

## **Beschlussempfehlung und Bericht**

### **des Ständigen Ausschusses**

#### **zu der Mitteilung des Landesbeauftragten für den Datenschutz vom 1. Dezember 2009 – Drucksache 14/5500**

#### **29. Tätigkeitsbericht des Landesbeauftragten für den Daten- schutz in Baden-Württemberg 2008/2009**

#### Beschlussempfehlung

Der Landtag wolle beschließen,

von der Mitteilung des Landesbeauftragten für den Datenschutz vom 1. Dezember 2009 – Drucksache 14/5500 – und der vom Innenministerium hierzu mit Schreiben vom 12. Februar 2010 vorgelegten Stellungnahme der Landesregierung (siehe Anlage zum Ausschussbericht) Kenntnis zu nehmen.

31. 03. 2010

Der Berichterstatter:

Thomas S. Bopp

Der Vorsitzende:

Winfried Mack

#### Bericht

Der Ständige Ausschuss beriet die Mitteilung des Landesbeauftragten für den Datenschutz vom 1. Dezember 2009, Drucksache 14/5500, in seiner 39. Sitzung am 31. März 2010.

Der Ausschussvorsitzende teilte mit, zur Beratung lägen ein Schreiben des Innenministeriums vom 12. Februar 2010 mit der Stellungnahme der Landesregierung zum 29. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (*Anlage*) sowie eine synoptische Darstellung des 29. Tätigkeitsberichts und der Stellungnahme der Landesregierung hierzu vor.

Der Landesbeauftragte für den Datenschutz wies eingangs darauf hin, dass der Datenschutz in Baden-Württemberg dieser Tage 30 Jahre alt werde. Denn

Ausgegeben: 13. 04. 2010

**1**

am 28. März 1980 sei das Landesdatenschutzgesetz in Kraft getreten, und am 1. April 1980 habe die erste Landesbeauftragte für den Datenschutz, Frau Dr. Ruth Leuze, ihr Amt angetreten.

Anschließend bedankte er sich für die Gelegenheit, sich zum vorliegenden 29. Tätigkeitsbericht auch mündlich zu äußern, und führte aus, in Datenschutzfragen habe vor allem aufgrund der technischen Entwicklung, aber auch ausgelöst durch internationale Einflüsse und dabei insbesondere durch Vorgaben seitens der EU eine starke Veränderung stattgefunden. Das Datenschutzrecht sei in einer Zeit der Großrechner mit knappem und teurem Speicherplatz entwickelt worden, und inzwischen sei die Datenverarbeitung in Echtzeit allgegenwärtig, und damit gehe eine Bedrohung für das Recht auf informationelle Selbstbestimmung einher. Für den Einzelnen werde es immer schwerer, zu überschauen, wer welche Informationen über ihn gesammelt habe und wie sie genutzt würden. Angesichts dieser drohenden Schieflage sei die gesamte Gesellschaft aufgefordert, gegenzusteuern.

Die öffentlichen Verwaltungen in Deutschland seien hinsichtlich des Datenschutzes auch im europäischen Vergleich derzeit nicht schlecht aufgestellt. Die gravierendsten Gefährdungen des Rechts auf informationelle Selbstbestimmung drohten derzeit vielmehr aus dem Bereich privater Unternehmen; der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der für den Datenschutz sowohl im öffentlichen als auch im privaten Bereich zuständig sei und bei dem u. a. die Zuständigkeit für die Firma Google liege, habe dazu mitgeteilt, dass rund 80 % der Eingaben den privaten Sektor beträfen.

Aus seiner Sicht hätten sowohl die Bundesregierung als auch die Bundestagsfraktionen ein Stück weit erkannt, welche Veränderungen es hinsichtlich des Datenschutzes gegeben habe, und deshalb habe der Bundestag auch die Enquetekommission „Internet und digitale Gesellschaft“ eingesetzt. Auch die Verlautbarungen des Bundesinnenministers und der Bundesjustizministerin ließen erwarten, dass dem Datenschutz, der informationellen Selbstbestimmung und der Wahrung der Privatsphäre eine ausreichende Bedeutung beigemessen werde.

Das Bundesverfassungsgericht habe in der Vergangenheit immer wieder wichtige Marksteine gesetzt, zuletzt mit seiner Entscheidung vom 2. März 2010 zur Vorratsdatenspeicherung. Bedeutsam sei jedoch auch die Entscheidung aus dem Jahr 2008 zur Online-Durchsuchung, in der das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ins Leben gerufen worden sei, mit der das Grundrecht auf informationelle Selbstbestimmung ergänzt werde. Aus diesen Entscheidungen könne ein gewisser Schutzanspruch des Bürgers gegenüber dem Staat abgeleitet werden, für eine sichere und datenschutzgerechte Kommunikation einzutreten. Deshalb müssten die Aspekte Datenschutz und Datensicherheit bei der Neuentwicklung von EDV-Systemen und -verfahren immer mitbedacht und berücksichtigt werden.

Der vorliegende Tätigkeitsbericht stamme nicht in vollem Umfang von ihm selbst; vielmehr habe er auf dem aufgebaut, was sein Vorgänger eingeleitet habe. Neben der technischen Entwicklung halte er auch die Entwicklung auf europäischer Ebene für berichtenswert, die auch auf Deutschland Einfluss habe. Er erinnere in diesem Zusammenhang an das Urteil des Europäischen Gerichtshofs vom 9. März 2010 zur Unabhängigkeit der Datenschutzaufsicht in Deutschland.

Ein wesentlicher Teil des vorliegenden Tätigkeitsberichts betreffe die Polizei, die mit sensiblen Daten umgehe und deshalb großen Wert auf den Datenschutz zu legen habe. Von der fachlichen Qualität der Sicherheitsbehörden in

Baden-Württemberg habe er auch aus eigener Anschauung eine hohe Meinung. Dies gelte im Übrigen sowohl für die Polizei als auch für den Personalkapazität seiner Dienststelle dadurch aufgestockt worden sei, dass im Wege der Abordnung ein Polizeibeamter zur Verfügung gestellt worden sei, der zuvor einige Jahre lang beim Gemeinsamen Terrorismusabwehrzentrum in Berlin tätig gewesen sei. Er halte den Erfahrungsaustausch mit Polizeipraktikern für beide Seiten für wichtig, zumal bei der Datenverarbeitung im Polizeibereich, wie aus dem vorliegenden Tätigkeitsbericht hervorgehe, eine gewisse Qualitätsverbesserung erforderlich sei. Dieser Bericht fokussiere sich im Übrigen nicht auf spektakuläre Einzelfälle, sondern beleuchte vielmehr das Alltagsgeschäft der Polizei und hierbei beispielsweise das polizeiliche Auskunftssystem für die alltägliche Polizeiarbeit, dessen Datenqualität verbesserungsbedürftig sei. Dazu habe er Vorschläge gemacht, worauf das Innenministerium am Vortag mit einem Schreiben Stellung genommen habe. Er halte in dieser Hinsicht vertiefte Gespräche mit dem Innenministerium für erforderlich und plädiere dafür, die Einführung der computergestützten Vorgangsbearbeitung ComVor bei der Polizei und die damit einhergehende Standardisierung von Prozessen dazu zu nutzen, Fehler der Vergangenheit nach Möglichkeit abzustellen und das Datenschutzniveau zu heben.

Im Tätigkeitsbericht sei die Datenqualität bei der polizeilichen Datenverarbeitung kritisiert worden, weil festgestellt worden sei, dass die Datenverarbeitung aus Sicht seiner Dienststelle dann, wenn Polizeibeamte selbst in strafrechtliche Ermittlungsverfahren verstrickt gewesen seien, besonders differenziert und sorgfältig erfolgt sei. Dies habe das Innenministerium jedoch offenbar als Votum aufgefasst, bei Polizeibeamten genauso streng wie bei jedem Bürger vorzugehen. Doch so sei dies nicht gemeint gewesen. Vielmehr halte seine Dienststelle das Vorgehen bei Polizeibeamten für angemessen, vor einer Einspeicherung abzuwarten, wie ein Ermittlungsverfahren ausgegangen sei, und im Übrigen die Vorgesetzten zu beteiligen und alles genau zu prüfen, und würde sich wünschen, dass diese Sorgfalt bei allen Bürgerinnen und Bürgern, soweit sie betroffen seien, in gleicher Weise an den Tag gelegt würde.

Ein zweiter Schwerpunkt des Tätigkeitsberichts sei der Schulbereich, den er in seiner Pressemitteilung vom 14. Dezember 2009 als Notstandsgebiet in Sachen Datenschutz bezeichnet habe. Weniger hart ausgedrückt hätte es auch „Entwicklungsgebiet“ heißen können, doch unabhängig von der Bezeichnung sehe er hinsichtlich Datenschutz noch Optimierungsbedarf. Große Defizite würden beispielsweise häufig hinsichtlich der Dokumentation von EDV-Verfahren in Schulen und der Einwilligungserklärungen für das Veröffentlichen von Fotos und anderer personenbezogener Daten durch die Schulen festgestellt, und bei Nachfragen ergebe sich vielfach, dass Schulleiter derartige Aufgaben eher als technische oder als Verwaltungsaufgaben betrachteten und delegierten, ohne auf die Datenschutzrelevanz zu achten. Die Schulen müssten ohne große Unterstützung durch die Schulaufsicht vielfach große EDV-Verfahren betreiben, ohne dass ihnen klar wäre, dass sie im Sinne des Datenschutzrechts verantwortliche Stelle seien, und fühlten sich im Grunde ein Stück weit alleingelassen.

Deshalb habe seine Dienststelle sowohl in einem persönlichen Gespräch mit Vertretern des Kultusministeriums als auch im Tätigkeitsbericht vorgeschlagen, in der Schulverwaltung wie in anderen großen Verwaltungskörpern Datenschutzbeauftragte zu etablieren, die bezogen auf die Schulverwaltung beispielsweise bei den Schulaufsichtsbehörden angesiedelt sein könnten und die Schulen in Sachen Datenschutz berieten, Fortbildungen organisierten, Handreichungen herausgäben usw. Daraufhin habe das Kultusministerium vor wenigen Tagen geschrieben, dieser Vorschlag sei aus landesspezifischen Gründen nicht durchführbar, weil die unteren Schulbehörden nicht über eine hin-

reichende Sachkunde verfügten und die Oberschulämter jeweils zu viele Schulen zu betreuen hätten. Er habe kein Verständnis dafür, dass Baden-Württemberg als „Kinderland“ so nachlässig mit dem Datenschutz an Schulen umgehe, zumal anderswo wie beispielsweise in Thüringen die Datenschutzsituation wesentlich besser sei.

Ihm sei bewusst, dass mit der Bestellung von behördlichen Datenschutzbeauftragten zunächst nur auf dem Papier etwas gewonnen sei, doch dann sei immerhin ein Ansprechpartner und auch Verantwortlicher vorhanden.

Weiter äußerte er, der Innenminister habe am 25. August 2009 im Zusammenhang mit der Vorstellung des Fünften Tätigkeitsberichts des Innenministeriums zum Datenschutz im nicht öffentlichen Bereich völlig zu Recht geäußert: „Datenschutz sollte Chefsache sein.“ In diesem Zusammenhang habe er an die Adresse der Unternehmen vorgebracht, die Selbstkontrolle des Datenschutzes in den Betrieben müsse dringend gestärkt werden; es dürfe nicht sein, dass selbst große Unternehmen keinen betrieblichen Datenschutzbeauftragten bestellen, obwohl dies gesetzlich vorgeschrieben sei. Es sei auch notwendig, gut ausgebildete Datenschutzbeauftragte einzusetzen, ihnen ausreichend Zeit für ihre Kontrollaufgabe zu geben und auf sie zu hören, wenn es um die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gehe. Dies werde in der Praxis leider häufig „vergessen“.

Dieser Aussage des Innenministers schließe er sich an und weise darauf hin, dass dies in der Landesverwaltung leider noch viel häufiger „vergessen“ werde. Er appelliere daher an die Landesverwaltung, diese Vorgaben an die Unternehmen auch im eigenen Verantwortungsbereich konsequent umzusetzen. Auch wenn die Bestellung von behördlichen Datenschutzbeauftragten mitunter als Formalie betrachtet werde, wäre ein solcher Schritt in allen Teilen der Landesverwaltung ein Fortschritt und stünde der Landesverwaltung gut zu Gesicht.

Abschließend brachte er vor, auf weitere Details des Tätigkeitsberichts wolle er im Rahmen seines einführenden Vortrags nicht eingehen. Er kündige jedoch an, dass seine Dienststelle die neuen Projekte, die ins Werk gesetzt worden seien, wie beispielsweise die Einschulungsuntersuchung oder die Umsetzung des Orientierungsplans hinsichtlich ihrer Umsetzung zu kontrollieren. Gleiches gelte für andere grundrechtssensible Bereiche wie beispielsweise die elektronische Aufsicht im Strafvollzug.

Ein Abgeordneter der SPD bedankte sich namens seiner Fraktion für den umfangreichen und auch sehr detailreichen Tätigkeitsbericht, aus dem auch hervorgehe, wo es dringenden Handlungsbedarf seitens der Politik gebe. Wenn Schulen hinsichtlich Datenschutz als Notstandsgebiet bezeichnet worden seien, müssten rasch Gegenmaßnahmen ergriffen werden. Dies sollte vom Landtag auch eingefordert werden.

Weiter führte er aus, erfreulicherweise sei der Grundsatzbeschluss gefasst worden, die Datenschutzaufsicht für den öffentlichen und den nicht öffentlichen Bereich zu bündeln, und dies sollte als Chance genutzt werden, den Datenschutz mehr als bisher ernst zu nehmen. Dies schließe ein, die neue Institution, die künftig für die Datenschutzaufsicht zuständig sein werde, unabhängig von der konkreten Ausgestaltung mit ausreichend personellen und sächlichen Mitteln auszustatten; denn es reiche nicht aus, seitens der Datenschutzaufsicht der technischen Entwicklung hinterherzulaufen oder eine Art „Reparaturbetrieb“ darzustellen. Vielmehr sollte die Datenschutzaufsicht neue Entwicklungen im Voraus bewerten und deren Einführung insoweit begleiten, dass der Datenschutz von vornherein beachtet werde, dass Datenschutzverstößen also vorgebeugt werde. Die Anforderungen des Europä-

ischen Gerichtshofs an die Datenschutzaufsicht sollten ernst genommen und umgesetzt werden, um die verlangte Unabhängigkeit zu gewährleisten. Die Datenschutzaufsicht für den nicht öffentlichen Bereich einfach zur Dienststelle des Landesbeauftragten für den Datenschutz zu verlagern würde wahrscheinlich nicht ausreichen; die konkrete Umsetzung werde jedoch sicher noch zu diskutieren sein.

Ein Abgeordneter der Grünen bedankte sich beim Landesbeauftragten für den Datenschutz für die Arbeit seiner Dienststelle sowie für den Tätigkeitsbericht, der wiederum gezeigt habe, welchen Stellenwert der Datenschutz haben sollte und welchen Stellenwert er habe. Nach dem Eindruck seiner Fraktion werde der Datenschutz auch in Landesbehörden mitunter noch als störend und behindernd angesehen, sodass auch aus Sicht seiner Fraktion ein Umdenken notwendig sei.

Seine Fraktion begrüße, dass die Datenschutzaufsichtsbehörden für den öffentlichen und den nicht öffentlichen Bereich endlich zusammengelegt würden, und bitte hierzu um Auskunft, wie die neue Datenschutzaufsichtsbehörde personell und finanziell ausgestattet sein solle. Denn allein eine Pro-Forma-Zusammenlegung ohne personelle Verbesserungen reiche aus Sicht seiner Fraktion nicht aus.

Ferner interessiere seine Fraktion mit Blick auf die Vorgaben von der europäischen Ebene hinsichtlich Unabhängigkeit, wie die neue Behörde in Bezug auf das Innenministerium positioniert sein werde.

