Landtag von Baden-Württemberg Drucksache 16 / 2118
16. Wahlperiode

Beschlussempfehlung und Bericht

des Ständigen Ausschusses

zu der Mitteilung des Landesbeauftragten für den Datenschutz vom 21. Januar 2016 – Drucksache 15/7990

32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg für die Jahre 2014/2015

B e s c h l u s s e m p f e h l u n g

Der Landtag wolle beschließen,

von der Mitteilung des Landesbeauftragten für den Datenschutz vom 21. Januar 2016 – Drucksache 15/7990 – und der vom Innenministerium hierzu mit Schreiben vom 27. April 2016 vorgelegten Stellungnahme der Landesregierung (siehe Anlage 1 zum Ausschussbericht) Kenntnis zu nehmen.

01. 06. 2017

Der Berichterstatter:	Der stellv. Vorsitzende:
Hans-Ulrich Sckerl	Jürgen Filius

B e r i c h t

Der Ständige Ausschuss beriet öffentlich die Mitteilung des Landesbeauftragten für den Datenschutz vom 21. Januar 2016, Drucksache 15/7990, in seiner 12. Sitzung am 1. Juni 2017.

Stellv. Vorsitzender Jürgen Filius teilte mit, in Verbindung mit der Beratung der Mitteilung des Landesbeauftragten für den Datenschutz vom 21. Januar 2016, Drucksache 15/7990, werde auch das Schreiben des Innenministeriums vom 27. April 2016 – Stellungnahme der Landesregierung zum 32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz – (*Anlage 1*) behandelt. Schließlich nehme der Ausschuss auch den mündlichen Bericht des Landesbeauftragten für den Datenschutz gemäß § 31 Absatz 3 Satz 4 des Landesdatenschutzgesetzes und den mündlichen Bericht des Landesbeauftragten für die Informationsfreiheit gemäß § 12 Absatz 3 des Landesinformationsfreiheitsgesetzes in Verbindung mit § 31 Absatz 3 Satz 4 des Landesdatenschutzgesetzes entgegen.

Ausgegeben: 20. 06. 2017

Er begrüßte den Landesbeauftragten für den Datenschutz und die Informationsfreiheit sowie dessen Vorgänger im Amt, Herrn Klingbeil, der die Mitteilung des Landesbeauftragten für den Datenschutz vom 21. Januar 2016 seinerzeit vorgelegt gehabt habe, im Ausschuss.

LfDI Dr. Brink legte dar, er freue sich sehr, im Ständigen Ausschuss Bericht erstatten zu dürfen. Der vorliegende schriftliche Bericht, der sich auf die Jahre 2014 und 2015 beziehe, sei von Herrn Klingbeil zwar bereits im Januar 2016 vorgelegt worden, habe jedoch nichts an Aktualität eingebüßt.

Ein erstes zentrales Thema sei die Europäische Datenschutz-Grundverordnung. Denn damit gehe die wahrscheinlich größte Umwälzung einher, die es im Bereich Datenschutz jemals gegeben habe. Die Europäische Datenschutz-Grundverordnung habe extreme Auswirkungen in allen Bereichen. Beispielsweise würden dadurch die Gesetzgebungsbefugnisse der Landtage deutlich eingeschränkt. Derzeit seien sowohl der Bund als auch die Länder dabei, Bundesrecht bzw. Landesrecht an die Datenschutz-Grundverordnung anzupassen. Dabei handle es sich um eine sehr schwierige und anspruchsvolle Aufgabe, die noch einige Zeit in Anspruch nehmen werde, sodass diese Arbeiten zumindest bezogen auf die Bundesebene voraussichtlich nicht bis zum 25. Mai 2018, ab dem die Datenschutz-Grundverordnung gelte, abgeschlossen seien. Die Datenschutz-Grundverordnung wirke sich nicht nur auf Parlamente aus, sondern auch auf die Behörden insgesamt, übrigens auch auf sein Haus. Dort sei beispielsweise mit der Einrichtung einer Stabsstelle für Europafragen reagiert worden, um sowohl öffentliche Stellen als auch nicht öffentliche Stellen zu der neuen Rechtsgrundlage mit der gebotenen Intensität beraten zu können. Gerade bei den Unternehmen, die neuen Anforderungen ausgesetzt seien, gebe es einen hohen Beratungsbedarf.

Vieles, was in der Datenschutz-Grundverordnung stehe, sei in Deutschland bekannt; denn Deutschland sei in Bezug auf den Datenschutz seit Jahrzehnten gut aufgestellt, und dies finde sich zum größten Teil auch in der Datenschutz-Grundverordnung wieder.

Wesentliche Veränderungen gebe es in Bezug auf die betrieblichen und behördlichen Datenschutzbeauftragten. Denn ab Mai 2018 müssten alle öffentlichen Stellen mit wenigen Ausnahmen im Sicherheitsbereich behördliche Datenschutzbeauftragte bestellen. In diesem Zusammenhang weise er darauf hin, dass die staatliche Datenschutzaufsicht wegen der knapp bemessenen Zahl der Personalstellen nur sehr mittelbar für das Datenschutzniveau bei Unternehmen und Behörden eine Rolle spiele. Vielmehr sei maßgeblich, wie der Datenschutz in den Unternehmen und Behörden gehandhabt werde. Dabei spielten die betrieblichen und behördlichen Datenschutzbeauftragten eine wichtige Rolle. Er sei dankbar, dass die Bundesregierung Wort gehalten habe und das Konzept des betrieblichen Datenschutzbeauftragten 1 : 1 in die Zeit nach Mai 2018 transferiert habe. Dies sei umso höher zu bewerten, als die meisten Mitgliedsstaaten der EU davon abgesehen hätten, eine verpflichtende Bestellung eines betrieblichen Datenschutzbeauftragten vorzusehen.

Die Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu bestellen, sei zwar mit Kosten verbunden, doch die von seiner Behörde gemachten Erfahrungen zeigten, dass letztlich der Nutzen überwiegen werde.

Eine zweite Neuerung, die die Datenschutz-Grundverordnung mit sich bringe, bestehe darin, dass Verstöße gegen Datenschutzvorschriften künftig mit exorbitanten Bußgeldern zu ahnden seien. Deren Höhe sei vergleichbar mit Strafen im Bereich des europäischen Kartellrechts. Dabei handle es sich nicht um eine Kannbestimmung, sondern um eine Sollbestimmung. Die Datenschutz-Grundverordnung enthalte die Vorgabe an die Aufsichtsbehörden, Datenschutzverstöße wirksam und abschreckend zu sanktionieren. Die Bußgelder, die auch Millionenbeträge ausmachen könnten, spielten künftig eine wesentliche Rolle. In Baden-Württemberg sei die Veränderung deshalb besonders stark spürbar, weil der Landesdatenschutzbeauftragte bisher keine Bußgeldstelle sei, sondern die Bußgeldverfahren über das Regierungspräsidium Karlsruhe abgewickelt würden. Ab Mai 2018 werde die Bußgeldstelle an seine Behörde angegliedert, und es werde in den Händen seiner Behörde liegen, damit vernünftig umzugehen.

