wo diese Themen einschließlich des Datenschutzes in die tägliche Unterrichtsarbeit eingebunden werden können. Dazu passende Medienangebote und Unterrichtshilfen sind über die Bildungsplanmatrix abrufbar.

### 8.3.2 Medienkompetenz macht Bildung

Das **Kultusministerium** weist darauf hin, dass Materialien zur Vermittlung von Medienkompetenz im Unterricht auch in Zukunft entwickelt und auf dem medienpädagogischen Portal MediaCultureOnline des LMZ Lehrkräften und allen Interessierten bereitgestellt werden. Auf dem genannten Portal hält das LMZ unter anderem einen Schwerpunkt Datenschutz vor. Die Materialien werden gegebenenfalls vor ihrer Veröffentlichung mit dem Landesbeauftragten für den Datenschutz abgestimmt.

### 8.3.3 Die Bildungsplanreform 2015 und der Datenschutz

Die Forderung nach einer durchgehenden Berücksichtigung der Medienkompetenz wird vom **Kultusministerium** unterstützt. Medienbildung kann jedoch nicht auf ein Fach reduziert werden, sondern muss – altersgerecht und angebunden an die konkreten Fachinhalte – Bestandteil aller Fächer sein. Deswegen hat sich die Landesregierung für die Vermittlung von Medienkompetenz für einen fächerintegrativen Ansatz entschieden.

Im Rahmen des fächerintegrativen Ansatzes wird in der Klasse 5 ein verbindlicher Basis-kurs Medienbildung im Umfang von 35 Jahreswochenstunden eingeführt werden, der die unterschiedlichen Vorkenntnisse der Schülerinnen und Schüler in Klasse 5 zusammenführt und eine verlässliche Grundlage zum weiteren Erwerb umfassender Medienbildung in der Sekundarstufe schafft. In diesem Basiskurs wird dem Datenschutz selbstverständlich ein hoher Stellenwert eingeräumt.

Das LMZ wird die Fachkommissionen bei der Verankerung von Medienbildung in den einzelnen Fächern intensiv beraten. Es wird außerdem alle Fachpläne der jeweiligen Klassenstufen auf die effektive Umsetzung des spiralcurricularen Ansatzes überprüfen.

## 9. Datenschutz in der Arbeitswelt

### 9.3 Datenschutzrechtliche Fragen bei Personalakten

Notwendige Unterlagen für die Berechnung von Urlaubsansprüchen werden im Geschäftsbereich des **Innenministeriums** als Personalaktendaten behandelt. Einen Zusammenhang mit Beschwerden, Behauptungen und Bewertungen, die für die jeweilige Beamtin oder den jeweiligen Beamten ungünstig sind oder ihnen nachteilig werden können, auf die sich die Anhörungspflicht von § 87 Absatz 4 des Landesbeamtengesetzes (LBG) bezieht, kann das Innenministerium dabei nicht erkennen. Wenn solche Beschwer-

den, Behauptungen oder Bewertungen in die jeweilige Personalakte aufgenommen werden sollen, wird von den Personalverwaltungen der Innenverwaltung jeweils die vorherige Anhörung des Betroffenen gemäß § 87 Absatz 4 LBG bzw. § 3 Absatz 6 Satz 4 TV-L durchgeführt.

## 11. Technik und Medien

### 11.1 Videoüberwachung

#### 11.1.3 Videoüberwachung in Arztpraxen

Die Berufsaufsicht über die in Baden-Württemberg tätigen Ärztinnen und Ärzte führt die Landesärztekammer Baden-Württemberg. Das **Sozialministerium** hat daher die Landesärztekammer Baden-Württemberg gebeten, ihre Kammermitglieder auf geeignetem Wege über die rechtlichen Voraussetzungen einer Videoüberwachung in Arztpraxen zu informieren.

#### 11.1.4 Zulässigkeit von Wildkamas

Der Einsatz von sogenannten Wildkamas ist landesweit festzustellen. Das **Ministerium für Ländlichen Raum und Verbraucherschutz** stimmt der rechtlichen Beurteilung des Landesbeauftragten für den Datenschutz insoweit zu, als es sich bei im Wald und der freien Landschaft eingesetzten Wildkamas um Videoüberwachungsanlagen handelt, deren Zulässigkeit sich nach § 6b BDSG richtet.

Dem gesetzlichen Betretens- und Erholungsrecht des Einzelnen im Wald und der freien Landschaft kommt eine hohe Bedeutung zu. Mit Blick darauf ist zu prüfen, inwieweit der Einsatz von Wildkamas im Einzelfall die Anforderungen des § 6b BDSG erfüllen kann. Insbesondere ist der Frage nachzugehen, inwieweit berechnete Interessen für konkret festgelegte Zwecke (z. B. Forschungszwecke, Wildtiermonitoring) einen Einsatz von Wildkamas ausnahmsweise rechtfertigen können.

Das Ministerium für Ländlichen Raum und Verbraucherschutz hat bereits Gespräche mit dem Landesbeauftragten für den Datenschutz aufgenommen, um in gegenseitiger Abstimmung die rechtlichen Anforderungen zu konkretisieren.

### 11.1.5 Videoüberwachung an Schulen nach § 20a LDSG

Das **Kultusministerium** schließt sich der Auffassung des Landesbeauftragten für den Datenschutz an, dass die Überwachung einer Schule während der Unterrichtszeiten in der Regel unzulässig ist und es im Ergebnis auf die konkreten Umstände des Einzelfalls ankommt.

Bereits in Stellungnahmen zu früheren Tätigkeitsberichten hatte das Kultusministerium darauf hingewiesen, dass für den erstmaligen Einsatz einer Videoüberwachung an Schulen eine vorherige Freigabe der verantwortlichen Stelle erforderlich ist. Dies ist bei den öffentlichen Schulen in der Regel der jeweilige Schulträger, sofern die Videoüberwachung außerhalb des Schulbetriebs erfolgt.

Diese Verantwortlichkeit des jeweiligen Schulträgers für die Videoüberwachung liegt letztendlich in der Zuständigkeit des Schulträgers für die äußeren Schulangelegenheiten nach § 48 Absatz 2 in Verbindung mit § 41 Absatz 1 SchG begründet. Wegen der Verantwortlichkeit des Schulträgers ist vor einer Freigabe der Videoüberwachung der behördliche Datenschutzbeauftragte beim Schulträger zu beteiligen und diesem ist die schriftliche Begründung zur Prüfung zuzuleiten.

## 11.2 Soziale Netzwerke

### 11.2.1 Facebook und der Datenschutz

Das **Innenministerium** hat bereits zum 30. Tätigkeitsbericht (LT-Drs. 15/1500, S. 20 f.) ausgeführt, dass es – wie die Datenschutzbeauftragten – eine Verbesserung des Datenschutzes bei sozialen Netzwerken in einer Reihe von Punkten für dringend erforderlich hält. 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 im Einklang mit datenschutzrechtlichen Vorschriften ermöglichen.

Da öffentliche Stellen zunehmend über soziale Netzwerke mit 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, welche u. a. Gespräche mit Facebook für das erste Halbjahr 2014 vorbereitet hat.