Die besondere Erwähnung der Bereiche Schule und Polizei durch den Landesbeauftragten für den Datenschutz sei richtig. Denn beispielsweise bei den DNA-Untersuchungen im Zusammenhang mit dem Heilbronner Polizistenmord seien 250 Personen untersucht worden, obwohl die richterlich festgelegten Verdachtsraster auf sie nicht zugetroffen hätten. Angesichts dieser großen Personenzahl sei nicht mehr von einem Versehen zu sprechen, sondern in diesem Fall seien die gesetzlichen Vorschriften aus seiner Sicht wohl bewusst „übersehen“ worden. Er bitte das Innenministerium um Auskunft, inwieweit Vorsorge getroffen worden sei, dass so etwas zukünftig nicht mehr vorkomme. Ferner wolle er wissen, wer für diesen Vorfall letztlich verantwortlich sei.

Mit Freude habe seine Fraktion zur Kenntnis genommen, dass in Schulen und in Freibädern nunmehr keine Videoüberwachung mehr stattfinde, zumal er nicht gehört habe, dass die Sicherheit dort massiv unter diesem Verzicht auf Videoüberwachung gelitten hätte, was zeige, dass manche Videoüberwachung vielleicht überflüssig sei. Ihn interessiere, was die Landesregierung zukünftig hinsichtlich Videoüberwachung zu tun gedenke und welche Schwerpunkte sie hinsichtlich Videoüberwachung setzen wolle.

Ganz besonders liege seiner Fraktion am Herzen, dass im gesamten Bildungsbereich und dabei insbesondere an den Schulen ein Bewusstsein für den Datenschutz geschaffen werde. Die Bestellung von behördlichen Datenschutzbeauftragten sei sicher ein richtiger Schritt, doch müsse durch eine entsprechende Personalauswahl sowie Ausbildung und Fortbildung dafür gesorgt werden, dass die erforderlichen Kompetenzen vorhanden seien bzw. erworben würden. Seine Fraktion erwarte von der Landesregierung, dass sie bis zum nächsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz ein Konzept vorlege, aus dem hervorgehe, was an den Schulen hinsichtlich Datenschutz zukünftig unternommen werde.

In der Rechtsprechung habe der Datenschutz, wie auch die jüngsten Entscheidungen des Bundesverfassungsgerichts zum Thema Datenschutz gezeigt hätten, nach wie vor einen hohen Stellenwert. Es sei notwendig, bei Gesetzesvorhaben darauf zu achten, dass der Datenschutz bei der Formulierung neuer Gesetze wie beispielsweise des Polizeigesetzes von vornherein stärker

berücksichtigt werde, als dies derzeit noch der Fall sei. Im Übrigen hoffe er, dass künftig u. a. wegen der Vorbildwirkung auch für alle öffentlichen Stellen im Land die Forderung des Innenministers, Datenschutz sollte Chefsache sein, gelte.

Ein Abgeordneter der CDU bedankte sich seitens seiner Fraktion beim Landesbeauftragten für den Datenschutz und dessen Mitarbeiterinnen und Mitarbeitern für den sehr umfassenden und aufschlussreichen Tätigkeitsbericht sowie beim Innenministerium für seine Stellungnahme dazu, in der das Ministerium intensiv auf den Tätigkeitsbericht eingegangen sei und viele Beanstandungen aufgegriffen habe. Dies zeige, dass die Landesregierung entgegen anderslautenden Unterstellungen dem Datenschutz eine sehr hohe Bedeutung beimesse.

Eine Schwierigkeit des Datenschutzes bestehe darin, dass es außerordentlich stark auf das Verhalten jedes Einzelnen ankomme. Doch leider verhielten sich viele Menschen widersprüchlich. Beispielsweise habe sich der Landesbeauftragte für den Datenschutz zwar mit der Frage auseinanderzusetzen gehabt, ob es datenschutzrechtlich korrekt sei, dass in manchen Schulen Kopien der Personalausweise der Schülerinnen und Schüler gefertigt und abgelegt würden, doch andererseits sei davon auszugehen, dass ein sehr hoher Anteil der betroffenen Schülerinnen und Schüler in sozialen Netzwerken im Internet freiwillig wesentlich mehr personenbezogene Daten einschließlich Fotos der Öffentlichkeit preisgäben, ohne sich über die möglichen Folgen beispielsweise bei einer Bewerbung im Klaren zu sein. Aus seiner Sicht müsse den Menschen viel stärker als derzeit ins Bewusstsein gerückt werden, dass sich die Verarbeitung einmal öffentlich preisgegebener Informationen der Kontrolle durch den Betroffenen entziehe und sich Informationen mitunter auch noch nach vielen Jahren negativ auswirken könnten.

Andererseits sei es in vielen Fällen notwendig, personenbezogene Daten zu erheben und zu verarbeiten, und diese Möglichkeit dürfe – eine datenschutzkonforme Verarbeitung vorausgesetzt – nicht unnötig eingeschränkt werden. In jedem Einzelfall müssten die Notwendigkeit, personenbezogene Daten datenschutzkonform zu verarbeiten, und das Persönlichkeitsrecht der Betroffenen sorgfältig gegeneinander abgewogen werden.

Ein Abgeordneter der FDP/DVP merkte an, der Datenschutz dürfe nicht der Abwägung unterworfen werden. Denn das Bundesverfassungsgericht habe den Datenschutz als ein Grundrecht ausgestaltet. Wie ernst das Bundesverfassungsgericht den Datenschutz nehme, werde auch dadurch deutlich, dass es das Gesetz zur Vorratsdatenspeicherung ohne Übergangsfrist kassiert habe. So ernst sollte auch der Landesgesetzgeber den Datenschutz nehmen.

Er bedankte sich beim Landesbeauftragten für den Datenschutz für den vorliegenden umfassenden Tätigkeitsbericht und äußerte, er sehe es als positiv an, dass der Justizbereich in diesem Tätigkeitsbericht ganze sechs Seiten einnehme. Im Übrigen sehe er die elektronische Fußfessel als datenschutzrechtlich weniger problematisch an, als es der Landesbeauftragte für den Datenschutz getan habe; denn die Alternative für einen Betroffenen wäre die Unterbringung in einer JVA.

Er teile die Auffassung des Abgeordneten der CDU, dass es immer wichtiger werde, die Bevölkerung und dabei insbesondere die Schülerinnen und Schüler auf die Wichtigkeit des Datenschutzes hinzuweisen. Denn mit sozialen Netzwerken werde teilweise viel zu nachlässig umgegangen. Die Informationen, die sich einmal im Internet befänden, ließen sich jedoch nie wieder vollständig löschen. Das Internet vergesse nichts.

Abschließend brachte er vor, hinsichtlich des Datenschutzes an Schulen müsse in der Tat nachgearbeitet werden. Denn Datenschutz sei ein Grundrecht.

Ein Abgeordneter der CDU erbat eine Einschätzung des Landesbeauftragten für den Datenschutz zu der Tendenz, dass immer mehr Menschen zahlreiche personenbezogene Daten sozialen Netzwerken zugänglich machten.

Anschließend merkte er an, im Tätigkeitsbericht fänden sich auch Ausführungen zum Orientierungsplan. Auch aus seiner Sicht würden über Kleinkinder so viele Informationen erhoben, dass die Datenverarbeitung durchaus hinterfragt werden müsse. Hierzu bitte er um ergänzende Informationen des Landesbeauftragten für den Datenschutz.

Der Ministerialdirektor im Innenministerium schloss sich den Dankesworten für den umfassenden und detaillierten Tätigkeitsbericht an und führte weiter aus, das Innenministerium habe Gelegenheit gehabt, schriftlich Stellung zu nehmen. Auf diese Stellungnahme (*Anlage*) verweise er.

Weiter äußerte er, die angesprochene DNA-Reihenuntersuchung sei nicht direkt falsch abgelaufen. Weitere Verfahrensregularien wie beispielsweise ein Erlass seien aus seiner Sicht nicht zwingend erforderlich; vielmehr sei das Verfahren mit einem Fehler verbunden gewesen, was leider auch für die Zukunft nicht völlig ausgeschlossen werden könne. Konkret sei bei 250 DNA-Proben das Verdachtsraster der richterlichen Anordnung überschritten worden.

Zu der Frage, ob bei einem neu aufgelegten flächendeckenden EDV-Verfahren wie ComVor, das vor allem eine Standardisierung zum Ziel habe, und, wenn ja, in welchem Umfang auch der Datenschutz mitberücksichtigt werde, liefen derzeit noch Gespräche zwischen dem Innenministerium und dem Landesbeauftragten für den Datenschutz. Denn das Ziel einer Standardisierung bedeute nicht zwingend einen höheren Datenschutz unter jedem Aspekt. Diese Gespräche seien noch nicht abgeschlossen, und folglich lasse sich auch noch nicht abschätzen, wie die flächendeckende Einführung von ComVor letztlich konkret ausgestaltet werde.

Anschließend brachte er vor, der EuGH habe hinsichtlich der Unabhängigkeit der Datenschutzaufsicht ein Urteil verkündet, das aus Sicht des Innenministeriums nicht die ursprünglich erhoffte Klarheit bringe. Sein Eindruck sei, dass dazu noch Klärungsbedarf bestehe. Es bestehe zwar Einigkeit darüber, eine größtmögliche Unabhängigkeit herbeiführen zu wollen, doch was dies in Sachen Fachaufsicht, Dienstaufsicht und organisatorische Fragen konkret bedeute, werde derzeit auf Bund-Länder-Ebene diskutiert. Er plädiere dafür, die Umsetzung des EuGH-Urteils auf Bund-Länder-Ebene gründlich vorzubereiten und möglichst harmonisch auszugestalten, damit große Bandbreiten möglichst vermieden werden könnten.

Abschließend erklärte er, für die Bestellung betrieblicher Datenschutzbeauftragter in der Privatwirtschaft gebe es klare bundesrechtliche Regelungen. Deshalb liege der Gedanke nahe, solche klaren Regelungen auch für den öffentlichen Bereich zu schaffen. Fakultativ könnten Behörden schon derzeit einen behördlichen Datenschutzbeauftragten bestellen. Um die Kleine Anfrage Drucksache 14/5798 beantworten zu können, habe auch eine Umfrage stattgefunden, wie es in dieser Hinsicht in den einzelnen Ressorts und Verwaltungen sowie teilweise auch auf kommunaler Ebene aussehe. Ob es sinnvoll oder geboten wäre, die Bestellung behördlicher Datenschutzbeauftragter im Land per Gesetz zwingend vorzuschreiben, sei eine offene Frage; bei deren Beantwortung müsse im Übrigen berücksichtigt werden, dass bei einer landesweit gültigen Vorschrift auch alle Kommunen betroffen wären, was in manchen Kommunen möglicherweise zu einem unverhältnismäßig hohen Aufwand führen würde.

Der Landesbeauftragte für den Datenschutz legte dar, der Umgang mit sozialen Netzwerken sei nicht einfach. Denn vielfach seien Menschen ausgegrenzt, wenn sie dort nicht präsent seien. Das gehe so weit, dass eine ent-

sprechende Präsenz und vielleicht 200 Follower bei Twitter bei einer Bewerbung beispielsweise im Marketingbereich vielfach sogar vorausgesetzt würden, was ihn zumindest derzeit noch befremde.

Ein Abgeordneter der SPD erklärte, hinsichtlich der Wattestäbchenproblematik sei im Innenausschuss eine sehr umfassende Diskussion geführt worden. Dabei habe der Innenausschuss eine Entwicklung aufgezeigt bekommen, die das zutage getretene Problem tiefgreifend und befriedigend löse.

Weiter äußerte er, seine Fraktion begrüße die Abordnung eines Spezialisten aus der Polizei zum Landesbeauftragten für den Datenschutz ausdrücklich. Denn dies sei der richtige Weg, um eine bessere Verbindung zwischen Datenschutzaufsicht und Polizei zu schaffen. Angesichts dieser Lösung hinsichtlich der Polizei und angesichts der Bezeichnung des Schulbereichs hinsichtlich Datenschutz als Notstandsgebiet werfe er die Frage auf, ob eine analoge Lösung auch in Zusammenarbeit mit dem Kultusministerium denkbar wäre. Ihn interessiere, welche Maßnahmen hinsichtlich des Schulbereichs konkret geplant seien. Denn angesichts eines „Notstandsgebiets“ sollte relativ schnell Abhilfe geschaffen werden.

Abschließend warf er unter Hinweis auf die immer zahlreicher werdenden sozialen Netzwerke die Frage auf, ob es Überlegungen dazu gebe, ob ein Persönlichkeitsschutz für diejenigen, die die Dimension ihrer Aktivitäten im Internet nicht überblicken könnten, sinnvoll oder geboten wäre.

Der Ministerialdirektor im Innenministerium erklärte, die Einführung datenschutzkonformer Verfahren in Schulen sei ein Thema für Spezialisten, sodass es durchaus sinnvoll wäre, wie bei der Polizei geschehen auch jemanden aus dem Kultusressort zum Landesbeauftragten für den Datenschutz abzuordnen. Dazu müsse sich jedoch das Kultusministerium äußern.

Die Datenschutzproblematik sozialer Netzwerke sei nicht einfach, und zwar vor allem deshalb nicht, weil diese Netzwerke von zahlreichen Menschen genutzt würden, ohne gleich von Nachteilen betroffen zu sein, sodass datenschutzbezogene Aufforderungen und Appelle häufig auf mangelnde Akzeptanz stießen. In diesem Bereich helfe aus seiner Sicht nur geduldige Information.

Ein Abgeordneter der Grünen äußerte, das Berichtsintervall für die Tätigkeitsberichte sei mit dem Ziel des Bürokratieabbaus auf zwei Jahre verlängert worden, doch seine Fraktion habe seinerzeit nur deshalb zugestimmt, weil sowohl seitens des damaligen Landesbeauftragten für den Datenschutz als auch seitens der Landesregierung erklärt worden sei, dass bei Handlungsbedarf kurzfristig auch zusätzlich berichtet werden könne. Ferner sei es den Abgeordneten unbenommen, bei Bedarf auch mit parlamentarischen Initiativen Informationen zu beschaffen. Er habe nicht den Eindruck, dass sich die Verdopplung des Berichtsintervalls negativ auf den Datenschutz ausgewirkt hätte.

Ein Vertreter des Ministeriums für Kultus, Jugend und Sport führte aus, das Ministerium für Kultus, Jugend und Sport habe bereits im November 2009 ein Gespräch mit dem Landesbeauftragten für den Datenschutz zu den im Kultusbereich festgestellten Problemen und Schwierigkeiten geführt. Dieser Kontakt bestehe weiterhin. Erst vor wenigen Tagen habe das Ministerium für Kultus, Jugend und Sport wieder ein Schreiben an den Landesbeauftragten für den Datenschutz gesandt, in dem dargelegt worden sei, wie der Datenschutz aus Sicht des Ministeriums für Kultus, Jugend und Sport in seinem Zuständigkeitsbereich verbessert werden könne.

Im Jahr 2010 habe das Ministerium für Kultus, Jugend und Sport eine sprachlich aufbereitete und inhaltlich aktualisierte Verwaltungsvorschrift zum Datenschutz an Schulen erlassen. Diese solle nunmehr u. a. auf Schullei-



tertaltungen bekannt gemacht werden. Den Schulen werde diese Verwaltungsvorschrift über das Intranet der Kultusverwaltung zugänglich gemacht. Dort seien auch weitere Hinweise beispielsweise zum Verzeichnisse eingestellt worden.

Ferner habe das Ministerium für Kultus, Jugend und Sport sofort angeordnet, dass das Thema Datenschutz Pflichtinhalt für die Schulleiterfortbildung werde, und derzeit werde im Rahmen einer Länderumfrage ermittelt, wie andere Länder hinsichtlich des Datenschutzes an Schulen vorgehen.

Ein Abgeordneter der FDP/DVP erkundigte sich danach, ob mit Blick auf die Datenschutzproblematik der häufig von Schülerinnen und Schülern genutzten sozialen Netzwerke erwogen werde, das Thema Datenschutz auch im Fach Gemeinschaftskunde zu behandeln.