Auf den Einwurf des Abg. Dr. Bernhard Lasotta CDU, dann finanziere sich die Datenschutzaufsichtsbehörde künftig selbst, stellte er klar, damit würden selbstverständlich keine Einnahmen für die Aufsichtsbehörde generiert. Vielmehr flössen die verhängten Bußgelder natürlich in den Landeshaushalt. Es sei zwar nicht ausgeschlossen, dass seiner Behörde ein Bruchteil der eingenommenen Gelder in Form einer verbesserten Ausstattung wieder zufließe, doch das liege nicht in der Hand seiner Behörde.

Das Problem bei den Sanktionen im Falle von Datenschutzverstößen sei der Umfang der Sanktionen. Die Datenschutz-Grundverordnung sehe vor, dass sich diese Bußgelder an einem Rahmen orientierten, der zwei bis vier Prozent des weltweiten jährlichen Umsatzes des Unternehmens ausmache. Dies sei nicht nur sehr massiv, sondern für manche Unternehmen auch existenzbedrohend. Denn auf einen Jahresgewinn oder das Doppelte eines Jahresgewinns könnten Unternehmen nicht ohne Weiteres verzichten.

Mit derartigen Bußgeldern werde sehr behutsam umgegangen werden müssen. Im Unterschied zur gegenwärtigen Situation werde es künftig nicht mehr so sein, dass die Aufsichtsbehörde im Rahmen eines Entschließungsermessens beurteile, ob eine Verletzung einer Datenschutzvorschrift sanktionswürdig sei oder nicht. In diesem Bereich unterlägen künftig vielmehr auch die Aufsichtsbehörden einer europäischen Harmonisierung. Nicht nur die Bußgelder, die verhängt würden, sondern auch die, die nicht verhängt würden, würden von europäischer Seite aus begutachtet, und es könne durchaus vorkommen, dass seine Behörde aus Brüssel die Vorgabe bekomme, sich bestimmte Verstöße, die sie als nicht ahnungswürdig erachtet habe, erneut vorzunehmen und möglicherweise ein Bußgeld zu verhängen.

Die Datenschutz-Grundverordnung habe eine weitgehende Umstellung des Bundes- und des Landesrechts zur Folge. Das Bundesdatenschutzgesetz werde prinzipiell durch die Datenschutz-Grundverordnung aufgehoben und werde nur in wenigen Bereichen weiterbestehen können. Es sei bereits erkennbar, dass beim Umsetzungsprozess erhebliche Probleme aufträten. Mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU werde beabsichtigt, ein neues Bundesdatenschutzgesetz auf den Weg zu bringen. Derzeit werde auf Bundesebene noch davon ausgegangen, dass für die Bundesebene nach wie vor ein weiter Regelungsspielraum bestehen werde, doch daran habe seine Behörde erhebliche Zweifel. Sie gehe vielmehr davon aus, dass die Regelungsspielräume sowohl für den Bundes- als auch für den Landesgesetzgeber sehr beschränkt seien und sich erst in den nächsten Jahren herausstellen werde, ob die Regelungsansätze, die die Mitgliedsstaaten weiterzuverfolgen beabsichtigten, von europäischer Seite aus akzeptiert würden. Entscheidend werde letztlich das sein, was der Europäische Gerichtshof dazu sage. Nach den bisherigen Erfahrungen sei damit zu rechnen, dass er bei der Frage, welche Spielräume den Mitgliedsstaaten zugestanden würden, eher zurückhaltend sein werde.

Deshalb zweifle seine Behörde sehr stark daran, dass bestimmte Regelungen im neuen Bundesdatenschutzgesetz (BDSG) wie beispielsweise die, nach der die Datenverarbeitungen im Bereich der freien Berufe wie z. B. in Arztpraxen, bei den Rechtsanwälten und Steuerberatern nicht mehr von den Aufsichtsbehörden kontrolliert werden dürften, europarechtskonform sein sollten. Denn es wäre eher überraschend, wenn die Mitgliedsstaaten, obwohl die europäische Ebene eine volle Kontrolle durch die Aufsichtsbehörden vorsehe, den Kontrollumfang reduzieren dürften, ohne dass eine Öffnungsklausel wirklich erkennbar wäre. Ob dies zulässig sei, werde sich jedoch vermutlich erst durch den Europäischen Gerichtshof klären lassen. Insgesamt sei ein deutliches Übergreifen europäischer Rechtsetzung in den nationalen Normsetzungsraum zu konstatieren.

Ein weiteres Thema sei die im Oktober 2015 ergangene außerordentlich interessante Entscheidung des Europäischen Gerichtshofs zum Stichwort „Safe Harbor". Dabei sei es um die Frage gegangen, unter welchen Bedingungen Europäer personenbezogene Daten in Drittländer exportieren und dort verarbeiten lassen dürften. Die Entscheidung des Europäischen Gerichtshofs laute, vereinfacht ausgedrückt, Drittstaaten, insbesondere die USA, die nicht das Datenschutzniveau hätten, das von europäischer Seite aus gefordert werde, seien im Prinzip keine geeigneten Empfänger von personenbezogenen Daten aus Europa. Diese Entscheidung sei jedoch nur sehr schwer umzusetzen und stelle insbesondere die Wirtschaft vor große Probleme. Denn es gebe inzwischen so umfassende Vernetzungen, dass praktisch kein Unternehmen mehr ohne Kontakte in die USA auskomme. Betroffen sei im Übrigen nicht nur der Datenaustausch zwischen Mutter- und Tochterunternehmen, sondern beispielsweise auch der Datenaustausch, wenn in den USA Dienstleistungen in Anspruch genommen würden, wenn beispielsweise das weit verbreitete Programm Microsoft Office 365 genutzt werde, welches jedenfalls in seiner ursprünglichen Form einen ständigen Datenaustausch mit Servern erfordere, die sich nicht zwingend in Europa befänden. Wenn die Entscheidung des Europäischen Gerichtshofs ernst genommen werde, was dringend zu empfehlen sei, seien entsprechende Datentransfers, die lange Zeit nicht problematisiert worden seien, nunmehr problematisch geworden.

Die Europäische Kommission habe das erkannt und deshalb versucht, einen Ersatz für das Safe-Harbor-Abkommen, das die Datentransfers zwischen Europa und den USA bisher reguliert habe, zu finden. Dieses heiße: „EU-US Privacy Shield“. Bei genauer Betrachtung werde jedoch deutlich, dass dies keine dauerhafte Lösung sein könne. Denn es beruhe nicht auf gesetzlichen Veränderungen in den USA aufgrund der EuGH-Rechtsprechung, sondern schlicht auf Zusagen der US-Administration noch unter Barack Obama. Die Europäische Kommission sei derzeit dabei, herauszufinden, ob die Zusagen, die damals gegeben worden seien, mittlerweile überhaupt noch gälten. Denn gewisse Zweifel lägen nicht ganz fern.

Insgesamt handle es sich um einen schwierigen Bereich, in dem seine Behörde als Aufsichtsbehörde gerade auch die größeren Unternehmen intensiv berate; denn bei näherem Hinsehen gebe es kaum gangbare Wege, um die entsprechenden Datentransfers rechtssicher auszugestalten.

Positiv hervorzuheben sei in diesem Zusammenhang die Reaktion US-amerikanischer Unternehmen, aus Furcht davor, den europäischen Markt zu verlieren, das aus Datenschutzsicht außerordentlich begrüßenswerte Angebot zu machen, bestimmte Leistungen aus Europa heraus zu erbringen, sodass die personenbezogenen Daten den europäischen Raum gar nicht mehr verlassen müssten. Diese von wirtschaftlichen Überlegungen getriebene Entwicklung sei aus seiner Sicht sehr positiv.