Der Vertreter des Ministeriums für Kultus, Jugend und Sport äußerte, er werde diese Frage mitnehmen.

Der Ausschussvorsitzende merkte an, für weitere Debatten zu diesem Thema wäre eher der Schulausschuss zuständig.

Der Abgeordnete der FDP/DVP warf ein, ihm komme es nur darauf an, dass die in Frageform gekleidete Anregung weitergegeben werde.

Der Landesbeauftragte für den Datenschutz teilte mit, seine Dienststelle höre immer wieder von Schulleitern, die angesprochene Verwaltungsvorschrift sei, weil sie in schwer verständlichem Juristendeutsch abgefasst sei, auch in der aktuellen Fassung für sie nur schwer verständlich und damit auch nur wenig hilfreich. Beispielsweise sähen sich viele Schulen als für die Umsetzung zentraler EDV-Verfahren zuständig an, die ihnen vorgegeben würden, seien sich jedoch nicht darüber im Klaren, dass sie im Sinne des Datenschutzrechts verantwortliche Stelle seien. Dies sei wohl auch eine Folge dessen, dass das Thema Datenschutz in der Fortbildung der Schulleiterinnen und Schulleiter derzeit praktisch keine Rolle spiele.

Abschließend erklärte er, er habe dem Ministerialdirektor im Ministerium für Kultus, Jugend und Sport angeboten, zwei Bedienstete für vielleicht drei Jahre in seine Dienststelle abzuordnen, um im gesamten Kultusbereich den Datenschutz zu verbessern und die Beschäftigten entsprechend fortzubilden. Doch nun sei das Ministerium für Kultus, Jugend und Sport am Zuge, dieses Angebot aufzugreifen. Denn diese Aufgaben, die das Ministerium für Kultus, Jugend und Sport als zu umfangreich für die Oberschulämter ansehe, könnten von dem Referenten seiner Dienststelle, der sich zusätzlich zum gesamten Kultusbereich auch noch mit der Finanzverwaltung, der Statistik und den Hochschulen zu befassen habe, nicht erledigt werden.

Der Ausschuss beschloss ohne förmliche Abstimmung, dem Plenum zu empfehlen, von der Mitteilung des Landesbeauftragten für den Datenschutz vom 1. Dezember 2009, Drucksache 14/5500, und der vom Innenministerium hierzu mit Schreiben vom 12. Februar 2010 vorgelegten Stellungnahme der Landesregierung (*Anlage*) Kenntnis zu nehmen.

11. 04. 2010

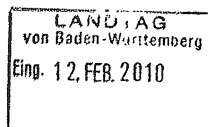
Thomas Bopp


**Anlage****Baden-Württemberg**INNENMINISTERIUM  
DER MINISTER

Innenministerium Baden-Württemberg • Pf. 10 24 43 • 70020 Stuttgart

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

Datum 12.02.2010  
Durchwahl 0711 231-3250  
Aktenzeichen 2-0551.7/43  
(Bitte bei Antwort angeben)



 Stellungnahme der Landesregierung zum 29. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (LT-Drs. 14/5500)

Anlagen  
Stellungnahme der Landesregierung  
Synopsis

Sehr geehrter Herr Landtagspräsident,

die Landesregierung hat in der Kabinettsitzung vom 1. Februar 2010 die Stellungnahme zum 29. 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 gesonderter Post zugeleitet.

Mit freundlichen Grüßen

Heribert Rech MdL

\*) Die o. g. Synopse kann beim Informationsdienst des Landtags eingesehen werden.

Dorotheenstr. 6 • 70173 Stuttgart • Telefon 0711 231-4 • Telefax 0711 231-3019

**Anlage****Stellungnahme der Landesregierung  
zum 29. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz****1. Teil: Zur Situation****1. Datenschutz in Bewegung**

Der Landesbeauftragte für den Datenschutz weist zu Recht darauf hin, dass in den vergangenen beiden Jahren im Datenschutz vieles in Bewegung geraten ist. Nicht zuletzt wurden zahlreiche schwerwiegende Datenschutzverstöße und -pannen bekannt, die die Bürger stark verunsichert haben. Dieser Entwicklung soll in organisatorischer Hinsicht durch eine Bündelung der Kräfte im Bereich des Datenschutzes Rechnung getragen werden: Die Datenschutzaufsicht über den öffentlichen und den nichtöffentlichen Bereich soll beim Landesbeauftragten für den Datenschutz zusammengefasst werden, während sich das Innenministerium auf seine ministeriellen Aufgaben in diesem Bereich konzentriert.

**2. Europäische Entwicklung****2.2 Die Harmonisierung der Sicherheitspolitik nach dem „Stockholmer Programm“:  
Bleibt der Datenschutz auf der Strecke?**

Der Landesbeauftragte für den Datenschutz weist zu Recht auf die zunehmende Bedeutung des europäischen Rechts auch im Sicherheitsbereich hin. Das Zusammenwachsen Europas erfordert nach Ansicht des **Innenministeriums** eine immer engere grenzüberschreitende Zusammenarbeit und damit auch eine Harmonisierung des Rechts. Die Bedeutung des Datenschutzes wurde auf Ebene der EU auch im Bereich der justiziellen und polizeilichen Zusammenarbeit erkannt. Entsprechende Rechtsakte bemühen sich um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten. Soweit der Landesbeauftragte für den Datenschutz hier ein Defizit auf EU-Ebene bemängelt, spricht dies umgekehrt für das in Deutschland inzwischen erreichte vergleichsweise hohe Datenschutzniveau.

**2.3 Die Umsetzung der EU-Dienstleistungsrichtlinie**

Der Landesbeauftragte für den Datenschutz bemängelt, im Anhörungsverfahren zum Entwurf eines Gesetzes über Einheitliche Ansprechpartner für das Land Baden-Württemberg (EAG BW) nicht beteiligt worden zu sein.

## Anlage

### 2

Nach Auffassung des **Wirtschaftsministeriums** war eine solche Beteiligung nicht zwingend geboten, weil es sich bei den im EAG BW enthaltenen, überwiegend verwaltungsorganisatorischen Regelungen lediglich um eine Aufgabenzuweisung für die elektronische Informationsbereitstellung und Verfahrensabwicklung im Zusammenwirken von zuständigen Behörden, Einheitlichen Ansprechpartnern, fachlich berührten Ministerien sowie der für die Redaktion des Dienstleistungsportals zuständigen Stelle handelt. Sie änderten nichts an dem bereits zuvor erlassenen Gesetz zur Änderung des Landesverwaltungsverfahrensgesetzes und anderer Gesetze vom 30. Juli 2009, mit dem die allgemeinen verwaltungsverfahrenrechtlichen Anforderungen der Dienstleistungsrichtlinie durch Einfügen des neuen Verfahrenstyps „Verfahren über eine einheitliche Stelle“ in das Landesverwaltungsverfahrensgesetz umgesetzt wurden. Nur dieses Gesetz trifft eine Regelung zum Schutz personenbezogener Daten und zum Verbot der Offenbarung von Betriebs- und Geschäftsgeheimnissen.

Das Wirtschaftsministerium wird den Landesbeauftragten für den Datenschutz jedoch beteiligen, sofern es von der in § 6 Abs. 2 EAG BW enthaltenen Verordnungsermächtigung Gebrauch machen und Regelungen zur elektronischen Informationsbereitstellung und Verfahrensabwicklung treffen wird.

### 3. Entwicklung auf Bundesebene

#### 3.2 Rechtsentwicklung im Sicherheitsbereich

Der Landesbeauftragte für den Datenschutz kritisiert Inhalt und Reichweite des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt.

Im Zuge der Föderalismusreform wurden dem Bundeskriminalamt präventiv-polizeiliche Aufgaben im Bereich des internationalen Terrorismus übertragen. Es ist daher nach Auffassung des **Innenministeriums** folgerichtig, das Bundeskriminalamt auch mit den hierfür erforderlichen Befugnissen auszustatten. Die Befugnisse des Bundeskriminalamts orientieren sich an den vergleichbaren Befugnissen in den Landespolizeigesetzen. Das Innenministerium begrüßt die Schaffung einer Befugnis zur sogenannten Online-Durchsuchung im Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG). Es besteht damit die Möglichkeit, Erfahrungen mit diesem neuartigen Eingriffsinstrument zu sammeln.

Hinsichtlich des beim Bundeskriminalamt geführten Informationssystems INPOL der deutschen Polizeien fordert der Landesbeauftragte für den Datenschutz, dieses auf eine

## Anlage

3

Rechtsverordnung nach § 7 Abs. 6 BKAG zu stützen und so die diesbezügliche Datenverarbeitung ausdrücklich zu regeln.

Das Informationssystem besteht aus einer Vielzahl von Einzeldateien. Die vom Landesbeauftragten für den Datenschutz angesprochene Datei "Gewalttäter Sport" ist eine davon. In ihr werden zur Zeit mehrere tausend Hooligans und andere bei Sportveranstaltungen auffällig gewordene Straftäter gespeichert. Nach Auffassung des Oberverwaltungsgerichts Lüneburg setzt die Führung von Verbunddateien nach § 7 Abs. 6 BKAG generell eine Rechtsverordnung voraus, in der das Nähere über die Art der Daten geregelt wird, die in der Datei gespeichert werden sollen. Eine solche Regelung wurde seitens des Bundes bislang nicht erlassen, da eine Rechtsverordnung zur Führung von Verbunddateien nach überwiegender Auffassung nicht erforderlich ist (vgl. Hessischer Verwaltungsgerichtshof, Urteil vom 16. Dezember 2004, Az.: 11 UE 2982/02; Verwaltungsgericht Schleswig, Entscheidung vom 23. April 2004, Az.: 1 A 219/02; Ahlf/Daub/Lersch/ Störzer, Kommentar zum BKAG, 1999, RN 24 zu § 7). Über die Revision gegen das Urteil des Oberverwaltungsgerichts Lüneburg hat das Bundesverwaltungsgericht noch nicht entschieden.

Eine Beteiligung der Länder zu dem im Tätigkeitsbericht zitierten Arbeitsentwurf des Bundesministeriums des Innern für eine Rechtsverordnung nach § 7 Abs. 6 BKAG ist bislang nicht erfolgt.

### 3.4 Gesetz über den elektronischen Entgeltnachweis (ELENA)

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit war in das Gesetzgebungsverfahren des Bundes eingebunden. Seinen auf die Realisierung des Verfahrens bezogenen Forderungen ist die Bundesregierung weitgehend nachgekommen. Bei der parlamentarischen Beratung ist dem Datenschutzaspekt besondere Aufmerksamkeit zugekommen. So wurde beschlossen, dass der Datenbank-Hauptschlüssel durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verwaltet wird. Die geforderte Ende-zu-Ende-Verschlüsselung hat sich nach einem Gutachten des Bundesamtes für Sicherheit in der Informationstechnik als nicht praktikabel erwiesen und wäre mit erheblichen Kostensteigerungen für die Arbeitgeber verbunden gewesen. Beim Bundesministerium für Wirtschaft und Technologie wurde zudem ein begleitender Beirat zur Umsetzung der ELENA-Verfahrensregelungen eingerichtet. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist Mitglied dieses beratenden Gremiums, so dass datenschutzrechtliche Anforderungen in diesem Rahmen eingebracht und berücksichtigt werden können. Der ELENA-Beirat soll auf seiner nächsten Sitzung noch einmal alle zu erhebenden Daten auf ihre zwingende Notwendigkeit hin überprüfen.

**Anlage**

4

**3.5 Das geplante Bundesmelderegister**

Der Referentenentwurf eines Bundesmeldegesetzes, der den Ländern im Sommer 2008 zur Stellungnahme vorlag, sieht die Einrichtung eines bundesweiten Melderegisters vor, in dem die bislang bereits auf Kommunal- und Landesebene bestehenden Melderegister zusammengeführt werden sollen. Hierdurch wird eine Steigerung von Qualität und Aktualität der Meldedaten erwartet. Im Zusammenhang mit einer Nutzungs- und Zugriffsmöglichkeit für die Sicherheitsbehörden würde ein bundesweites Melderegister entscheidend zur Aufgabenerfüllung beitragen und ist aus polizeilicher Sicht grundsätzlich zu begrüßen. Aus datenschutzrechtlicher Sicht bestehen gegen die umfangreiche Datenspeicherung sowohl nach Auffassung des **Innenministeriums** als auch des Landesbeauftragten für den Datenschutz erhebliche Bedenken.

Die Bedenken des Landesbeauftragten für den Datenschutz gegen ein Bundesmelderegister wurden in die Stellungnahme des Innenministeriums gegenüber dem Bundesministerium des Innern aufgenommen. Auch das Bundesministerium der Justiz hatte wegen der Mehrfachspeicherung von Meldedaten (Kommune, Land, Bund) erhebliche Einwände gegen den Gesetzentwurf. Ob dieser Dissens zwischen den Bundesministerien des Innern und der Justiz inzwischen beigelegt ist und wann das Bundesministerium des Innern den Ländern einen gegebenenfalls überarbeiteten Gesetzentwurf übermittelt, ist nicht bekannt.

**3.6 Elektronischer Pass und elektronischer Personalausweis**

Das am 1. September 2009 in Kraft getretene Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften vom 18. Juni 2009 (BGBl. I S. 1346) schafft die Möglichkeit, eine Funktion für die qualifizierte elektronische Signatur nach dem Signaturgesetz auf dem Personalausweis aufzubringen. Die Signaturfunktion wird dem Ausweisinhaber nur auf Antrag bei einem Zertifizierungsdienstinhaber zur Verfügung gestellt. Der Landesbeauftragte für den Datenschutz mahnt einen datenschutzkonformen Umgang mit den neuen Möglichkeiten des elektronischen Personalausweises an und fordert unter anderem, das Auslesen des Datenflusses und der jeweiligen PIN zuverlässig zu unterbinden.

Das Bundesministerium des Innern führt zusammen mit ausgewählten Passbehörden, dem Passhersteller und dem Bundesamt für Sicherheit in der Informationstechnik derzeit einen Testbetrieb durch. Weiter ist ein Anwendungstest für den elektronischen Personalausweis vorgesehen. Offene oder zusätzliche Fragestellungen werden nach Ansicht des **Innenministeriums** in diesem Zusammenhang zu klären sein.

## Anlage

5

## 4. Videoüberwachung

Mit dem Landesbeauftragten für den Datenschutz besteht Einigkeit darüber, dass eine normenklare Rechtsgrundlage für die nichtpolizeiliche Videoüberwachung durch öffentliche Stellen geschaffen werden muss, wenn diese auch in Zukunft möglich sein soll. Das **Innenministerium** hat einen Gesetzentwurf erarbeitet, mit dem eine neue Videoüberwachungsvorschrift in das Landesdatenschutzgesetz aufgenommen werden soll. Diese lässt die Videoüberwachung im öffentlichen Bereich unter engen Voraussetzungen zu. Der Gesetzentwurf soll noch im ersten Halbjahr 2010 in das parlamentarische Verfahren eingebracht werden.

Im Polizeibereich ist die Abwehr von Gefahren ohne vorangegangene Gefahrenaufklärung und damit im Vorfeld konkreter Gefahren ansetzender Informationsgewinnung und -verarbeitung überhaupt nicht denkbar. Die Videoüberwachung ist ein Instrument, das hierzu eingesetzt werden kann.

Die Landesregierung stimmt dem Landesbeauftragten für den Datenschutz darin zu, dass Videoüberwachung den Einsatz von Personal nicht ersetzen kann und es insbesondere keinesfalls zu einer flächendeckenden Videoüberwachung kommen darf. Gleichwohl kann eine punktuelle Videoüberwachung ein sinnvolles Instrument sein, um Menschen und Sachen vor Beeinträchtigungen und Beschädigungen zu schützen. Die Landesregierung steht zu ihrer Position, Videoüberwachung zu ermöglichen, wo eine sorgfältige Abwägung des Zwecks der Videoüberwachung mit dem informationellen Selbstbestimmungsrecht der davon Betroffenen ergibt, dass eine Videoüberwachung sinnvoll und verhältnismäßig ist.

Im polizeilichen Bereich soll die Videoüberwachung die Polizei vor allem bei Veranstaltungen und Ansammlungen in die Lage versetzen, im Entstehen begriffene Gefahren frühzeitig zu erkennen, so dass Störungen verhindert oder andauernde Störungen unterbunden werden können. Dabei hat die Polizei Veranstaltungen im Blick, die auf Grund polizeilicher Erfahrung ein besonderes Gefährdungsrisiko aufweisen. Der unterstützende Einsatz von Videokameras ist heute Teil eines modernen Einsatzkonzepts zur Gewährleistung der Sicherheit bei größeren Veranstaltungen. Der Einsatz von Videokameras ersetzt nicht die Präsenz von Einsatzkräften. Aber die Erfahrungen zeigen, dass entstehende Gefahren auch bei hoher Präsenz vor Ort nicht in gleicher Weise und ebenso rasch erkannt werden können wie im Falle eines unterstützenden Einsatzes von Videosystemen.

Die Meinung des Landesbeauftragten für Datenschutz, Videoaufzeichnungen könnten helfen, Straftäter zu ermitteln, dem Opfer einer Straftat helfe dies jedoch nur bedingt, greift zu kurz. Abgesehen davon, dass es den Opfern von Straftaten auch wichtig ist, dass Straftä-

**Anlage**

## 6

ter identifiziert und verurteilt werden, wird die präventive Wirkung der Videoüberwachung, die in der Abschreckung potentieller Straftäter liegt, zu Unrecht marginalisiert.

Nicht geteilt wird ferner die Auffassung des Landesbeauftragten für den Datenschutz, dass von einer Videoüberwachung alle anwesenden Personen ohne erkennbare Zweckbestimmung erfasst würden. Die gesetzlichen Befugnisnormen lassen Videoüberwachungen nur zu bestimmten Zwecken zu. Der Zweck einer bestimmten Videoüberwachung ist vor dem Einsatz zu konkretisieren und festzulegen.

#### 4.1 Videoüberwachung an Schulen

Die Auffassung des Landesbeauftragten für den Datenschutz, die Videoüberwachung an den 17 Mannheimer Schulen sei ohne Rechtsgrundlage erfolgt, wird vom **Innenministerium** geteilt. Da sämtliche Schulen in städtischer Trägerschaft stehen, war für die Maßnahmen die Stadt Mannheim zuständig. Durch die zwischenzeitlich erfolgte Abschaltung der Videokameras ist den Bedenken des Landesbeauftragten für den Datenschutz Rechnung getragen worden. Falls auch weiterhin Bedarf für eine Videoüberwachung an diesen Schulen besteht, sollte der Schulträger nach Inkrafttreten der neuen Videoüberwachungsvorschrift im Landesdatenschutzgesetz prüfen, ob deren Voraussetzungen vorliegen.

#### 4.2 Videoüberwachung im gemeindlichen Freizeitbad

Das **Innenministerium** teilt die Rechtsauffassung des Landesbeauftragten für den Datenschutz. Schlussendlich hat die Gemeinde ihr durch Entfernen sämtlicher Videokameras Rechnung getragen.

#### 4.4 Mannheim behält den Schutz vor Kriminalität im Fokus

Die auf das Polizeigesetz gestützte Videoüberwachung an den genannten Kriminalitätsbrennpunkten in Mannheim hat sich nach Auffassung des **Innenministerium** im Ergebnis bewährt. Die Videoüberwachung hat dort zu einem deutlichen Rückgang der Kriminalität geführt.

In dem zweiten geschilderten Fall wurde eine Videokamera am Bahnhofsvorplatz in Mannheim, die für den Zweck bestimmt war, Übersichtsaufnahmen zur Beobachtung des Verkehrsflusses anzufertigen, für andere Einsatzzwecke ohne ausreichende verfahrensrechtliche Sicherungen verwendet. Das Innenministerium hält daher die Kritik des Landesbeauftragten für den Datenschutz für berechtigt.



**Anlage**

7

**2. Teil: Öffentliche Sicherheit und Justiz****1. Abschnitt: Öffentliche Sicherheit****1. Gesetzgebung****1.1 Polizeigesetz**

Mit der Novellierung des Polizeigesetzes hat die Polizei die Instrumente erhalten, die sie zur Erfüllung ihres Schutzauftrags gegenüber der Bevölkerung und damit der dem Staat gegenüber dem Bürger obliegenden staatlichen Schutzpflicht benötigt. Nach Auffassung des **Innenministeriums** bleibt dabei die Balance zwischen den Rechten der Bürger einerseits und den Erfordernissen einer effektiven Gefahrenabwehr andererseits gewahrt.

Zu der vom Landesbeauftragten für den Datenschutz kritisierten Verdachtsspeicherung ohne Prognose einer Wiederholungsgefahr ist Folgendes anzumerken: Die Speicherung personenbezogener Daten aus strafprozessualen Ermittlungen zur vorbeugenden Bekämpfung von Straftaten erforderte nach altem Recht eine Prognose, dass der Betroffene erneut straffällig wird. Diese sogenannte Wiederholungsprognose konnte gerade bei Massen- und Bagatelldelikten oft nicht gestellt werden. Dies führte dazu, dass Tatverdächtige bei erneuter Straftatbegehung nicht als Mehrfachtäter erkannt werden konnten. Zur Verbesserung der polizeilichen Datenbasis dürfen Straftatverdächtige jetzt auch ohne Wiederholungsprognose für zwei Jahre als Prüffall gespeichert werden. Sofern die betroffene Person während der zweijährigen Prüffrist nicht erneut in den Verdacht gerät, eine Straftat begangen zu haben, sind ihre Daten zu löschen. Das Bestreben der alten Regelung, die Verhältnismäßigkeit der Speicherung des Straftatverdächtigen durch die Wiederholungsprognose sicherzustellen, hat zu keinem optimalen Ausgleich zwischen dem öffentlichen Interesse an der Verfügbarkeit der Daten zur Kriminalitätsbekämpfung und dem Interesse der Betroffenen, nicht durch die Datenspeicherung belastet zu sein, geführt. Die Neuregelung vermeidet den mit der alten Regelung verbundenen Verlust an erforderlichen Informationen und kompensiert die erleichterte Speichermöglichkeit durch eine Verkürzung der Regelspeicherfrist von bis zu zehn Jahren auf zwei Jahre.

**1.2 Landesversammlungsgesetz**

Mit dem geplanten Landesversammlungsgesetz sollen klare Regelungen zum Schutz der Versammlungsfreiheit und der öffentlichen Sicherheit geschaffen werden. Dazu zählen beispielsweise das Militanzverbot, welches ein paramilitärisches Auftreten untersagt, das den Eindruck der Gewaltbereitschaft vermittelt und die Bevölkerung einschüchtern soll,

**Anlage**

## 8

oder auch bereichsspezifische Regelungen über die Datenerhebung und die Bild- und Tonaufzeichnung.

Entgegen der Ansicht des Landesbeauftragten für den Datenschutz will der vom **Innenministerium** erarbeitete Gesetzentwurf die Versammlungsfreiheit nicht einschränken, sondern stärken: das Stören der Versammlung, das Entstehen unfriedlicher Versammlungen, die vom Grundrecht der Versammlungsfreiheit nicht erfasst sind, und Störungen der öffentlichen Sicherheit, die zu einer Auflösung der Versammlung führen könnten, sollen möglichst von vornherein verhindert werden.

Die Kritik des Landesbeauftragten für den Datenschutz an den Datenerhebungsregelungen des Gesetzentwurfs ist in Teilen nicht nachvollziehbar. So sieht der Gesetzentwurf etwa, entgegen dem Vortrag des Landesbeauftragten für den Datenschutz, keine Pflicht der befragten Versammlungsteilnehmer zur Angabe der Personalien vor. Auch besteht beispielsweise keine Notwendigkeit, strengere Anforderungen für die selbsttätige Bildaufzeichnung einzufügen, weil bei Versammlungen der Einsatz von Geräten für selbsttätige Bildaufzeichnungen ohnehin kein Thema ist.

Die Arbeiten an dem Gesetzentwurf für ein Landesversammlungsgesetz Baden-Württemberg ruhen bis zu der Hauptsacheentscheidung des Bundesverfassungsgerichts über die Verfassungsbeschwerden gegen das Bayerische Versammlungsgesetz. Dies erlaubt es, mögliche Forderungen und Maßgaben des Bundesverfassungsgerichts an versammlungsrechtliche Regelungen zu berücksichtigen und in den Gesetzentwurf einzuarbeiten. In diesem Zusammenhang wird sich das Innenministerium dann auch mit den im Rahmen der öffentlichen Anhörung vorgetragenen Einwänden und Anregungen sowie mit der Kritik des Landesbeauftragten für den Datenschutz nochmals eingehend auseinandersetzen.

## 2. Polizeiliche Datenverarbeitung

### 2.1 Szenekundige Beamte und ihre Datenbank

Der Landesbeauftragte für den Datenschutz kritisiert, dass der Polizeivollzugsdienst einem Betroffenen in einem Einzelfall unvollständig Auskunft über die zu seiner Person gespeicherten Daten erteilt hat, weil er eine Datenspeicherung in der Arbeitsdatei „Szenekundige Beamte“ (SKB-Datenbank) nicht berücksichtigte. Dafür gibt es eine einfache Erklärung:

Derzeit werden bei elf Polizeidienststellen SKB-Datenbanken betrieben. Die Anwendung unterstützt die szenekundigen Beamten bei der Verwaltung „ihrer“ Problemfälle, das heißt

**Anlage**

9

Personen, die im Zusammenhang mit Fußballspielen polizeilich auffällig geworden sind. Zur Zeit sind rund 2.000 Personen in den elf Dateien erfasst.

Die Datenbanken werden dezentral betrieben, wodurch ein zentraler oder wechselseitiger Zugriff auf die Datenbestände anderer Polizeidienststellen derzeit technisch nicht möglich ist. Dies hat in Einzelfällen bedauerlicherweise dazu geführt, dass Auskunftersuchen unvollständig beantwortet wurden. Das Landeskriminalamt arbeitet derzeit daran, die bestehenden Datenbanken bis zur neuen Spielsaison 2010/2011 durch eine neue Anwendung, die eine zentrale Datenhaltung ermöglicht, abzulösen. Die Verbesserungsvorschläge des Landesbeauftragten für den Datenschutz werden mit der neuen Anwendung umgesetzt.

## 2.2 Polizeiliche Informationssysteme - Anspruch und Wirklichkeit

Das polizeiliche Auskunfts- und Informationssystem POLAS-BW ist eine der zentralen Datenbanken der Polizei. In diesem System werden Straftatverdächtige, gegen die ein Ermittlungsverfahren geführt wurde, gespeichert, um künftige Ermittlungen zu erleichtern.

### 2.2.3 Die üblichen Verdächtigen - wessen Daten sind in polizeilichen Auskunftssystemen zu finden?

Der Landesbeauftragte für den Datenschutz zeigt aus seiner langjährigen Prüfungspraxis typische Bearbeitungsfehler auf, deren rechtliche Bewertung ganz überwiegend unstrittig ist. Ein typischer Fehler ist beispielsweise, dass nach Ausgang des justiziellen Verfahrens die Speicherung (unzulässigerweise) aufrecht erhalten wird, obwohl ein Freispruch erfolgt oder inzwischen eine andere Person als Täter festgestellt werden konnte.

Die Speicherung Straftatverdächtiger in POLAS-BW ist bei der Polizei ein „Massengeschäft“. Trotz umfangreicher Regelungen (zum Beispiel in der Dienstanweisung für die Anwendung POLAS, im Datenschutz- und Sicherheitskonzept), verfahrensrechtlicher Sicherungen (zum Beispiel Prüfdienst bei den Datenstationen, 4- bzw. 6-Augen-Prinzip) und Schulungsmaßnahmen kann es bei der Bearbeitung zu Fehlern kommen.

Seitens des Landesbeauftragten für den Datenschutz werden verschiedene Verbesserungsvorschläge gemacht. Diese werden derzeit vom **Innenministerium** gemeinsam mit dem Landeskriminalamt geprüft. Es ist davon auszugehen, dass eine Reihe dieser Vorschläge aufgegriffen wird.

**Anlage**

10

**2.2.4 Sind Polizeibeamte Menschen wie du und ich? Betrachtungen zur Speicherpraxis in POLAS-BW**

Der Landesbeauftragte für den Datenschutz kritisiert im Besonderen eine deutlich restriktivere Speicherpraxis in Ermittlungsverfahren gegen Polizeibeamte. Nach Auffassung des **Innenministeriums** gibt es dafür nachvollziehbare Gründe:

- Für Polizeibeamte besteht ein erhöhtes Risiko, einem strafrechtlichen Ermittlungsverfahren ausgesetzt zu sein, da die von polizeilichen Maßnahmen Betroffenen häufig pauschal Anzeige gegen die handelnden Beamten erstatten. Das erhöhte Risiko liegt ferner darin begründet, dass zahlreiche polizeiliche Maßnahmen tatbestandlich eine Straftat darstellen und sich die Verneinung der Strafbarkeit erst aus dem Vorliegen entsprechender Rechtfertigungsgründe (rechtmäßige Amtshandlungen) ergibt.
- Die vom Landesbeauftragten für den Datenschutz wiedergegebene Anzahl der Fälle, in denen eine Speicherung in POLAS-BW wegen einer Verneinung des Tatverdachts nicht erfolgt ist, kann keinen Anspruch auf Vollständigkeit erheben. Eine lückenlose Erfassung dieser Fälle wäre nur im Rahmen einer vollständigen Durchsicht von landesweit rund 24.000 Personalakten möglich gewesen. Dies war mit vertretbarem Verwaltungsaufwand nicht leistbar. Die Dienststellen konnten daher (regelmäßig) nur solche Fälle erfassen, bei denen das strafrechtliche Ermittlungsverfahren auch zu einer dienstaufsichtsrechtlichen Prüfung („Disziplinarakte“) geführt hat. Fälle, in denen sich die Anschuldigungen gegen die betroffenen Polizeibeamten als offensichtlich haltlos herausgestellt und die deshalb nicht zu einer dienstaufsichtsrechtlichen Prüfung geführt haben, sind in den vom Landesbeauftragten für den Datenschutz zitierten statistischen Daten somit nicht erfasst. Den im Tätigkeitsbericht für den Datenschutz wiedergegebenen Zahlen, in denen eine Speicherung von Polizeibeamten in POLAS-BW entgegen der sonst üblichen Speicherpraxis nicht erfolgt sei, stehen daher zahlreiche weitere Verfahren gegenüber, in denen zu Recht keine Speicherung der betroffenen Beamten in POLAS-BW erfolgte. Diese Verfahren finden sich im Tätigkeitsbericht des Landesbeauftragten für den Datenschutz nicht wieder, wodurch hinsichtlich der genannten Zahlen die Relation zur Gesamtverfahrenszahl nicht deutlich wird. Die Statistik wird dadurch zu Ungunsten der Gruppe der Polizeibeamten verzerrt. Prozentual war die Speicherpraxis, gemessen an der Gesamtzahl der Verfahren gegen Polizeibeamte, in einem weitaus höheren Maße korrekt, als es der Bericht des Landesbeauftragten für den Datenschutz nahe legt.
- Die Gründe in Fällen, in denen keine Speicherung in POLAS-BW erfolgt ist, lassen sich häufig nicht beziehungsweise nicht im Einzelnen ermitteln. Dies ist darauf zu-

**Anlage**

11

rückzuführen, dass nur die Speicherung in POLAS-BW mit einem Grundrechtseingriff verbunden ist. Infolgedessen werden nur für die gespeicherten Fälle (stichwortartig) die Gründe dokumentiert.