Weiter führte er aus, der Sicherheitsbereich werde nicht von der Datenschutz-Grundverordnung reguliert, sondern von einer europäischen Richtlinie, die zukünftig auch durch Landesrecht umgesetzt und ausgefüllt werden könne.

Ein interessanter Aspekt sei der Bereich Precops, mit dem versucht werde, Big-Data-Überlegungen in die Polizeiarbeit zu integrieren. Dies sei ein naheliegender und auch nach Auffassung seines Vorgängers durchaus gangbarer Weg mit dem Ziel, zu versuchen, durch Datenanalysen bestimmte Verhaltensweisen von Kriminellen vorherzusagen, um idealerweise vor einem Straftäter am Tatort zu sein. Dass dies alles datenschutzrechtlich hochproblematisch sei, müsse nicht gesondert betont werden. Umso schöner sei es, dass es ausweislich des vorliegenden Tätigkeitsberichts für die Jahre 2014 und 2015 in Zusammenarbeit mit dem LKA gelungen sei, unter dem Stichwort Precops eine Analysesoftware zu entwickeln und einzusetzen, die sich im Wesentlichen auf die Analyse von Wohnungseinbrüchen bezogen habe und mit anonymisierten Daten arbeite, sodass keine personenbezogenen Daten als Grundlage für die Vorhersage von zukünftigem kriminellem Verhalten herangezogen werden müssten. Dies sei ein sehr schönes Beispiel dafür, wie moderne Technologien auch im Sicherheitsbereich eingesetzt werden könnten, ohne dass dies zu datenschutzrechtlichen Problemen führen müsse.

Zu erwähnen sei ferner, dass es im Sicherheitsbereich jede Menge datenschutzrechtlich hoch spannende und auch kontrovers diskutierte Themen gebe. Seine Behörde habe sich in der Vergangenheit beispielsweise zu Bodycams, Videoüberwachungsanlagen und auch zu Aspekten geäußert, die in den Sicherheitsgesetzen geregelt würden, die dem Landtag bald vorgelegt würden. Dadurch könne seine Behörde wichtige Hinweise in Bezug auf Datenschutzaspekte geben.

Zum Thema „Connected Car“ führte er aus, dieses Thema stehe beispielhaft für die Digitalisierung der Lebenswelt. Dabei gehe es um das vernetzte und automatisierte Fahren, verbunden mit dem Ende des anonymen Fahrens. Denn seit drei oder vier

Jahren komme immer mehr Anonymität abhanden. Wer auf dem Tablet Zeitung lese, ermögliche, dass sehr genau nachvollzogen werden könne, welche Inhalte besonders interessierten, was mehrfach gelesen werde, was überhaupt nicht gelesen, sondern überblättert werde, und was archiviert werde. Wer einen Smart-TV nutze, tue dies ebenfalls nicht anonym, weil der Fernseher analysiere, was geschaut werde und was beim Zappen schnell übersprungen werde. Auch die Internetznutzung und das Telefonieren erfolgen nicht anonym. Überall würden Datenspuren hinterlassen.

Es sei unstreitig, dass auch beim automatisierten Fahren die Datenschutzproblematik eine Rolle spiele. Die Automobilindustrie stehe deshalb in einem sehr engen Austausch mit Datenschützern; beispielsweise seien entsprechende Arbeitskreise gegründet worden. In Baden-Württemberg gebe es z. B. die sogenannten Ladenburger Gespräche.

Die Autobauer hätten sehr lange die Auffassung vertreten, die Daten, die in Fahrzeugen verarbeitet würden, seien weniger personenbezogene Daten als vielmehr technische Daten. Mittlerweile bestehe jedoch Einigkeit darüber, dass es sich selbstverständlich um personenbezogene Daten handle. Denn beispielsweise Ortungssysteme und Sicherheitsfeatures seien immer auch mit Fahrzeughaltern bzw. Fahrern verknüpft. Wer gerade fahre, sei auch deshalb von Interesse, um automatisch die favorisierte Raumtemperatur oder die bevorzugte Sitzposition einzustellen und den favorisierten Radiosender voreinzustellen.

Ein wichtiger Datenschutzaspekt sei der Arbeitnehmerdatenschutz. Lange Zeit habe, was die Zahl der Eingaben und die Zahl der Nachfragen nach Beratungstätigkeit angehe, das Thema Videoüberwachung an der Spitze gestanden, und nunmehr sei dies der Arbeitnehmerdatenschutz. Dies beobachteten auch andere Datenschutzaufsichtsbehörden. Seine Behörde werde vermehrt auch von Betriebsräten und Gewerkschaften kontaktiert.

Beschäftigte, die ihre personenbezogenen Daten, ihr Verhalten und ihre Leistung durch den Arbeitgeber kontrolliert sähen, stellten sich nicht auf den Standpunkt, der Umgang mit ihren Daten sei ihnen egal, weil sie nichts zu verbergen hätten, sondern sie interessierten sich dafür, was zulässig sei, ob der Arbeitgeber beispielsweise E-Mails lesen dürfe, das Dienstfahrzeug orten dürfe oder den PC kontrollieren dürfe. Die technische Entwicklung habe dazu geführt, dass inzwischen sehr stark darauf geachtet werden müsse, dass die Kontrollbefugnisse des Arbeitgebers, die es selbstverständlich gebe, nicht in einem so starken Maße wahrgenommen würden, dass die Interessen der Mitarbeiterinnen und Mitarbeiter in den Hintergrund träten.

Seine Behörde habe diese Problematik und die zahlreichen entsprechenden Anfragen, die an sie herangetragen würden, zum Anlass genommen, eine Orientierungshilfe zusammenzustellen, in der die wesentlichen Fallgestaltungen in kurzer, knapper und ansprechender Form dargestellt würden und in der Lösungsmöglichkeiten aufgezeigt würden. Es sei vorgesehen, diese Orientierungshilfe Ende des Monats öffentlich vorzustellen. Zum einen werde darin anhand konkreter Fälle dargestellt, mit was für Überwachungsmaßnahmen von Arbeitgeberseite gerechnet werden müsse und welche Reaktionsmöglichkeiten es auf Arbeitnehmerseite gebe, und zum anderen werde aufgezeigt, wie datenschutzkonforme Lösungen in diesem Bereich aussähen.

Anschließend brachte er vor, ein Thema sei in Baden-Württemberg auch ausweislich des Tätigkeitsberichts in der Vergangenheit sehr kontrovers behandelt worden, und dies sei die Frage, ob öffentliche Stellen Social-Media-Angebote nutzen dürften, ob beispielsweise die Polizei twittern dürfe, eine Behörde eine Facebook-Fanpage betreiben dürfe oder ein Eichamt via Snapchat kommunizieren dürfe. Er habe dies zum Anlass genommen, innerhalb seiner Behörde noch einmal einen Diskussionsprozess anzustoßen und die Frage zu stellen, welche kontrollierbaren und auch durchsetzbaren Vorgaben für diesen Bereich gemacht werden dürften. Denn auf den verschiedenen Ebenen von der Landesregierung über Mittelbehörden bis hin zu kommunalen Stellen gebe es sehr unterschiedliche Auffassungen in Bezug auf Social-Media-Angebote, und aus seiner Sicht sei es sinnvoll, in diesem Bereich bestimmte Grundsätze festzulegen und Nutzungsmöglichkeiten klar zu beschreiben und voneinander abzugrenzen. Auch dazu werde seine Behörde noch vor der Sommerpause ein Ergebnis präsentieren.

Zum Thema Informationsfreiheit erklärte er, angestoßen durch den Landtag von Baden-Württemberg sei die Informationsfreiheit im Dezember 2015 auch in Baden-Württemberg angekommen. Bei der Informationsfreiheit handle es sich um den voraussetzungslosen Zugang zu prinzipiell allen amtlichen Informationen. Diese Grundsatzentscheidung des Parlaments habe sehr große Auswirkungen, und der Prozess, diese frohe Botschaft auch in alle Behörden hinein zu kommunizieren, sei noch nicht abgeschlossen. Die Zielsetzung habe zum einen darin bestanden, eine transparentere Verwaltung zu haben, und zum anderen darin, öffentliche Beteiligungsmöglichkeiten zu eröffnen. Die Informationsfreiheit gebe Bürgerinnen und Bürgern sowie auch Gruppen wie beispielsweise Bürgerinitiativen die Chance, auf amtliche Informationen, bei denen es sich in aller Regel um valide Informationen handle, zuzugreifen und sie für die eigenen Zwecke zu nutzen. Die erweiterte Transparenz erleichtere im Übrigen auch die Korruptionsbekämpfung in der Verwaltung und führe zu einer neuen Kommunikation zwischen Bürgern und Verwaltung. Die Umsetzung sei jedoch ein schwieriges Unterfangen, das auch mit sehr vielen Umstellungen verbunden sei und das in erster Linie in den Köpfen der in der Verwaltung Beschäftigten verankert werden müsse. Die entsprechenden Abläufe müssten eingeübt werden; ferner bedürfe es Schulungen.

In anderen Ländern und auch beim Bund gebe es bereits seit vielen Jahren Informationsfreiheitsgesetze, und es sei geradezu unvermeidbar, die Informationsfreiheit flächendeckend sicherzustellen. Denn es gebe keinen Grund, zu glauben, dass die Digitalisierung und das Internetzeitalter ohne Auswirkungen auf die öffentliche Verwaltung blieben. Die öffentliche Verwaltung müsse den neuen Anforderungen an Transparenz entsprechen; dies gelte umso mehr, je stärker von den Möglichkeiten der E-Akte und der elektronischen Kommunikation Gebrauch gemacht werde.

Seine Behörde sei u. a. die Informationsstelle, die über die gesetzlichen Neuerungen informiere und Fragen dazu beantworte. Sie sei Beratungsstelle für die Bürgerinnen und Bürger, aber keineswegs nur für diese. Die Hälfte der Anfragen, die an seine Behörde gerichtet würden, kämen von öffentlichen Stellen, die wissen wollten, ob sie erbetene Auskünfte geben und die gewünschten Informationen liefern müssten, welche Einschränkungsmöglichkeiten es gebe, ob Gebühren erhoben werden dürften usw. Es gebe einen sehr großen Informationsbedarf mit steigender Tendenz. Im vergangenen Jahr seien rund 50 Eingaben eingegangen, und im laufenden Jahr habe sich allein in den ersten fünf Monaten diese Zahl verdoppelt. Seine Behörde versuche, Schwung in die Nutzung der neuen Möglichkeiten hineinzubringen und fungiere auch als Schlichtungsstelle, um zwischen Bürgern auf der einen Seite und Verwaltungen auf der anderen Seite, die nicht alle Bürgerwünsche erfüllen könnten oder meinten, sie nicht erfüllen zu können, zu vermitteln.

Die Etablierung der Informationsfreiheit in der Praxis erfordere noch etwas Zeit; denn der Weg dorthin sei in der Tat ein Kulturwandel von einer Verwaltung, die für sich grundsätzlich ein Geheimhaltungsbedürfnis sehe, hin zu einer Verwaltung, die grundsätzlich alles, was sie tue, öffentlich präsentieren könne. Selbstverständlich gebe es jedoch auch in Zukunft Bereiche, die davon ausgenommen seien, beispielsweise der Sicherheitsbereich.

Seine Behörde biete in diesem Zusammenhang Schulungen an, um die Unsicherheit in Bezug darauf, wie mit der neuen Situation umzugehen sei, aufzulösen. Dabei handle es sich um halbtägige Schulungen in den Behörden. Zuerst habe seine Behörde auf ministerialer Ebene nach den Erfahrungen gefragt, und nunmehr würden die Regierungspräsidien geschult.

Gleichzeitig versuche seine Behörde die Nachfrage in Bezug auf die Informationsfreiheit zu unterstützen. Denn das Recht auf Informationsfreiheit werde bisher keineswegs umfassend genutzt. Selbst Journalisten sei häufig nicht bekannt, dass sie diese Möglichkeit des Zugangs zu Informationen hätten. Wenn entsprechend informiert werde, lasse sich sicher noch viel mehr Bewegung in das Thema Informationsfreiheit hineinbringen. In diesem Zusammenhang sei anzumerken, dass Informationsfreiheit in erster Linie ein kommunales Thema sei; denn auf kommunaler Ebene gebe es traditionell sehr enge Beziehungen zwischen Bürger und

Kommune, und diese könnten durch die Informationsfreiheit weiter gestärkt werden. Mit den Kommunen, die in Bezug auf die Informationsfreiheit unabhängig von gesetzlichen Vorgaben bereits sehr weit seien – Beispiele seien Freiburg, Ulm, Heidelberg oder Karlsruhe –, sei seine Behörde in engem Kontakt. Im Wege des Meinungsaustauschs werde gemeinsam mit der kommunalen Ebene versucht, weiterzukommen.

Weiter führte er aus, der Gesetzgeber habe festgelegt, dass das Informationsfreiheitsgesetz bis 2020 evaluiert werden solle. Es sei auch sehr sinnvoll, sich mit dieser neuen Materie noch einmal grundsätzlich zu beschäftigen. Seine Behörde bereite diese Evaluierung bereits vor, und er wisse, dass auch das Ministerium für Inneres, Digitalisierung und Migration so vorgehe. Es sei wichtig, in diesem Bereich intensiv Informationen zu sammeln und eine gute Basis dafür zu schaffen, dass das Parlament sich im Jahr 2019 oder im Jahr 2020 dieses Gesetz noch einmal sehr genau anschauen könne. Es gebe Bereiche, in denen das Gesetz von 2015 im Vergleich zu denen in anderen Ländern etwas zu zaghaft gewesen sei, und das habe dazu geführt, dass Baden-Württemberg bei Evaluierungen der Gesetzeslage bundesweit zwar bislang nie auf dem letzten Platz insgesamt gelandet sei, jedoch auf dem letzten Platz der Länder, die überhaupt über ein Informationsfreiheitsgesetz verfügten. Hinter Baden-Württemberg befänden sich zwar noch Bayern und Sachsen, aber dort gebe es gar kein Informationsfreiheitsgesetz. Seine Behörde wolle die Evaluierung des Informationsfreiheitsgesetzes von Baden-Württemberg intensiv unterstützen.