Einzuräumen ist jedoch, dass die genannten Gründe die abweichende Speicherpraxis bei Polizeibeamten nicht vollständig zu erklären vermögen. Das Innenministerium wird in den regelmäßigen Besprechungen mit den Leitern der Polizeidienststellen auf eine einheitliche Praxis hinwirken. Die Einführung der Prüffallregelung durch die Novellierung des Polizeigesetzes (vgl. § 38 Abs. 2 PolG) dürfte dazu führen, dass die Fälle, in denen die Nichtspeicherung mit der Verneinung der Wiederholungsgefahr begründet wurde, künftig zumindest für zwei Jahre als Prüffall in POLAS-BW erfasst werden. Die Problematik dürfte sich daher relativieren, weil die fehlende Wiederholungsprognose nicht mehr als Grund für die Nichtspeicherung der Daten eines Polizeibeamten herangezogen werden kann.

### 2.3 Identitätsfeststellungen, Durchsuchungen, Fahndungsmaßnahmen und DNA-Proben - Datenschutz im polizeilichen Alltag

Unter der Überschrift „Wattestäbchen und das informationelle Selbstbestimmungsrecht“ berichtet der Landesbeauftragte für den Datenschutz von Ermittlungsmaßnahmen zum Abgleich einer DNA-Spur, die wiederholt in verunreinigten Wattestäbchen gefunden wurde.

Im Zusammenhang mit den Ermittlungen zum Mord an einer Polizeibeamtin und dem Mordversuch an ihrem Kollegen in Heilbronn wurden unter anderem DNA-Reihenuntersuchungen bei Personen durchgeführt, die nach dem Stand der Ermittlungen einem Verdachtsraster entsprachen. Die DNA-Reihenuntersuchung erfolgte auf der Grundlage einer richterlichen Anordnung (§ 81 h der Strafprozessordnung).

Der Landesbeauftragte für den Datenschutz stellt zutreffend dar, dass Polizeidienststellen in den Landkreisen Heilbronn und Ludwigsburg rund 250 Personen in die Reihenuntersuchung einbezogen haben, die nicht dem in der richterlichen Anordnung festgelegten Verdachtsraster entsprachen. Das **Innenministerium** bedauert diesen Fehler. Selbstverständlich muss die Polizei ein richterlich festgelegtes Verdachtsraster bei ihrer Ermittlungstätigkeit unbedingt beachten. Individuelle Fehler können jedoch trotz aller Bemühungen nicht vollständig ausgeschlossen werden. Die gewonnenen Proben wurden nach Feststellung des Fehlers umgehend vernichtet und die Daten gelöscht.

## Anlage

12

**2. Abschnitt: Justiz****1. Gesetzgebung****1.2 Gesetz über die elektronische Aufsicht im Vollzug - die „elektronische Fußfessel“ kommt!**

Der Landesbeauftragte für den Datenschutz hatte im Anhörungsverfahren „keine grundlegenden Bedenken“ vorgetragen und lobend erwähnt, dass der Entwurf „die datenschutzrechtlichen Aspekte der elektronischen Aufsicht sachgerecht regelt“. Im Gesetzgebungsverfahren wurden die Regelungen zur Verarbeitung personenbezogener Daten durch die „zuständige Stelle“ auf Grund des konstruktiven und hilfreichen Austauschs mit dem Landesbeauftragten für den Datenschutz weiter präzisiert. Das Gesetz über die elektronische Aufsicht im Vollzug der Freiheitsstrafe schafft die Rechtsgrundlage für die Datenverarbeitung und stellt sicher, dass sensible Daten nur eingeschränkt verarbeitet werden dürfen.

Soweit der Landesbeauftragte für den Datenschutz grundsätzliche Bedenken zur (Teil-) Privatisierung des Justizvollzugs äußert, werden nach Auffassung des **Justizministeriums** die Besonderheiten der elektronischen Aufsicht außer Acht gelassen. Es entspricht weltweitem Standard, dass private Organisationen die Technik für die elektronische Aufsicht anbieten. Sie verfügen über das notwendige Know-how. Nach umfassenden Informationen über Ausgestaltung und Funktionsweise zahlreicher ausländischer Programme zum Electronic Monitoring ist kein Fall bekannt geworden, in dem die technische Überwachung in staatlichen Händen liegt. Die Einbindung von Firmen im Sicherheitsgewerbe ist aus sachlichen Gründen unvermeidbar. Eingriffe in Grundrechte der Gefangenen, etwa durch Disziplinierung oder Rückführung in die Justizvollzugsanstalt unter Anwendung von unmittelbarem Zwang, erfolgen selbstverständlich durch hoheitlich tätig werdende Kräfte aus dem Justizvollzug.

**1.3 Justizvollzugsgesetzbuch**

Der Landesbeauftragte für den Datenschutz bedauert, dass das neugeschaffene Justizvollzugsgesetzbuch für die Untersuchungshaft keine differenzierte Regelung vorsehe. Dem hält das **Justizministerium** entgegen, dass das Justizvollzugsgesetzbuch dem Umstand, dass Untersuchungsgefangenen die Freiheit entzogen wird, obwohl sie nicht rechtskräftig zu einer Freiheitsstrafe oder freiheitsentziehenden Maßregeln der Besserung und Sicherung verurteilt worden sind, durchaus Rechnung trägt. Es sieht differenzierte Regelungen für den Bereich der Untersuchungshaft vor und gewährleistet für die Untersu-

**Anlage**

13

chungsgefangenen eine im Vergleich zu den Strafgefangenen privilegierte Vollzugsgestaltung.

Die für den Untersuchungshaftvollzug getroffenen Regelungen zum Besuchs-, Schrift- und Telefonverkehr der Gefangenen sind angesichts des Auftrags der Justizvollzugsanstalten, die Aufrechterhaltung der Sicherheit und Ordnung für alle Haftarten zu gewährleisten, angemessen. Dies gilt umso mehr, als die gesetzlichen Regelungen hinreichend flexibel sind, Untersuchungsgefangenen im Einzelfall eine ihren persönlichen Lebensumständen entsprechende Pflege ihrer sozialen Beziehungen aus der Haft heraus zu ermöglichen.

**3. Teil: Bildungsbereich**

1. Von Schlüsselszenen und Lernspuren - der Orientierungsplan für Bildung und Erziehung in baden-württembergischen Kindergärten und weiteren Kindertageseinrichtungen

Der Landesbeauftragte für den Datenschutz geht in seinen Ausführungen davon aus, dass der Orientierungsplan verpflichtend eingeführt werden soll und hält daher, beispielsweise wegen der von den Kindergärtnerinnen eingesetzten Bewertungsbögen, eine gesetzliche Grundlage im Hinblick auf die vorgesehenen Eingriffe in das informationelle Selbstbestimmungsrecht der Kindergartenkinder für erforderlich. Für verbindlich erklärt werden soll jedoch nur der Personalschlüssel, nicht aber der Orientierungsplan. Dies hat der Ministerialdirektor des **Kultusministeriums** dem Landesbeauftragten für den Datenschutz bereits in einem Gespräch Ende November vergangenen Jahres mitgeteilt.

Die Landesregierung und die kommunalen Landesverbände haben mittlerweile eine entsprechende politische Übereinkunft erzielt. Bei dieser Sachlage müssen datenschutzrechtliche Regelungen nicht mehr durch Gesetz getroffen werden.

Wie dem Landesbeauftragten für den Datenschutz in dem erwähnten Gespräch mit dem Amtschef des Kultusministeriums ebenfalls angekündigt worden ist, wird das Kultusministerium im Zusammenwirken mit den Kindergartenträgern eine Handreichung zum Datenschutz im Zusammenhang mit dem Orientierungsplan erarbeiten und den Kindergärten zur Verfügung stellen. Einem dabei vom Landesbeauftragten für den Datenschutz gegebenen Hinweis entsprechend sollen auch die bestehenden kirchlichen Regelungen mit als Arbeitsgrundlage einbezogen werden.

## Anlage

14

## 2. „Kompetenzanalyse Profil AC“ - ohne datenschutzrechtliche Kompetenz?

Die öffentlichen Schulen sowie die oberen und unteren Schulaufsichtsbehörden wurden bereits im Nachgang zum 25. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und im Hinblick auf die strukturellen Veränderungen im Zuge der Verwaltungsreform 2005 mit Runderlass vom 23. Februar 2005 ausführlich über die Belange des Datenschutzes informiert. Am 2. August 2005 trat die in Abstimmung mit dem Landesbeauftragten für den Datenschutz erarbeitete Verwaltungsvorschrift des **Kultusministeriums** "Verarbeitung personenbezogener Daten durch öffentliche Schulen und Einsichtnahme in schulische Prüfungsunterlagen und deren Aushändigung" in Kraft. Sie enthält unter anderem konkrete Regelungen über die Verpflichtung der Schulen, ein Verfahrensverzeichnis nach § 11 LDSG zu führen. Dabei wird sowohl auf die Hinweise des Landesbeauftragten für den Datenschutz zum Verfahrensverzeichnis vom 30. Oktober 2002 als auch auf eine im Intranet der Kultusverwaltung abrufbare Ausfüllanleitung verwiesen.

Das Kultusministerium hat die Beanstandung des Landesbeauftragten für den Datenschutz zum Anlass genommen, alle die Kompetenzanalyse anwendenden Schulen, darunter auch die vom Landesbeauftragten für den Datenschutz direkt angeschriebenen Schulen, nochmals auf ihre Verpflichtung hinzuweisen, ein Verfahrensverzeichnis für das Verfahren „Kompetenzanalyse Profil AC“ an Schulen zu führen und dieses dem Landesbeauftragten für den Datenschutz zu übersenden, soweit kein behördlicher Datenschutzbeauftragter bestellt ist. In diesem Schreiben hat das Kultusministerium die Schulen auf das Verfahrensverzeichnisformular samt Ausfüllhinweisen hingewiesen, die es in seinem Intranet bereithält. Bei den Schulungen zur Kompetenzanalyse wird im Übrigen allen Lehrkräften ein Handbuch ausgehändigt, in dem auch Ausführungen zum Datenschutz bei der Kompetenzanalyse enthalten sind. Damit bietet das Kultusministerium den Schulen eine umfassende Unterstützung bei der Erstellung des Verfahrensverzeichnisses.

Nicht aufgegriffen werden kann hingegen der Vorschlag des Landesbeauftragten für den Datenschutz, "Stellen der Kultusverwaltung" sollten für die Schulen die Rolle des behördlichen Datenschutzbeauftragten übernehmen und die Schulen betreuen. Bei über 4.500 Schulen ist dies nicht möglich.

Bei den unteren Schulaufsichtsbehörden fehlt in aller Regel die erforderliche Sachkenntnis. Die oberen Schulaufsichtsbehörden könnten die hohen Fallzahlen nicht bewältigen. Die schulträgerbezogenen Unterschiede bei der Hard- und Software würden in Hunderten von Fällen Rückfragen bei den Schulen erforderlich machen. Darauf hat der Amtschef des Kultusministeriums den Landesbeauftragten für den Datenschutz bereits in dem Gespräch Ende November 2009 hingewiesen.



**Anlage**

15

Selbstverständlich ist dem Kultusministerium daran gelegen, die Schulen für die Belange des Datenschutzes stärker zu sensibilisieren und sie bei der Wahrung datenschutzrechtlicher Belange zu unterstützen. Hierzu sollen folgende Maßnahmen dienen:

- Am 1. Februar 2010 ist eine neue Verwaltungsvorschrift des Kultusministeriums zum "Datenschutz an öffentlichen Schulen" in Kraft getreten (abgedruckt im Amtsblatt des Kultusministeriums Kultus und Unterricht 2010, S. 59 ff.), die den aktuellen Belangen des Datenschutzes Rechnung trägt und soweit möglich so abgefasst ist, dass auch Laien sie besser lesen und verstehen können.
- Die neue Verwaltungsvorschrift wurde in das Intranet des Kultusministeriums eingestellt. Weitere dort eingestellte Informationen zum Datenschutz wurden überarbeitet.
- Mit den oberen Schulaufsichtsbehörden ist darüber hinaus bereits vereinbart, das Inkrafttreten der neu gefassten Verwaltungsvorschrift zum Anlass zu nehmen, das Thema Datenschutz mit den zuständigen Referenten der oberen Schulaufsichtsbehörden zu besprechen. Diese werden es ihrerseits in Dienstbesprechungen mit den unteren Schulaufsichtsbehörden und den Schulen im Rahmen der Schulleitertagungen erörtern.
- Datenschutz wird ab sofort in den Führungsseminaren für Schulleiter Pflichtinhalt sein.

3. „Offene Mathe-Foren“ und eine Vielzahl anderer Probleme an einem Gymnasium

Die Darstellung im Tätigkeitsbericht ist zutreffend. Das **Kultusministerium** schließt sich der Bewertung des Landesbeauftragten für den Datenschutz an.

Das Regierungspräsidium Tübingen hat aufgrund der vom Landesbeauftragten für den Datenschutz ausgesprochenen Beanstandung inzwischen mit dem Schulleiter ein klärendes Gespräch geführt und ihn auf die Verpflichtung zur Einhaltung der datenschutzrechtlichen Bestimmungen hingewiesen.

Daraufhin hat die Schule ein Verzeichnisse nach § 11 LDSG erstellt und den bislang nicht vorhandenen Auftrag für eine „Datenverarbeitung im Auftrag“ durch die Stadt erteilt. Auch die übrigen Verstöße, wie die rechtswidrige Veröffentlichung von Schülerfotos im Internet und der vom Landesbeauftragten für den Datenschutz kritisierte Umgang mit den Klassentagebüchern und den Schülerakten, wurden inzwischen abgestellt.

**Anlage**

16

**4. Die Tücken des Verfahrens „winprosa“**

Im Rahmen des EDV-Verfahrens winprosa wurde den Schülern eines Gymnasiums von diesem ein Datensatz "Jahrgangspaket" zur Verfügung gestellt, der es den Schülern ermöglichen sollte, von ihrem heimischen Computer aus den eigenen Leistungsstand zu überprüfen und Modellrechnungen für das Abitur und eine optimale Kurswahl durchzuführen. Der Zugang zur Anwendung des Programms und zu den eigenen Daten erfolgte für den einzelnen Schüler durch einen individuellen Zugangscode. Eine automatische Sperrung des Zugangs bei Fälscheingaben erfolgte nicht. Da in den den Schülern zur Verfügung gestellten Datensätzen die Daten aller Mitschüler eines Jahrgangs, wenn auch verschlüsselt, hinterlegt waren, war die Möglichkeit nicht auszuschließen, dass diese auch von Unbefugten zur Kenntnis zu nehmen waren, sofern diese die fremden Zugangscodes anderer Schüler kannten oder sich erschließen konnten.

Auf Grund der Bedenken des Landesbeauftragten für den Datenschutz hat die Schule die Möglichkeit, die Datensätze außerhalb der Schule nutzen zu können ("externe Pakete"), noch am Tag des Kontrollbesuchs des Landesbeauftragten für den Datenschutz beendet.

Eine Nutzung des Programms ist heute für Schüler nur noch in den EDV-Räumen an der Schule möglich, wo es ihnen unter Aufsicht für einen gewissen Zeitraum zur Erfassung ihrer Kurswahl zugänglich gemacht wird.

Die für die Programmgestaltung verantwortliche Firma hat dem **Kultusministerium** außerdem mitgeteilt, dass sie ihre Kunden umgehend von der Auffassung des Landesbeauftragten für den Datenschutz unterrichtet habe, externe Pakete sollten nicht genutzt werden. Sie will im Übrigen die entsprechenden Datensätze in einer der folgenden Versionen so anpassen, dass in diesen keine Daten zu Namen und Adressen von Schülern mehr enthalten sind. Außerdem soll der Zugang der Schüler zu den Datensätzen neu geregelt werden.

**5. Prüfungspläne mit Namen von Abiturienten haben im Internet nichts zu suchen**

Das **Kultusministerium** hat nach Bekanntwerden des Vorgangs alle Gymnasien des Landes schriftlich gebeten, bestehende Listen über die Teilnahme von Abiturienten an mündlichen Prüfungen aus dem Internet zu entfernen und künftig keine derartigen Listen mehr zu veröffentlichen.

**Anlage**

17

**7. Die Kopie des Personalausweises in der Schulkartei**

Die betroffene Schule nimmt nach Angaben des Schulleiters jährlich zwischen 650 und 700 Schüler auf und hat deswegen erstmals zur Beschleunigung des Anmeldeverfahrens und zur Verkürzung der Wartezeiten die Bewerber um eine Kopie des Personalausweises gebeten und diese in die Schulakten aufgenommen. Die Schule hat auf Veranlassung des **Kultusministeriums** die Personalausweiskopien inzwischen aus den Schülerakten entfernt.

**8. Personenbezogene Daten von Studenten im Internet - Datenschutzverstoß an einer Pädagogischen Hochschule**

Das **Wissenschaftsministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz. Die technischen und organisatorischen Maßnahmen der Hochschule waren unzureichend.

Unmittelbar nach der vom Landesbeauftragten für den Datenschutz ausgesprochenen Beanstandung hat die Pädagogische Hochschule das Verfahren eingestellt. Der behördliche Datenschutzbeauftragte führt nunmehr regelmäßig „virtuelle Rundgänge“ auf den Webseiten der Pädagogischen Hochschule durch, um dort datenschutzrechtlich problematische Sachverhalte zu erkennen und unverzüglich zu bereinigen. Über die Belange des Datenschutzes wird in der Hochschulzeitschrift informiert. Die Bereichswebmaster der Hochschule werden darüber hinaus explizit nochmals auf die im Tätigkeitsbericht dargestellte Problematik und auf die bestehende Rechtslage hingewiesen.

**4. Teil: Personalwesen****1. Rechnungsprüfungsamt gleicht Personaldaten ab**

Der Landesbeauftragte für den Datenschutz hält „anlasslose“ Überprüfungen für nicht von vornherein und unter allen Umständen für unzulässig und verweist auf seinen Bericht an den Landtag (LT-Drucksache 14/4675).

Er fordert jedoch, für solche Datenabgleiche künftig geeignete „Spielregeln“ zu entwickeln und differenzierte verfahrensmäßige Sicherungen zur Wahrung der Grundrechte der Betroffenen vorzusehen. Das **Innenministerium** hat diesen Vorschlag aufgegriffen und eine Arbeitsgruppe „Kommunale Rechnungsprüfung und Datenabgleich“ gegründet, der unter anderem Vertreter des Landesbeauftragten für den Datenschutz, der kommunalen Lan-

**Anlage**

18

desverbände, der Gemeindeprüfungsanstalt und des Rechnungshofs angehören. Die Arbeitsgruppe hat im Oktober 2009 ihre Arbeit aufgenommen.

3. Grundsätzlich keine Namen von Beschäftigten ins Internet

Nach Auffassung des **Kultusministeriums** hat der Landesbeauftragte für den Datenschutz die von einer Schule vorgenommene Veröffentlichung personenbezogener Daten über Lehrkräfte zu Recht beanstandet.

Die Schule hat die entsprechenden Seiten inzwischen aus dem Internet entfernt.

Zusätzlich hat das Kultusministerium bei der Neufassung der Verwaltungsvorschrift "Datenschutz an öffentlichen Schulen" die Rechtslage in derartigen Fällen noch klarer als bisher dargestellt.

Auf Bedenken des **Innenministeriums** stößt hingegen, dass der Landesbeauftragte für den Datenschutz in seinen allgemeinen Ausführungen die Veröffentlichung personenbezogener Daten eines Beschäftigten auf der Internetseite einer Behörde nur dann für zulässig hält, wenn eine normenklare Vorschrift es erlaubt oder der Betroffene nach umfassender Aufklärung über die damit verbundenen Gefahren eingewilligt hat. Das Bundesverwaltungsgericht beurteilt diese Frage sehr viel großzügiger. In einer Entscheidung vom 12. März 2008 (2 B 131.07) heißt es wörtlich:

„Soweit eine juristische Person des öffentlichen Rechts befugt ist, ihre behördliche und organisatorische Struktur zu regeln, ist sie auch ohne ausdrückliche gesetzliche Ermächtigung befugt, dem außenstehenden Benutzer, für dessen Bedürfnisse sie eingerichtet worden ist, einen Hinweis darauf zu geben, welche natürlichen Personen als Amtswalter (Beamte, Angestellte) mit der Erfüllung einer bestimmten Aufgabe betraut und damit in einer auf Außenkontakt gerichteten Behörde für das Publikum der zuständige Ansprechpartner sind. Ob die Behörde dies in herkömmlicher Weise durch schriftliche Behördenwegweiser, Übersichtstafeln, Namensschilder, veröffentlichte oder auf Antrag einsehbare Geschäftsverteilungspläne oder in moderner Weise durch entsprechende Verlautbarungen auf ihrer Internetseite tut, liegt allein in ihrem organisatorischen Ermessen. Sie kann bestimmen, ob und gegebenenfalls auf welche Weise sie die tatsächliche Erreichbarkeit ihrer Bediensteten durch Außenstehende sicherstellen will. Kein Bediensteter einer Behörde hat Anspruch darauf, von Publikumsverkehr und von der Möglichkeit, postalisch oder elektronisch von außen mit ihm Kontakt aufzunehmen, abgeschirmt zu werden, es sei denn, legitime Interessen z. B. der Sicherheit gebieten dies. Mit der Nennung des Namens, der Dienstbezeichnung, der dienstli-

## Anlage

19

chen Telefonnummer und der dienstlichen E-Mail-Adresse des Beamten werden keine in irgendeiner Hinsicht schützenswerten personenbezogenen Daten preisgegeben, so dass sich die Frage einer für Eingriffe in individuelle Rechte erforderlichen Ermächtigungsgrundlage nicht stellt."

**5. Teil: Gesundheit und Soziales****1. Abschnitt: Gesundheit****1. ESU - die neue Einschulungsuntersuchung**

Der Landtag hat am 5. November 2008 mit der Neufassung von § 91 Abs. 2 des Schulgesetzes die Neukonzeption der Einschulungsuntersuchung beschlossen. Das Gesetz hat folgenden Wortlaut:

"Die Pflicht zur Untersuchung besteht nach Beginn des Schuljahres auch für die Kinder, die bis zum 30. September des laufenden Kalenderjahres das vierte Lebensjahr vollendet haben; für diese Kinder führt das Gesundheitsamt in begründeten Fällen eine Sprachstandsdiagnose durch, für die das Kultusministerium die Kriterien im Einvernehmen mit dem Ministerium für Arbeit und Soziales festlegt. Darüber hinaus besteht in begründeten Fällen die Pflicht zur Untersuchung für die zur Schule angemeldeten Kinder."

Bereits im Gesetzgebungsverfahren hatte der Landesbeauftragte für den Datenschutz kritisiert, dass aus datenschutzrechtlichen Gründen die Sprachstandsdiagnose und auch die Gruppe der Kinder, die nach Absatz 2 Satz 2 nochmals vor der Einschulung untersucht werden, näher beschrieben werden müssen. Diese Kritik des Landesbeauftragten für den Datenschutz wurde bei der Darstellung der Anhörungsergebnisse in der Gesetzesbegründung ausführlich wiedergegeben (LT-Drucksache 14/3254). Sie hat auch zu zusätzlichen Klarstellungen in der Gesetzesbegründung geführt.

Im Übrigen waren und sind das **Kultusministerium** und das **Ministerium für Arbeit und Soziales** der Auffassung, dass die neu konzipierte Einschulungsuntersuchung dem verfassungsrechtlichen Bestimmtheitsgebot genügt und zusammen mit den Vorschriften des Landesdatenschutzgesetzes eine ausreichende Grundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darstellt.

Die Entscheidung über die unterschiedlichen Rechtsauffassungen oblag dem Landtag. Indem der Landtag die Fassung des Gesetzentwurfs als Gesetz verabschiedete, folgte er der Rechtsauffassung des Kultusministeriums und des Ministeriums für Arbeit und Soziales.

**Anlage**

20

Zur Relevanz des Elternfragebogens sowie des Fragebogens für Erzieher für die Bewertung der Schulreife ist vorab darauf hinzuweisen, dass alle Angaben auf freiwilliger Basis erfolgen. Die Angaben dienen primär der Vorbereitung der Elternberatung und der Erarbeitung eines auf das Kind und seine Familie individuell abgestimmten Förderplans. Nur ausgewählte Angaben werden gruppenstatistisch ausgewertet. Eine Liste der zu erfassenden Merkmale einschließlich der Kennzeichnung der gruppenstatistisch auszuwertenden Merkmale wurde dem Landesbeauftragten für den Datenschutz bei der Abstimmung der Neukonzeption ESU bereits frühzeitig vorgelegt.

Zu den kritischen Ausführungen des Landesbeauftragten für den Datenschutz ist im Einzelnen Folgendes zu sagen:

Bei Schritt 1 der ESU im vorletzten Kindergartenjahr ist nicht die Schulreife, sondern die Entwicklung der Kinder bezüglich schulischer Vorläuferfähigkeiten und der sozial-emotionalen Kompetenzen maßgebend. Es handelt sich, anders als bei Schritt 2 der ESU im letzten Kindergartenjahr, um eine Untersuchung mit Fokus auf gesundheitsfördernde und präventive Aspekte.

In den letzten Jahren hat sich gezeigt, dass die sozial-emotionalen Kompetenzen für den Schulerfolg von erheblicher Bedeutung sind. Daraus haben Baden-Württemberg und auch andere Bundesländer, jüngst beispielsweise Nordrhein-Westfalen, Konsequenzen gezogen und entsprechende Entwicklungsaspekte in die Untersuchung beziehungsweise Anamneseerhebung bei der Einschulungsuntersuchung mit einbezogen, unter anderem den SDQ (Strengths and difficulties questionnaire - Fragebogen zu Stärken und Schwierigkeiten) im Fragebogen für Eltern und Erzieher. Er wird auch in anderen Bundesländern und international verwendet.

Des Weiteren wird Eltern, die die Schulreife ihres Kindes abschätzen wollen, auch von der Stiftung Warentest ein vergleichbarer Fragenkatalog empfohlen.

Hinzu kommt, dass in Baden-Württemberg der SDQ nur ein Angebot an die Eltern ist, wenn diese sich Sorgen um das Verhalten und die Stimmungen ihres Kindes machen:

Wenn die Eltern hierzu eine Beratung durch den schulärztlichen Dienst wünschen, können sie zur Vorbereitung dieses Gesprächs diesen Bogen ausfüllen.

Beim Fragebogen für Erzieher wurde das häufig verwendete Konzept der Grenzsteine von Professor Michaelis ausgewählt. Es handelt sich um ein wissenschaftlich begründetes, breit getestetes und einfach zu nutzendes Instrument, das schon von vielen Einrichtungen eingesetzt wird. Die Relevanz für die körperliche, kognitive und sozial-emotionale Kompetenz, also die Hauptkriterien für schulische Vorläuferfähigkeiten, ist in Fachkreisen unbestritten. Es wird im Übrigen auch von zahlreichen Stuttgarter Einrichtungen verwendet.

## Anlage

21

Ein vernünftiger Medienkonsum ist für die Sprachfähigkeit eines Kindes von hoher Bedeutung. Hierauf hat unter anderem auch die Bundeszentrale für gesundheitliche Aufklärung mit entsprechenden Empfehlungen hingewiesen.

Auch die Berufstätigkeit der Eltern spielt insofern eine Rolle, als damit die Zeitreserven der Eltern für die mögliche Umsetzung häuslicher Förderempfehlungen oder auch das Wahrnehmen therapeutischer Angebote in Erfahrung gebracht werden können.

Der Stuttgarter Weg basiert nicht auf Überlegungen zum Datenschutz, sondern auf dem Entschluss des Stuttgarter Elternbeirates für Kindertageseinrichtungen, allen Eltern zu empfehlen, den Elternfragebogen nicht auszufüllen.

Aus fachlicher Sicht ist sowohl der von der Stadt Stuttgart als auch der vom Land eingeschlagen Weg möglich. Die Stadt Stuttgart ist aufgrund ihrer personellen Ausstattung und der räumlichen Nähe von Gesundheitsamt und Kindertageseinrichtungen anders als ein Flächenkreis in der Lage, jedes Kind einem Arzt vorzustellen: In Stuttgart beträgt das Verhältnis Arzt zu Kindern eines Jahrgangs 1 zu 560, im Landesschnitt 1 zu 1200. Der Stuttgarter Weg ließe sich deshalb nur mit einer erheblichen Personalaufstockung (Verdoppelung) landesweit umsetzen.

Die Neukonzeption der Einschulungsuntersuchung wurde in frühzeitiger und enger Abstimmung mit dem Landesbeauftragten für den Datenschutz erarbeitet. Ungeachtet einzelner Vorbehalte, beispielsweise bezüglich des Fragebogens, wurde dabei das gewählte Verfahren dem Grunde nach akzeptiert.

Es ist vorgesehen, 2010/11 nach Vorliegen eines kompletten Untersuchungszyklus der Einschulungsuntersuchung (Schritt 1 und 2) etwa erforderliche Änderungen einzuarbeiten.

### 2. Krebsregister für Baden-Württemberg

#### 2.2 Hautkrebs-Screening

Das **Ministerium für Arbeit und Soziales** teilt die Einschätzung des Landesbeauftragten für den Datenschutz. Insbesondere ist nicht vorgesehen, die bei der Kassenärztlichen Vereinigung Baden-Württemberg vorliegenden Screeningdaten an das Krebsregister Baden-Württemberg zu übermitteln.

Die Hautärzte werden voraussichtlich ab Mai 2011 - wie alle anderen niedergelassenen Ärzte auch - die Möglichkeit haben, Daten über Krebserkrankungen an das Krebsregister Baden-Württemberg zu melden. Um auch die zwischen 2009 und 2011 angefallenen Daten über Krebserkrankungen möglichst vollständig in das Krebsregister Baden-Württemberg einzuführen, können die Hautärzte auch im Jahr 2011 die in der Vergangen-

## Anlage

22

heit liegenden Diagnose-, Therapie- und Verlaufsdaten zu Krebspatienten melden, sofern eine Unterrichtung des Patienten nach § 4 Abs. 2 des Landeskrebsregistergesetzes in Verbindung mit der Behandlung oder im Nachgang erfolgt. Eine Nutzung der Daten der Kassenärztlichen Vereinigung Baden-Württemberg für das Krebsregister Baden-Württemberg ist nicht zulässig.

Im September 2009 wurde das in Abstimmung mit dem Landesbeauftragten für den Datenschutz gefundene Prüfungsergebnis an den verantwortlichen ärztlichen Vertreter des Screeningprogramms weitergegeben und angeboten, die Möglichkeiten zu erörtern, die Hautkrebs-Screeningdaten retrospektiv ab Mai 2011 dem Krebsregister Baden-Württemberg zuzuführen.

## 2. Abschnitt: Die gesetzliche Krankenversicherung

### 5. Patientengewinnung für strukturierte Behandlungsprogramme

Die betroffene Krankenkasse hat das fehlerhafte Verhalten der Bezirksdirektion eingeräumt. Dem **Ministerium für Arbeit und Soziales** liegen keine Anhaltspunkte für eine weitere Verbreitung des vom Landesbeauftragten für den Datenschutz kritisierten Verfahrens vor.

## 3. Abschnitt: Soziales

### 1. Neuordnung der Grundsicherung für Arbeitsuchende

Das **Ministerium für Arbeit und Soziales** teilt die Auffassung des Landesbeauftragten für den Datenschutz, wonach eine Neuregelung der Trägerschaft weiterhin dringend erforderlich ist und dabei auch datenschutzrechtliche Aufsichtszuständigkeiten eindeutig zu regeln sind.

Im Rahmen seiner Einflussmöglichkeiten bei der Entwicklung der neuen Trägerschaftsorganisation sowie gegebenenfalls im Rahmen der Beteiligung im Bundesrat wird sich das Land für eine den Vorgaben des Bundesverfassungsgerichts entsprechende Organisationsform einsetzen, die auch die Aufsichtszuständigkeiten eindeutig regelt.