Abschließend erklärte er, viele seien in der Vergangenheit bereits auf seine Behörde zugekommen und hätten zum Datenschutzbereich und zum Informationsfreiheitsbereich das Gespräch gesucht. Dazu lade er alle ein; denn es sei zentrale Aufgabe seiner Behörde, auch den Landtag zu beraten und mit ihrem Know-how zur Verfügung zu stehen. Seine Behörde sei sehr gern bereit, dies vertrauensvoll und so nachhaltig wie möglich zu tun.

Stellv. Vorsitzender Jürgen Filius bedankte sich unter dem Beifall des Ausschusses bei Herrn Dr. Brink für den mündlichen Bericht und merkte an, in diesen Dank schließe er Herrn Klingbeil ein, der den vorliegenden schriftlichen Tätigkeitsbericht für die Jahre 2014 und 2015 vorgelegt habe.

Abg. Hans-Ulrich Sckerl GRÜNE legte dar, die Datenschutz-Grundverordnung werde den Landtag noch massiv beschäftigen. Er wäre an einer allgemeinen Information darüber interessiert, was in diesem Zusammenhang vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu erwarten sei und welcher Zeitraum für die Umsetzung zu veranschlagen sei. Ferner bitte er um eine Information darüber, wie der Landesbeauftragte für den Datenschutz und die Informationsfreiheit den aktuellen Stand der bundesgesetzlichen Umsetzung, die gerade aus den Reihen der Datenschutzbeauftragten der Länder zum Teil auch sehr kritisch bewertet werde, sowie das gesamteuropäische Vorhaben beurteile. Denn es sei nicht einfach, auf der Basis der Datenschutz-Grundverordnung in allen 27 Mitgliedsstaaten der Europäischen Union die Bedingungen für den Datenschutz zu nivellieren. Dazu interessiere ihn, ob hierzu ein Austausch unter Beteiligung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit stattfinde, was die damit verbundenen Herausforderungen für seine Behörde bedeuteten und mit welchen Anforderungen gerechnet werden müsse.

Weiter führte er aus, das Thema Vorratsdatenspeicherung werde auch in Zukunft ein wichtiges Thema sein. Zu der europäischen Richtlinie gebe es ein EuGH-Urteil, und es gebe ein neues Bundesgesetz, gegen das vor dem Bundesverfassungsgericht geklagt werde. Ihn interessiere, wie der Landesbeauftragte für den Datenschutz und die Informationsfreiheit dieses Gesetz und die verfassungsrechtliche Auseinandersetzung darüber aus Datenschutzsicht beurteile.

Abschließend erklärte er, er habe zur Kenntnis genommen, auf welchem Platz Baden-Württemberg im bundesweiten Vergleich in Bezug auf die Informationsfreiheit stehe. Es sei jedoch nicht einfach gewesen, in Baden-Württemberg überhaupt ein Informationsfreiheitsgesetz zu etablieren. Er sehe die Ausführungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit als Ansporn, das Informationsfreiheitsgesetz in Baden-Württemberg noch besser zu machen. Er bitte um eine Einschätzung, wie sich die Inanspruchnahme der neuen gesetzlichen Möglichkeiten entwickelt habe, ob bereits positive Folgen zu konstatieren seien und ob die Behörden in Baden-Württemberg genug unternähmen, um diesem Anspruch auf proaktive Information gerecht zu werden, oder ob es Verbesserungsmöglichkeiten gebe.

Abg. Sascha Binder SPD äußerte, er bedanke sich sowohl für den schriftlichen Tätigkeitsbericht als auch für den mündlichen Bericht in der laufenden Sitzung. Von seinem Vorredner wolle er wissen, ob er mit seiner Frage, mit welchen Anforderungen gerechnet werden müsse, gesetzgeberische Anforderungen an den Landtag oder personelle und finanzielle Anforderungen gemeint habe. Wenn er personelle und finanzielle Anforderungen gemeint habe, sei anzumerken, dass der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in einem Schreiben an die Fraktionsvorsitzenden bereits seine Anforderungen formuliert habe, nämlich 14,5 Personalstellen zusätzlich, um den neuen Vorgaben auch personell gerecht werden zu können. Ihn interessiere, ob es zwischenzeitlich darüber hinausgehende Anforderungen gebe.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit habe in seinem mündlichen Bericht Berufsgruppen angesprochen, die nach dem Willen des Bundesgesetzgebers aus der einheitlichen Aufsicht durch die Datenschutzaufsichtsbehörden herausgenommen werden sollten. Es gebe ein Spannungsfeld zwischen dem Auftrag an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Datenschutzaufsicht zu betreiben, und der Verschwiegenheitspflicht von Rechtsanwälten. Deshalb sei seitens der Rechtsanwälte vorgeschlagen worden, bei den Kammern einen eigenen Datenschutzbeauftragten anzusiedeln, um diesem Spannungsfeld Rechnung zu tragen. Vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit wolle er wissen, ob er dieses Spannungsfeld sehe und wie er es auflösen würde.

Abg. Arnulf Freiherr von Eyb CDU brachte vor, er bedanke sich für den detaillierten schriftlichen Tätigkeitsbericht. Ihn interessiere lediglich die Auffassung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit dazu, dass es einerseits Ängste gebe, dass personenbezogene Daten missbraucht werden könnten, dass sich jedoch andererseits viele Menschen permanent leichtfertig im Tagesablauf über diese Ängste hinwegsetzten und ihre personenbezogenen Daten mehr oder weniger großzügig preisgäben. In diesem Zusammenhang interessiere ihn auch, welche Lösungsmöglichkeiten der Landesbeauftragte für den Datenschutz und die Informationsfreiheit sehe.

Abg. Nico Weinmann FDP/DVP schloss sich den Dankesworten seiner Vorredner an und führte weiter aus, in Bezug auf die Datenschutzaufsichtsbehörde interessiere er sich zum einen für die Stellensituation dort und zum anderen für den Umgang mit der Landesregierung. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit habe angekündigt, auch gegenüber der Landesregierung beratend tätig sein zu wollen. In diesem Zusammenhang interessiere ihn, inwieweit der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in die Erarbeitung des vom Minister für Inneres, Digitalisierung und Migration angekündigten Sicherheitspakets beispielsweise auch in Bezug auf Quellen-TKÜ, Kennzeichenlesesysteme usw. involviert sei und inwieweit er in die Erarbeitung der wohl bereits kursierenden Gesetzentwürfe eingebunden sei oder ob der Landesbeauftragte für den Datenschutz abwarten müsse, bis ein Gesetzentwurf vorgelegt werde.

Abg. Thomas Hentschel GRÜNE äußerte, auch er bedanke sich für den schriftlichen Tätigkeitsbericht und den mündlichen Bericht. Angesichts dessen, dass das Projekt E-Justice im Kommen sei und die elektronische Akte sicherlich auch im Verwaltungsbereich eine immer größere Rolle spielen werde, interessiere ihn, welche „Baustellen“ der Landesbeauftragte für den Datenschutz und die Informationsfreiheit insbesondere aufseiten der Gerichte und der Grundbuchämter sehe.

Der geänderte § 81 e der Strafprozessordnung werde es ermöglichen, DNA-Proben auch in Bezug auf Alter und Geschlecht der betroffenen Person zu analysieren. Weiterführend könnte auch eine Aussage zur Herkunft gemacht werden. Ihn interessiere, wie der Landesbeauftragte für den Datenschutz und die Informationsfreiheit dies aus datenschutzrechtlicher Sicht bewerte.