## Anlage

23

## 2. Kontrollbesuche bei zwei Arbeitsgemeinschaften

## 2.3 Nichtzulassung einer Überprüfung durch unsere Dienststelle

Der Landesbeauftragte für den Datenschutz hat den Vorgang zu Recht beanstandet. Das **Ministerium für Arbeit und Soziales** wird ihn zum Anlass nehmen, die Arbeitsgemeinschaften über die Kontrollbefugnisse des Landesbeauftragten für den Datenschutz zu unterrichten.

## 3. Datenerhebung einer Arbeitsgemeinschaft bei Dritten

Die Darstellung des Sachverhalts und seine rechtliche Beurteilung sind zutreffend. Die Beanstandung ist zu Recht erfolgt. Der Landesbeauftragte für den Datenschutz hat seine Rechtsauffassung auf der Grundlage einer entsprechenden Beteiligung des **Ministeriums für Arbeit und Soziales** erarbeitet. Es ist beabsichtigt, die Träger über die gemeinsame Auffassung zu informieren.

## 5. Datensammelwut beim Sozialamt

Der rechtlichen Beurteilung durch den Landesbeauftragten für den Datenschutz wird gefolgt. Das **Ministerium für Arbeit und Soziales** beabsichtigt, die Sozialleistungsträger entsprechend zu informieren.

## 6. Teil: Kommunales und anderes

## 1. Abschnitt: Kommunales

## 1. Haupt- oder Nebenwohnung? Diese Frage sorgt immer wieder für Nachfragen und Irritationen.

Der Landesbeauftragte für den Datenschutz beanstandete nach Auffassung des **Innenministeriums** zu Recht die Ermittlungstätigkeit einer Meldebehörde ohne hinreichende Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit des Melderegisters. Die Voraussetzungen für die Datenerhebung nach § 5a Abs. 2 des Meldegesetzes lagen im konkreten Einzelfall nicht vor.

Den in dieser Sache eingelegten Petitionen wurde insoweit abgeholfen.

Die betroffene Meldebehörde wurde darauf hingewiesen, dass sie aufgrund der rechtswidrig erlangten Anhaltspunkte für die Unrichtigkeit des Melderegisters in Bezug auf den

## Anlage

24

Wohnungsstatus des Betroffenen nicht berechtigt war, von Amts wegen zu ermitteln. Sie hat inzwischen alle Melderegisterdaten des Betroffenen, die aufgrund der rechtswidrigen Recherche erhoben wurden, gelöscht und die Abfrageaktion eingestellt. Weitergehende Maßnahmen sind aus Sicht des Innenministeriums nicht erforderlich.

Das Innenministerium hat den Vorgang zum Anlass genommen, im Gesetzgebungsverfahren zum Bundesmeldegesetz die Schaffung einer eindeutigen Regelung zur Überprüfung von Zweifelsfragen bei Haupt- und Nebenwohnungen anzuregen. Konkret wurde die Anfügung eines Absatzes 5 in § 18 des Entwurfs eines Bundesmeldegesetzes vorgeschlagen, der den Meldebehörden das Recht einräumt, den Wohnungsstatus von mit Nebenwohnung gemeldeten Personen in regelmäßigen Abständen (zum Beispiel alle fünf Jahre) anhand einer begründeten Erklärung zum Wohnungsstatus zu überprüfen.

Der Vorschlag des Landesbeauftragten für den Datenschutz, bei einer Ablösung des Melderechtsrahmengesetzes und der Landesmeldegesetze eine Regelung dahingehend zu treffen, es bei mehreren Wohnungen im Inland den Meldepflichtigen zu überlassen, welche Wohnung sie als Hauptwohnung festlegen, wird nicht unterstützt. Eine Bestimmung der Hauptwohnung nach objektiven Merkmalen ist im Hinblick auf die daran anknüpfenden Rechtsfolgen (zum Beispiel Zuständigkeitsregelungen, Finanzzuweisungen) sachgerecht und notwendig. Der Entwurf eines Bundesmeldegesetzes entspricht in diesem Punkt der geltenden gesetzlichen Regelung. Bedenken gegen diese Regelung wurden weder von Baden-Württemberg noch von anderen Bundesländern vorgebracht.

2. Willkürliche Änderung des Auszugstages durch eine Meldebehörde sowie Auskunftsanspruch des Betroffenen

Der Landesbeauftragte für den Datenschutz hat die willkürliche Abänderung des Auszugsdatums durch eine Meldebehörde nach Auffassung des **Innenministeriums** zu Recht beanstandet. Die Voraussetzungen für eine Berichtigung des Melderegisters nach § 5a Abs. 1 Satz 1 des Meldegesetzes lagen nicht vor. Zwar hatte das Regierungspräsidium als zuständige Aufsichtsbehörde die Sach- und Rechtslage zunächst hiervon abweichend bewertet und eine fehlerhafte tatsächliche Würdigung des Sachverhalts durch die Stadt nicht festgestellt. Nachdem ihr jedoch die Rechtsauffassung des Landesbeauftragten für den Datenschutz bekannt wurde, hat sie die Meldebehörde aufgefordert, das Melderegister erneut zu korrigieren und den von der Meldepflichtigen mitgeteilten Auszugstag zu speichern. Die betroffene Meldebehörde hat dem Folge geleistet. Weitergehende Maßnahmen sind aus Sicht des Innenministeriums deshalb nicht erforderlich.

**Anlage**

25

**3. Die Weitergabe von Meldedaten**

Das **Innenministerium** stimmt der rechtlichen Beurteilung der Datenweitergabe des Landesbeauftragten für den Datenschutz zu.

Soweit der Landesbeauftragte für den Datenschutz allerdings fordert, die derzeitige Widerspruchslösung bei der Weitergabe von Melderegisterdaten durch eine Einwilligungslösung zu ersetzen, kann dem nicht gefolgt werden. Die Einwohner werden über ihre Widerspruchsmöglichkeiten nach § 34 des Meldegesetzes regelmäßig durch öffentliche Bekanntmachungen und im Einzelfall bei der Anmeldung informiert. Diese Maßnahmen reichen aus, um die Interessen der Meldepflichtigen zu schützen. Weitergehende Hinweispflichten sind nach Auffassung des Innenministeriums nicht erforderlich. Im Übrigen geht auch der Entwurf eines Bundesmeldegesetzes von der Widerspruchslösung aus.

**2. Abschnitt: Bau- und Wohnungswesen, Vermessungswesen, Geodaten****1. Internet-Veröffentlichung von Bürgerstellungnahmen im Bauleitplanverfahren**

Soweit der Landesbeauftragte für den Datenschutz anhand eines Einzelfall darlegt, dass weder das Kommunalrecht noch das Landesdatenschutzgesetz eine Rechtsgrundlage dafür vorsehen, personenbezogene Daten enthaltende Unterlagen, welche den Mitgliedern des Gemeinderats zur Vorbereitung einer Gemeinderatssitzung überlassen werden, Dritten zugänglich zu machen, teilt das **Innenministerium** diese Auffassung.

Anders als der Landesbeauftragte für den Datenschutz sieht das **Wirtschaftsministerium** jedoch auch im Baurecht keine Rechtsgrundlage dafür, die Unterlagen Dritten zugänglich zu machen oder im Internet zu veröffentlichen.

Die vom Landesbeauftragten für den Datenschutz für seine Bewertung herangezogenen § 4a Abs. 4 und § 3 Abs. 2 des Baugesetzbuchs sind nicht einschlägig. Die Vorschriften schaffen lediglich die Möglichkeit, das gesetzlich vorgeschriebene Öffentlichkeitsbeteiligungsverfahren (das heißt sowohl die frühzeitige Öffentlichkeitsbeteiligung als auch die spätere Auslegung) zusätzlich elektronisch über das Internet vorzunehmen. Die Vorschriften enthalten jedoch keine Befugnis für die Veröffentlichung einer Stellungnahme eines Bürgers, die dieser im Zuge der Öffentlichkeitsbeteiligung in einem baurechtlichen Verfahren gemacht hat. Dies gilt auch, wenn eine Stellungnahme den Unterlagen zur Vorbereitung einer Gemeinderatssitzung beigelegt wird. Stellungnahmen von Bürgern können allenfalls im Rahmen der gesetzlichen Öffentlichkeitsbeteiligung als umweltbezogene Stellungnahmen nach § 3 Abs. 2 Satz 1 des Baugesetzbuchs ausgelegt oder veröffentlicht

## Anlage

26

werden. Dabei ist allerdings der Datenschutz zu beachten. Dies bedeutet, dass der Absender entweder unkenntlich gemacht werden muss oder bei dennoch möglicher Identifizierung auf die Veröffentlichung der betreffenden Stellungnahme im Internet verzichtet wird

### 3. Abschnitt: Landwirtschaft und Umwelt

#### 1. Das Verfahren FIONA (Flächeninformation und Online-Antrag)

Der Landesbeauftragte für den Datenschutz äußert Zweifel, ob für den Abruf personenbezogener Daten aus FIONA in jedem Fall eine Rechtsgrundlage vorhanden ist. Bei den in FIONA enthaltenen Informationen zu Bezeichnung, Gestalt, Größe, örtlicher Lage und Nutzung von Flurstücken handelt es sich nicht um unmittelbar personenbezogene, sondern um personenbeziehbare Daten, die mit Ausnahme der Bezeichnung auch durch bloße Inaugenscheinnahme ermittelt werden können. Dies bedeutet, dass zur Herstellung des Personenbezugs Daten aus anderen Quellen benötigt werden. Beispielsweise ist für die Feststellung der Grundstückseigentümer eine Einsichtnahme in das Grundbuch notwendig. Hierfür muss ein berechtigtes Interesse dargelegt werden. Erst dann erhält ein Antragsteller die Informationen, die für die Herstellung des Personenbezugs in FIONA erforderlich sind. Der Nutzer von FIONA hat daher für die Flurstücke, auf die er in FIONA zugreift, ein berechtigtes Interesse.

Hinzukommt, dass das **Ministerium für Ernährung und Ländlichen Raum** nach den EG-Verordnungen für Flächen bezogene Beihilfen (VO (EG) Nr. 73/2009, 1122/2009 beziehungsweise den Vorgängerverordnungen ein Flächenreferenzsystem einzurichten und dem Landwirt/Antragsteller Daten zu den Referenzflächen und der dortigen landwirtschaftlichen Fläche zur Verfügung zu stellen hat. Die Referenzfläche stellt in Baden-Württemberg das Katasterflurstück dar. Diese Möglichkeit eröffnen sowohl die EG-Verordnungen als auch die nationale Verordnung über die Durchführung von Stützungsregelungen und gemeinsamen Regeln für Direktzahlungen nach der Verordnung Nr. 1782/2003 im Rahmen des Integrierten Verwaltungs- und Kontrollsystems. Der Antragsteller muss die Möglichkeit haben, sich über diese Daten zu informieren: Nach Artikel 12 Abs. 1 Buchstabe d) der Verordnung (EG) Nr. 1122/2009 der Kommission vom 30. November 2009 ist der Antragsteller des Gemeinsamen Antrags verpflichtet, in seinem Antrag alle zweckdienlichen Angaben zur Identifizierung aller landwirtschaftlichen Parzellen seines Betriebes, ihrer Fläche ausgedrückt in Hektar mit zwei Dezimalstellen, ihrer Lage und gegebenenfalls ihrer Nutzung mit dem Hinweis, ob die Parzelle bewässert wird, zu machen. Bei neu erworbenen beziehungsweise gepachteten Flächen kann er diese Angaben nur machen, wenn er Zugang zu diesen relevanten Informationen bekommt. Die elekt-

**Anlage**

27

ronische Form bietet dem Landwirt einfache Zugriffsmöglichkeiten und vor allem den aktuellen Datenbestand.

Das Ministerium für Ernährung und Ländlichen Raum geht daher davon aus, dass FIONA in seiner derzeitigen Ausgestaltung datenschutzrechtlich nicht zu beanstanden ist. Im Übrigen stellt die elektronische Datenbereitstellung in Form von Landkarten unter Angabe der Flächengröße der landwirtschaftlichen Nutzung in allen Bundesländern und den meisten Mitgliedstaaten der Gemeinschaft ein gängiges Verfahren dar.

Aufgrund der oben genannten, für alle Verfahrensteilnehmer zugänglichen Informationen sind zudem keine Rückschlüsse auf die ausgezahlten Fördergelder möglich. Bereits beim Besuch des Landesbeauftragten für den Datenschutz im März 2008 wurden dessen diesbezügliche Bedenken ausgeräumt. Selbst zur Ermittlung der Höhe der einheitlichen Betriebsprämie, die als einzige Fördermaßnahme unmittelbar an die bewirtschaftete Fläche anknüpft, sind umfangreiche weitere Informationen erforderlich, die weder in FIONA enthalten noch über sonstige allgemein zugänglichen Quellen beziehbar sind.

Ein Verfahrensteilnehmer, der die Höhe der seinem Nachbarn zustehenden Fördergelder berechnen möchte, müsste über die nachstehenden Zusatzinformationen verfügen:

- die Anzahl der Flurstücke, für die eine Förderung beantragt wurde,
- den auf den beantragten Flächen bewirtschafteten Flächenanteil,
- ob es sich um Acker- oder Grünland handelt,
- in welchem Umfang passende Zahlungsansprüche vorhanden sind, um für die bewirtschaftete Fläche auch eine Förderung zu bekommen,
- den Wert in Euro, den die im landwirtschaftlichen Betrieb verfügbaren Zahlungsansprüche, durch die Flächen aktiviert werden können, haben,
- ob Verrechnungen mit anstehenden Rückforderungen oder Zahlungen aus anderen Antragsjahren stattgefunden haben.

Außerdem werden im Gemeinsamen Antrag eine Vielzahl weiterer Fördermaßnahmen beantragt, deren Höhe sich nicht unmittelbar aus der Größe der bewirtschafteten Fläche ableiten lässt. Hierfür bietet FIONA auch keine Anhaltspunkte.

Eine tatsächliche Beschwerde der Betroffenen ist somit nicht gegeben.

Bei FIONA besteht auch nicht die Gefahr, dass Verfahrensteilnehmer die in das Flurstücksverzeichnis eingetragenen Daten per Download lokal speichern und ein „privates Kataster“ aufbauen können.

**Anlage**

28

Der Nutzer von FIONA kann lediglich selbst digitalisierte und mit eigenen Sachattributen versehene Geometrien, nicht aber die hinterlegten Katasterinformationen, herunterladen.

FIONA dient in erster Linie dazu, dem Anwender die Beantragung landwirtschaftlicher Flächenprämien zu erleichtern. Unabhängig davon, dass die Anwender von FIONA die Möglichkeit nicht haben, die anderen Verfahrensteilnehmern zustehenden Fördergelder zu berechnen beziehungsweise Rückschlüsse auf die ihnen zustehenden Fördersummen zu ziehen, sind zwischenzeitlich die Fördersummen für Agrarbeihilfen im Rahmen der Transparenzinitiative der EU im Internet frei zugänglich.

Der Landesbeauftragte für den Datenschutz kritisiert jedoch, dass es FIONA jedem bei der Landwirtschaftsverwaltung registrierten Antragsteller von landwirtschaftlichen Flächenprämien ermöglicht, für das gesamte Landesgebiet Daten der automatisierten Liegenschaftskarte einzusehen und jedes Grundstück in Baden-Württemberg vermessen zu können. Er hat deshalb dem Ministerium für Ernährung und Ländlichen Raum Empfehlungen unterbreitet, die zum Ziel haben, die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zu beschränken. Das Ministerium hat diese Empfehlungen mit folgendem Ergebnis geprüft:

- Die räumliche Eingrenzung auf die Landkreise, in denen der Verfahrensteilnehmer im letzten Jahr für Flächen eine Förderung beantragt hat, ist nicht sachgerecht: Landwirtschaftliche Betriebe in Baden-Württemberg verfügen in der Regel über einen sehr hohen Anteil an Pachtflächen, sodass deren Bewirtschaftung sich nicht nur auf Flächen innerhalb eines Landkreises oder einer Gemeinde beschränkt. Hinzu kommt, dass jährlich Pachtflächen landkreisübergreifend erworben beziehungsweise getauscht werden. Eine örtliche Zugriffsbegrenzung ist daher nicht praktikabel. Es gibt nämlich eine Reihe von Fällen, in denen der Landwirt erstmals in einem angrenzenden Landkreis eine Förderung für Flächen beantragen möchte oder größere Unternehmen einen zweiten Betriebssitz in einem anderen Landkreis gründen. Die Zugriffsberechtigung für außerhalb des Landkreises oder einer anderen Gemeinde erworbene beziehungsweise gepachtete Flächen müsste die zuständige Behörde manuell einrichten. Unterstellt man, dass allein bei 1% der Antragsteller - die realistische Zahl wird wahrscheinlich um ein Vielfaches höher liegen -, Flächen außerhalb eines Landkreises erworben oder gepachtet werden, müssten bei rund 50.000 Antragstellern in Baden-Württemberg 500 Zugriffsberechtigungen innerhalb einer Antragszeit von drei Monaten manuell eingerichtet werden.
- Nicht durchführbar ist auch der Vorschlag des Landesbeauftragten für den Datenschutz, die von einem landwirtschaftlichen Betrieb im letzten Jahr bewirtschafteten

**Anlage**

29

Flurstücke im Folgejahr automatisch in dessen Flurstücksverzeichnis aufzunehmen mit der Folge, dass der Zugriff auf dieses Flurstücksverzeichnis für weitere Benutzer gesperrt ist. Dies erklärt sich damit, dass ein Flurstück von mehreren Landwirten bewirtschaftet werden kann und jeder von ihnen den Gemeinsamen Antrag stellen kann, was häufig vorkommt (zum Beispiel gesamter Schwarzwald, Oberschwaben). Auch kommt es oft zum Flächentausch; in diesem Fall müsste das Flurstück zunächst freigegeben werden, bevor der Nachfolger den Zugriff erhalten kann. Nutzt beispielsweise der vorherige Bewirtschafter FIONA gar nicht, kann eine Freigabe für den Nachfolger nicht erfolgen. Gerade für überregional tätige Unternehmen und Betriebe mit hohem Sonderkulturannteil, die aus Gründen des Fruchtwechsels zum Teil jährlich einen umfangreichen Flächentausch durchführen, wäre eine Beschränkung der Informationsmöglichkeiten auf die im letzten Jahr angegebenen Flurstücke kontraproduktiv und würde den Nutzen von FIONA erheblich in Frage stellen.

- Der Vorschlag des Landesbeauftragten für den Datenschutz, der jeweilige Antragsteller solle den Zugriff auf seine Flurstücke dadurch erhalten, dass er sich jeweils anmelden muss, würde die Bearbeitung des Gemeinsamen Antrages mittels FIONA erheblich erschweren. Beispielsweise werden zahlreiche große Grundstücke von Gemeinden, Kirchen oder anderen Grundbesitzern historisch bedingt auf sogenannte „Lose“ aufgeteilt und an verschiedene Landwirte weiterverpachtet.

In Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz soll jedoch dessen Vorschlag näher geprüft werden, den Zugriff auf die Daten zu protokollieren.

**4. Abschnitt: Verkehr****1. Webcams an Bundesautobahnen und Videoüberwachung an Lichtsignalanlagen**

Der Landesbeauftragte für den Datenschutz wurde beim Projekt „Webcams an Bundesautobahnen“ von Beginn an beteiligt. Er hat im Wesentlichen darauf hingewiesen, dass zur Vermeidung eines Personenbezugs die Fahrzeuginsassen und die Kfz-Kennzeichen nicht erkennbar sein dürften. Diesem Anliegen wurde durch eine eingeschränkte Auflösung der Bilder Rechnung getragen, was jedoch im Tätigkeitsbericht des Landesbeauftragten für den Datenschutz nicht erwähnt wird. Das **Innenministerium** legt Wert auf die Feststellung, dass auf den Webcambildern keine Fahrzeuginsassen und keine Kfz-Kennzeichen erkennbar sind.

Im Laufe der frühzeitigen Beteiligung hat der Landesbeauftragte für den Datenschutz darüber hinaus noch Bedenken geäußert, wonach die Bilder unabhängig vom Kfz-Kenn-

## Anlage

30

zeichen „individuelle Merkmale mit Bezug zu einer Person“ liefern könnten (beispielsweise Oldtimer, Schriftzüge auf größeren Fahrzeugen). Diese Bedenken werden vom Innenministerium nicht geteilt. Hinzu kommt, dass die Kameras nur einmal pro Minute ein Standbild erzeugen und somit eine lückenlose oder gezielte Beobachtung ausgeschlossen ist. Ergänzend weist das Innenministerium darauf hin, dass es in Hessen und in Rheinland-Pfalz entsprechende Angebote der Straßenbauverwaltungen gibt. In Rheinland-Pfalz hat der dortige Landesbeauftragte für den Datenschutz in seinem Tätigkeitsbericht Webcams an Bundesautobahnen für zulässig erklärt.

### 3. Datenschutz hat grundsätzlich Vorrang im Verfahren

Der Landesbeauftragte für den Datenschutz wirft in diesem Beitrag unter anderem die Frage nach dem Verhältnis des Landesdatenschutzgesetzes zum Verwaltungsverfahrensgesetz des Landes auf. Hierbei vertritt er die Auffassung, das Landesdatenschutzgesetz habe bei der Verarbeitung von personenbezogener Daten grundsätzlich Vorrang im gesamten Verwaltungsverfahren und damit auch vor § 14 des Landesverwaltungsverfahrensgesetzes.

Diese Rechtsauffassung wird vom **Innenministerium** so nicht geteilt. Grundsätzlich gilt, dass sich die Behörde im Falle einer Bevollmächtigung nach § 14 Abs. 3 des Landesverwaltungsverfahrensgesetzes nicht nur an den Bevollmächtigten wenden kann, sondern dies tun soll. Dies schließt die Befugnis der Behörde zur Übermittlung personenbezogener Daten an den Bevollmächtigten ein, allerdings beschränkt auf das Verwaltungsverfahren, für das die Bevollmächtigung erteilt wurde. Insoweit geht das Landesverwaltungsverfahrensgesetz dem Landesdatenschutzgesetz nach § 2 Abs. 5 Satz 1 des Landesdatenschutzgesetzes vor.

Eine andere Auffassung würde im Ergebnis eine Bevollmächtigung immer dann ins Leere laufen lassen, wenn personenbezogene Daten betroffen sind, was im Verwaltungsverfahren die Regel sein dürfte.

Über das Ergebnis im konkreten Fall besteht jedoch Einigkeit, da in dem konkreten Verwaltungsverfahren nicht von einer wirksamen Bevollmächtigung ausgegangen werden dürfte. Die Behörde hätte sich vor einer Übermittlung personenbezogener Daten nach § 14 Abs. 1 Satz 3 des Landesverwaltungsverfahrensgesetzes die Bevollmächtigung nachweisen lassen müssen.



## Anlage

31

Die betroffene Stadt hat der Auffassung des Landesbeauftragten für den Datenschutz inzwischen Rechnung getragen und eine interne Anweisung erlassen, nach der in vergleichbaren Fällen zunächst die ausdrückliche Einwilligung des Betroffenen einzuholen ist.

#### 7. Teil: Informations- und Kommunikationstechnik (IuK)

##### 1. Der datenschutzrechtliche „GAU“

Die Darstellung des Landesbeauftragten für den Datenschutz ist zutreffend. Die rechtliche Beurteilung wird geteilt.

Die Stadt hat eingeräumt, dass es ein Fehler war, sich auf die mündlichen Zusagen der Lieferfirma zu verlassen. Sie hat sich auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz intensiv mit dem Thema Datenschutz auseinandergesetzt und organisatorische Maßnahmen ergriffen, um künftig den Datenschutz in der Stadtverwaltung zu gewährleisten.

##### 4. EDV in der Praxis: Probleme bei Datei-Zugriffsberechtigungsstrukturen und die Tücken gekaufter Software

Die Darstellung des Sachverhalts durch den Landesbeauftragten für den Datenschutz ist zutreffend, seine rechtliche Beurteilung wird geteilt. Folgende Maßnahmen wurden beziehungsweise werden ergriffen:

Das **Ministerium für Arbeit und Soziales** hat bereits 1999 anlässlich einer gemeinsam mit dem Landesbeauftragten für den Datenschutz durchgeführten Fortbildungsveranstaltung – unter anderem zur Aktenführung und zu Zugangsberechtigungen – die Gesundheitsämter darauf hingewiesen, dass es sich bei Patientendaten um besonders sensibles Datenmaterial handelt, bei dem ein abteilungsübergreifender Zugriff grundsätzlich nicht zulässig ist. Durch eine strikte Handhabung der Zweckbindung und Zugriffsberechtigung sei sicherzustellen, dass die Daten nur im Rahmen des jeweiligen Sachzusammenhangs genutzt werden.

Die damaligen Ausführungen und Hinweise des Landesbeauftragten für den Datenschutz wurden den Gesundheitsämtern mit der Bitte um Beachtung übersandt. In den Folgejahren wurden die Gesundheitsämter mehrfach auf die datenschutzrechtlichen Erfordernisse hingewiesen.

**Anlage**

32

Die vom Landesbeauftragten für den Datenschutz ausgesprochene Beanstandung wird das Ministerium für Arbeit und Soziales zum Anlass nehmen, die Gesundheitsämter bei der im Frühjahr 2010 stattfindenden Amtsärztetagung nochmals auf den datenschutzgerechten Umgang mit sensiblen personenbezogenen Daten hinzuweisen und eventuell vorhandene Unklarheiten zur Handhabung des Datenschutzes auszuräumen.

Für die Beschaffung und auch für Verbesserungen der vom Landesbeauftragten für den Datenschutz angesprochenen Software sind die Stadt- und Landkreise zuständig.

Ungeachtet dessen wird das Ministerium für Arbeit und Soziales den Hersteller der Software über die vom Landesbeauftragten für den Datenschutz festgestellten Mängel unterrichten.

Ebenso wird das Ministerium für Arbeit und Soziales die Gesundheitsämter sowie den Städtetag und den Landkreistag bei der Amtsärztetagung 2010 auf die festgestellten Mängel aufmerksam machen und – soweit möglich – auf eine individuelle Überarbeitung der Programme vor Ort hinwirken. In diesem Zusammenhang wird auch darauf hingewiesen, dass bei der Beschaffung künftiger Software die datenschutzrechtlichen Anforderungen zu beachten sind.

#### 6. Polizeiliche Datenverarbeitung

##### 6.1 Die polizeiliche Vorgangsbearbeitung ComVor

Die Anwendung ComVor dient der Vorgangsbearbeitung der Polizeidienststellen. Der Landesbeauftragte für den Datenschutz kommt zu dem Ergebnis, dass die Polizei mit der neuen Vorgangsbearbeitung ein leistungsfähiges System entwickelt hat, das datenschutzrechtlichen Anforderungen gerecht wird. Grundsätzliche Mängel wurden bei seiner Kontrolle nicht festgestellt.

##### 6.2 Der NATO-Gipfel

Im April 2009 fand anlässlich des 60-jährigen Jubiläums der NATO der Doppelgipfel in Straßburg, Kehl und Baden-Baden statt. Die Gewährleistung der Sicherheit dieser epochalen Veranstaltung, zu der die Staats- und Regierungschefs sowie Verteidigungs- und Außenminister aller NATO-Mitgliedsstaaten nebst Begleitpersonen und sonstigen Gästen nach Baden-Württemberg kamen, stellte eine einzigartige Herausforderung für die Polizei und andere beteiligte Stellen dar. Durch die umfassende Vorbereitung konnte ein sicherer und friedlicher Verlauf der Veranstaltungen gewährleistet werden.

## Anlage

33

Die Kritik des Landesbeauftragten für den Datenschutz, die Polizei habe eine „EDV by patchwork“ betrieben, wird nicht geteilt. Die zur Vorbereitung und Durchführung des Einsatzes anlässlich des NATO-Gipfels 2009 realisierte IT-Konzeption war daran ausgerichtet, auf der Grundlage einer einheitlichen technischen Plattform zu arbeiten und eine Vielfalt der Systeme zu vermeiden.

Auf Grund der Dimension dieses Polizeieinsatzes, der Größe des Einsatzraumes, der großen Dynamik der Planungsprozesse und der vielfältigen polizeilichen Aufgaben war die Verwendung unterschiedlicher Anwendungssysteme zur sachgerechten Bewältigung nicht zu vermeiden und notwendig. Neben der klassischen Bürokommunikation und vorhandenen Informationssystemen (beispielsweise POLAS, INPOL) wurden auch weitere Fachverfahren und andere temporäre Dateien (beispielsweise Anwohner- und Waffenbesitzerdateien) eingesetzt. Die Vielfalt der eingesetzten Systeme und die damit verbundene Komplexität stellte hohe Anforderungen an die Planung und Umsetzung technisch-organisatorischer Maßnahmen zur Gewährleistung einer gesetzeskonformen Datenverarbeitung. Nach Auffassung des **Innenministeriums** hat die realisierte IT-Konzeption aber zu keinem unbeherrschbaren „Wildwuchs“ geführt. Eine einheitliche Software, mit welcher die meisten fachlichen Bedarfe zur Bewältigung der unterschiedlichsten Aufgaben derartiger Polizeieinsätze abgedeckt werden könnten, steht absehbar nicht zur Verfügung.

8. Die Neuregelung der informationstechnischen Zusammenarbeit zwischen Bund und Ländern - wo bleibt der Datenschutz?

Der Sachverhalt ist im Wesentlichen zutreffend wiedergegeben.

Der Landesbeauftragte für den Datenschutz spricht allerdings von einem „Ausführungsgesetz“ zum Staatsvertrag. Hierzu ist klarstellend darauf hinzuweisen, dass es sich dabei um das „Zustimmungsgesetz“ handelt, dessen einziger Inhalt die Zustimmung zum Vertrag zur Ausführung von Artikel 91 c Grundgesetz (IT-Staatsvertrag) ist. Weitere Regelungen sind nicht enthalten. Der Staatsvertrag beruht auf Artikel 91 c Absatz 2 des Grundgesetzes und wurde zusammen mit diesem zwischen Bund und Ländern im Rahmen der Kommission zur Modernisierung der Bund-Länder-Finanzbeziehungen (Föderalismuskommission II) verhandelt.

Der Landesbeauftragte für den Datenschutz hatte mit Schreiben vom September 2009 verschiedene Vorschläge zum Datenschutz unterbreitet und darum gebeten, diese, soweit noch verhandelbar, in die Verhandlungen über den IT-Staatsvertrag einzubringen. Da der IT-Planungsrat jedoch bereits im April 2010 seine konstituierende Sitzung abhalten soll, das Umsetzungsgesetzgebungsverfahren bis dahin also abgeschlossen sein muss, hatte

**Anlage**

34

Herr Ministerpräsident den ausgehandelten Staatsvertrag zum damaligen Zeitpunkt bereits unterzeichnet. Daher konnten die Vorschläge des Landesbeauftragten für den Datenschutz in den Verhandlungen über den IT-Staatsvertrag nicht mehr berücksichtigt werden.

Im Übrigen ist darauf hinzuweisen, dass die öffentlichen Stellen des Landes auch ohne ausdrückliche Regelung im Staatsvertrag verpflichtet sind, das geltende Datenschutzrecht zu beachten.

Das **Innenministerium** hat dem Landesbeauftragten für den Datenschutz in einem Schreiben zugesichert, dass sich die Vertragschließenden bewusst sind, dass im Rahmen der Tätigkeit des IT-Planungsrats die Belange des Datenschutzes zu berücksichtigen und die bestehenden bundes- und landesrechtlichen technischen und organisatorischen Datenschutzstandards einzuhalten sind. Ihm wurde außerdem versichert, dass er immer rechtzeitig über die im IT-Planungsrat anstehenden und den Datenschutz betreffenden Themen informiert wird. Im Übrigen kann der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrates mit beratender Stimme teilnehmen.