Abg. Wilhelm Halder GRÜNE bedankte sich ebenfalls für die Berichte und führte weiter aus, ihn hätten bereits Anfragen von Personen erreicht, die sich Sorgen machten, dass die Informationsfreiheit den Opferschutz einschränken könnte. Denn vor einer Einsichtgewährung oder Herausgabe würden zwar Namen in Unterlagen geschwärzt, doch wer den betreffenden Vorgang kenne, könne Rückschlüsse auf die Identität der betreffenden Person ziehen. Ihn interessiere, ob es möglich sei, Personen oder Gruppen, die vom Verfassungsschutz beobachtet würden, in ihrer Informationsfreiheit einzuschränken.

Abg. Emil Sänze AfD erklärte, auch er bedanke sich für die Berichte. Ab 2018 werde das Notrufsystem eCall in allen Neufahrzeugen Pflicht. Dies erfordere eine bidirektionale Schnittstelle für den Datentransfer, über die auch Bewegungsdaten übertragen würden. Ein solches System könne nicht nur von der Versicherungswirtschaft genutzt werden, sondern unter Umständen auch eine Überwachung des Fahrzeugführers ermöglichen. Ihn interessiere, ob dies in den einschlägigen Verordnungen bereits berücksichtigt sei.

LfDI Dr. Brink legte dar, er freue sich, dass so zahlreiche unterschiedliche und auch spannende Aspekte angesprochen worden seien. Aus Zeitgründen müsse er sich bei der Beantwortung der gestellten Fragen kurz fassen, biete jedoch an, bei entsprechendem Interesse entweder im Ausschuss oder an anderer Stelle vertieft auf einzelne Themen einzugehen.

Zu der Frage, wie die Arbeit des Landtags durch die europäische Gesetzgebung beeinflusst werde und was zu tun sei, könne bezogen auf das Land Baden-Württemberg festgestellt werden, dass es sich um einen Kraftakt handle, der gefordert werde. Denn im Zuge der Anpassung des Landesrechts an die Datenschutz-Grundverordnung müsse natürlich nicht nur das Landesdatenschutzgesetz geändert werden. Es müsse vielmehr eine dreistellige Zahl von Landesgesetzen, die datenschutzrechtliche Vorschriften enthielten, geändert werden. In jedem Einzelfall müsse geprüft werden, ob die Vorschriften weiter Bestand haben könnten oder geändert oder gestrichen werden müssten. Hierzu sei anzumerken, dass, wenn es zu einer Überlagerung von nationalem Recht mit der Datenschutz-Grundverordnung komme, die entsprechende Bestimmung im nationalen Recht gestrichen werden müsse, weil gleichlautendes oder gleichlaufendes nationales Recht nicht fortgeführt werden dürfe.

Dabei handle es sich um einen außerordentlich schwierigen Prozess, und zwar auch deshalb, weil gerade die öffentlichen Stellen auch in Baden-Württemberg gewohnt seien, mit dem bisherigen Normenbestand zu arbeiten und die Affinität zu bekannten Gesetzen mit Sicherheit höher als die zu neuen Regeln wie beispielsweise der Datenschutz-Grundverordnung sei, die denjenigen, die sie zu beachten hätten, in vielfacher Hinsicht, beispielsweise in Bezug auf die Systematik oder die Gesetzessprache, nicht so vertraut sei. Deswegen gebe es eine gewisse Tendenz dazu, eher zu versuchen, am nationalen Normenbestand soweit wie möglich festzuhalten. Das führe jedoch zu enormen Problemen. Ab Mai 2018 würde dies dazu führen, das sich vorgelagert vor den eigentlichen datenschutzrechtlichen Fragestellungen ein Streit darüber entwickle, was die anwendbare Gesetzesgrundlage sei. Dieses Problem betreffe im Übrigen nicht nur den öffentlichen Bereich, sondern auch den privaten Bereich, beispielsweise Auskunfteien. Denn diesen sei der Bundesgesetzgeber insofern entgegengekommen, als es im neuen BDSG nunmehr eine Vorschrift zu Auskunfteien und Scoring gebe, auf deren Grundlage die bisherige Datenverarbeitung aufrechterhalten bleiben könne. Es sei jedoch völlig ungeklärt, ob der Gesetzgeber solche „Geschenke“ machen dürfte. Diese Fragen müssten in den nächsten Jahren geklärt werden.

Bis dahin bleibe eine Unsicherheit bestehen, doch an Unsicherheit seien die betroffenen Unternehmen am allerwenigsten interessiert. Er gehe nicht davon aus, dass sich die große Aufgabe der Umstellung des nationalen Rechts bis Mai 2018 abschließen lassen werde. Denn dafür seien die Herausforderungen zu groß. Auf Bundesebene wirke sich erschwerend aus, dass im Zeitraum bis Mai 2018 auch noch eine Bundestagswahl stattfinde, was die Gesetzgebungsverfahren deutlich verzögere.

Die Datenschutz-Grundverordnung führe zu grundlegenden Veränderungen, die auch seine Behörde beträfen. Beispielsweise werde es in Zukunft unumgänglich sein, verstärkt auf europäischer Ebene zu kommunizieren, und das geschehe selbstverständlich auf Englisch. Wer sich darauf berufe, dass im Landesverwaltungsverfahrensgesetz Baden-Württemberg stehe, die Amtssprache sei Deutsch, werde sich somit nicht mehr aktiv und zeitnah an den europäischen Diskussionen beteiligen können. Somit werde es erforderlich sein, zu schulen und gewisse Hemmungen abzubauen. Dies betreffe zahlreiche Behörden.

Die Vorratsdatenspeicherung sei gerade für Datenschützer eine schwerwiegende Problematik. Das Problem bei der Vorratsdatenspeicherung bestehe immer darin, dass es sich um ein Instrument handle, das im Ergebnis nicht mehr regulierbar und nicht mehr kontrollierbar sei. Denn es finde eine Entkopplung des Erhebungs- und Verarbeitungszwecks auf der einen Seite und der Nutzung von Daten auf der anderen Seite statt. Zum Zeitpunkt der Erhebung von Daten, beispielsweise von Telekommunikationsdaten, wüssten die Behörden noch nicht genau, in welchem Kontext sie diese Daten später nutzen wollten. Das werde auch in dem Begriff „Vorratsdatenspeicherung“ deutlich. Es sei unstreitig, dass dieses Mittel im Bereich der Kriminalitätsbekämpfung effektiv sein könne. Dies setze jedoch voraus, dass die Sicherheitsbehörden gelernt hätten, mit so großen Datenmengen überhaupt sinnvoll umzugehen.

In diesem Zusammenhang sei anzumerken, dass es bisher kaum einen terroristischen Anschlag gegeben habe, bei dem bei Sicherheitsbehörden nicht schon im Vorfeld Informationen über den Täter bzw. das Umfeld vorhanden gewesen seien, dass die Sicherheitsbehörden jedoch aufgrund der Menge der Daten oder aufgrund der Schwierigkeit, sie richtig zu bewerten, nicht in der Lage gewesen seien, daraus die richtigen Schlüsse zu ziehen. Insofern sei Vorratsdatenspeicherung nicht nur rechtlich problematisch, sondern auch tatsächlich problematisch. Er wolle jedoch nicht ausschließen, dass sich in Zukunft auch durch den Einsatz von Software Konstellationen ergäben, die dazu führten, dass über diese Probleme möglicherweise auch anders gesprochen werden müsse.

Zu der erwähnten Rechtsprechung von EuGH und Bundesverfassungsgericht sei eine interessante Entwicklung zu konstatieren. Lange Zeit sei es so gewesen, dass das Bundesverfassungsgericht die Instanz gewesen sei, die den Datenschutz in Deutschland beginnend mit der Volkszählungsentscheidung im Jahr 1983 massiv gefördert habe. Zu erwähnen sei in diesem Zusammenhang, dass zahlreiche Sicherheitsgesetze vom Bundesverfassungsgericht kassiert oder zumindest eingeschränkt worden seien. Inzwischen sei es so, dass der EuGH jedenfalls im Bereich Datenschutz insgesamt und dabei auch im Bereich Vorratsdatenspeicherung das Bundesverfassungsgericht in seiner Bürgerrechtsfreundlichkeit noch übertreffe. Dies nähmen die Datenschützer natürlich sehr gern zur Kenntnis; sie sehen jedoch auf der anderen Seite auch, dass dadurch nationale Regelungsspielräume verloren gingen. Aus deutscher Sicht sei es besser, vom Bundesverfassungsgericht Vorgaben zu erhalten als von einer europäischen Institution.

In Bezug auf die Informationsfreiheit sehe er es als Aufgabe seiner Behörde an, das Gesetz, das vom Landtag verabschiedet worden sei, zu promoten und dafür zu sorgen, dass verstärkt von den entsprechenden Rechten Gebrauch gemacht werde. Im kommunalen Bereich sei die Informationsfreiheit bereits vor dem Inkrafttreten dieses Gesetzes gelebt worden; denn es sei Informationsfreiheit, wenn ein Bürger, der in einer Behörde anrufe, auch die gewünschte Information erhalte, und dies sei im Sinne von Bürgerfreundlichkeit schon viel früher praktiziert worden. Gleichwohl gebe es in diesem Bereich noch erheblichen Aufklärungsbedarf, und zwar auf allen Ebenen. Deswegen würden Fortbildungsveranstaltungen angeboten und werde mit den Kommunen kooperiert; auch bei den kommunalen Landesverbänden gebe es eine sehr große Offenheit gegenüber diesem Thema.

Auch mit der Staatsrätin für Zivilgesellschaft und Bürgerbeteiligung habe es bereits einen guten Austausch gegeben; dabei seien auch Schnittmengen für gemeinsame Aktivitäten ausgelotet worden. Nichtsdestotrotz bleibe die Informationsfreiheit für die Verwaltung ein schwieriges Thema und auch ein Thema, bei dem Geduld erforderlich sei. Es sei nicht so, dass die öffentliche Verwaltung nicht bereit wäre, Gesetze umzusetzen; allerdings gebe es durchaus Ängste, beispielsweise insofern, als einzelne Beamte befürchteten, stärker als bisher kontrolliert zu werden, weil nicht nur die Akten transparent würden, sondern beispielsweise auch die für deren Bearbeitung aufgewandte Zeit. Dafür müsse aus seiner Sicht Verständnis aufgebracht werden.

Ferner sei zu konstatieren, dass in bestimmten Bereichen der Verwaltung dort Beschäftigte viel stärker sichtbar würden, als sie es bisher gewesen seien. Ein Mitarbeiter einer Ausländerbehörde, der eine Ausweisungsverfügung unterschreibe, diesen Bescheid nach außen gebe und ihn später im Internet wiederfinde, werde in ganz anderer Weise als bisher mit dieser behördlichen Entscheidung identifiziert. Es bedürfe einer Auseinandersetzung darüber, ob die derzeitige Regelung im Informationsfreiheitsgesetz, nach der personenbezogene Daten von Beschäftigten im öffentlichen Dienst wie deren Namen nicht geschwärzt würden, in dieser Pauschalität noch sinnvoll sei. Darüber müsse nachgedacht werden. Er stelle jedenfalls fest, dass es vonseiten der öffentlich Bediensteten erhebliche Ängste gebe, dass sie auch persönlich für Entscheidungen verantwortlich gemacht würden, an denen sie zwar beteiligt gewesen seien, diese jedoch möglicherweise in dieser Ausprägung bislang nicht hätten öffentlich vertreten müssen.

Zur Frage, welche personellen Konsequenzen die Datenschutz-Grundverordnung habe, sei festzustellen, er habe in der laufenden Woche in der Tat die Fraktionsvorsitzenden angeschrieben. Seitdem seien ihm keine weiteren notwendigen Bedarfe als darin festgehalten aufgefallen. Mit diesem Schreiben habe er im Blick auf die Aufstellung des nächsten Haushalts frühzeitig signalisieren wollen, welche Situation in seiner Behörde herrsche, und einen Entscheidungsprozess anstoßen wollen, für den er auch weiterhin sehr gern zur Verfügung stehe.

Die zukünftige Kontrollberechtigung der Aufsichtsbehörden bei Rechtsanwälten und Ärzten sei in der Tat ein Riesenproblem. Er habe Verständnis für die Grundthematik, dass Ärzte und Rechtsanwälte in Bezug auf Patienten und Mandanten eine traditionell berufsständisch entwickelte Schweigeverpflichtung, der sie natürlich nachkommen müssten, hätten und deshalb grundsätzliche Bedenken hätten, wenn sich eine öffentliche Stelle, zu denen auch Datenschutzaufsichtsbehörden gehörten, in das sehr enge persönliche Verhältnis einmische. Über diese Thematik werde mit Vertretern der Anwälte bereits seit Jahrzehnten diskutiert, und im Ergebnis hätten die Anwälte im Wesentlichen erkannt, was die Rolle seiner Behörde sei und wo sie auch beratend tätig sein könne, was durchaus hilfreich sei.

Das Ziel, Verständnis in Bezug auf die Aufgabenabgrenzung zu finden, sei fast erreicht worden. Nunmehr sei es den genannten Berufsgruppen durch geschickte Arbeit jedoch leider gelungen, im Datenschutz-Anpassungs- und -Umsetzungsgesetz EU diese Norm zu etablieren, die den Datenschutzaufsichtsbehörden künftig den Zugang zu den Kanzleien mehr oder weniger verwehre.

Dies werde an der Kontrollpraxis seiner Behörde jedoch nur wenig ändern, denn die Fälle, die in diesem Bereich an sie herangetragen würden, seien gerade die Fälle, in denen derjenige, zu dessen Gunsten die Schweigepflicht bestehe, nämlich der Patient oder der Mandant, das Gespräch mit der Aufsichtsbehörde suche, sodass die Schweigepflicht dann keine Rolle mehr spiele. Denn in diesem Fall handle die Aufsichtsbehörde im Interesse des Schweigebegünstigten. Im Übrigen habe sich der Kontrolldruck, den seine Behörde auf Anwaltskanzleien und Arztpraxen ausgeübt habe, in der Vergangenheit sehr in Grenzen gehalten, was auch daran liege, dass eine Aufsichtsbehörde angesichts der Vielzahl der Kontrollmöglichkeiten danach schaue, wo eine Kontrolle zum größten Nutzen führe, und Anwälte, Ärzte und Steuerberater in Prinzip sehr gut wüssten, wie sie mit den Daten ihrer Mandanten, ihrer Patienten oder ihrer Kunden umgingen, sodass bis auf die Ausreißer, die im Beschwerdeweg von der Aufsichtsbehörde bearbeitet würden, kein grundsätzlicher Anlass vorhanden sei, zu glauben, das in Arztpraxen oder Anwaltskanzleien in irgendeiner Form „Schindluder“ getrieben würde.

Bei dem von Abg. von Eyb angesprochenen Phänomen handle es sich um das sogenannte Datenschutzparadoxon, welches beschreibe, dass Menschen einerseits mit ihren Daten sehr freigiebig seien, andererseits jedoch von sehr vielen Ängsten geplagt seien. Dabei handle es sich um eine Standardproblematik des Datenschutzes. Er erinnere in diesem Zusammenhang daran, dass mit der Begründung, in Zeiten von Facebook, Google & Co. hätte sich der Datenschutz überholt, immer wieder einmal der Abgesang auf den Datenschutz angestimmt werde.

Die Debatte müsse jedoch differenzierter geführt werden. Es sei nicht so, dass alle Menschen alles vom Frühstück bis zur Abendbeschäftigung auf Facebook posten würden. Tatsächlich gingen nur einige wenige so vor. Die meisten verhielten sich jedoch anders, weil sie entweder gelernt hätten oder von vornherein eine andere Einstellung zum Umgang mit ihren persönlichen Daten gehabt hätten.

Hierzu sei festzuhalten, die informationelle Selbstbestimmung sei sehr umfassend und beinhalte natürlich auch die Befugnis des Einzelnen, seinen gesamten persönlichen privaten Lebensbereich öffentlich darzustellen. Wer dies wolle, habe das grundrechtlich verbriefte Recht, das zu tun. Die Frage sei, ob dies sinnvoll sei. Seine Behörde als Aufsichtsbehörde habe in diesem Zusammenhang die Aufgabe, zu beraten, aufzuklären und darauf hinzuweisen, wo die Probleme lägen, wann Rechte Dritte berücksichtigt werden müssten und welche negativen Konsequenzen es haben könne, wenn sich jemand in einer bestimmten Art und Weise im sozialen Netz bewege. Die Entscheidung, wie sich jemand letztlich dort bewege, müsse jeweils individuell getroffen werden. Dieses Recht hätten mündige Bürger, und er habe großes Verständnis dafür, dass der eine oder andere sich verbitte, bevormundet zu werden. Dies sei auch nicht sein Verständnis.

Die Aufklärung und Beratung ziele in erster Linie auf Minderjährige und Jugendliche, die in vielen Bereichen bei dem, was an moderner Technik angeboten werden, „Versuchskaninchen“ seien und auch negative Erfahrungen machten und in der Folge allmählich lernten, wie mit personenbezogenen Daten umgegangen werden sollte.

Es spreche nichts dagegen, moderne Techniken zu nutzen, doch müsse dies aufgeklärt und mündig getan werden. In diesem Zusammenhang müsse dafür gesorgt werden, dass die Nutzungsbedingungen so ausgestaltet seien, dass eine Identifikation mit den Ergebnissen erfolgen könne.

Als Informationsfreiheitsbeauftragter müsse selbstverständlich auch er transparent sein. Deshalb stehe seine Behörde, wie es auch bei seinem Vorgänger der Fall gewesen sei, in einem sehr guten und vertrauensvollen Kontakt mit dem Ministerium für Inneres, Digitalisierung und Migration. Vorab und informell gebe es einen intensiven Austausch zu sehr vielen Fragestellungen. Diese gute Beziehung führe dazu, dass viele Fragestellungen bereits im Vorfeld in guter Art und Weise gelöst werden könnten. Dies sei bei den angesprochenen Gesetzesvorhaben nicht anders. Letztlich werde er, sobald die Landesregierung ihre Entscheidung gerade zu dem angesprochenen Sicherheitspaket getroffen habe, gegenüber dem Parlament seine Stellungnahme abgeben.

In bestimmten Bereichen seien mit dem Ministerium für Inneres, Digitalisierung und Migration über diese traditionellen Kontakte hinaus auch schon einzelne Kooperationspläne entwickelt worden. Ein Beispiel sei die sogenannte intelligente Videoüberwachung. Er habe davon abgesehen, von vornherein kundzutun, dies werde vonseiten der Datenschützer grundsätzlich abgelehnt, sondern zum Ausdruck gebracht, versuchen zu wollen, dieses Thema soweit wie möglich gemeinsam zu entwickeln und gemeinsam auszutesten. Dies geschehe derzeit. Dies ändere nichts an der Bereitschaft seiner Behörde, bestimmte Datenerhebungen und Datenverwendungen auch zu kritisieren und dies auch in grundsätzlicher Weise zu tun. Doch auf der anderen Seite wolle seine Behörde, wo immer es ihr möglich erscheine, derartige moderne Formen der Datenverarbeitung, in denen immer ein großes Potenzial stecke, begleiten und sei in diesem Zusammenhang auch für die Zusammenarbeit dankbar.

Beim Thema E-Justice gehe es in erster Linie um die technische Ausstattung. In Rheinland-Pfalz sei die Justiz Vorreiter in Bezug auf die elektronische Datenverarbeitung gewesen. Zunächst seien neue Möglichkeiten im Bereich der Justiz erprobt worden; erst dann habe der Rest der Landesverwaltung nachgezogen. Es wäre auch aus Gründen der Bürgerfreundlichkeit absolut zu begrüßen, wenn weitere Schritte folgen würden. Der Schulungsbedarf auch im Justizbereich und auch der Aufwand, der dazu betrieben werden müsse, dürften jedoch nicht unterschätzt werden. Er sei gespannt, wie die Resonanz in diesem Bereich aussehe.

Auch die DNA-Analyse sei ein wichtiges Thema. Insbesondere aus polizeilicher Sicht enthielten DNA-Proben unerschlossene Erkenntnisse, die eingesammelt werden könnten. Die Frage sei, zu welchem Preis dies erfolge und welche Folgen dies im Übrigen habe. Im Moment beschränke sich die Debatte darauf, bei der DNA-Analyse solche Merkmale in den Fokus zu nehmen, die ohnehin äußerlich erkennbar seien und beispielsweise auch bei einer polizeilichen Beobachtung ins Auge fielen. Dies sei jedoch nicht das Ende der Fahnenstange; denn die Aussagekraft von menschlichem Erbgut gehe weit darüber hinaus und sei nach seinem Eindruck von der medizinisch-technischen Entwicklung und Forschung her bei Weitem noch nicht ausgeschöpft. Hierzu müssten eine gesellschaftliche und eine parlamentarische Debatte geführt werden; denn es gehe um eine Technik, die alle unmittelbar betreffe, weil jeder Mensch notwendigerweise, ohne es beeinflussen zu können, überall DNA-Spuren hinterlasse, und wenn die Analysemöglichkeiten ausgeweitet würden – nicht nur im öffentlichen Bereich, sondern auch im privaten Bereich –, würde das die gesellschaftlichen Verhältnisse massiv verändern. Darüber müsse ein gesellschaftlicher Diskurs geführt werden, und dazu müssten eindeutige parlamentarische Vorgaben gemacht werden. Deshalb sei er dankbar dafür, dass sich die Debatte bislang auf die Erschließung äußerlich sichtbarer Merkmale beschränkt habe.

In diesem Zusammenhang sei anzumerken, dass das, was er in der laufenden Sitzung darlege, weder erschöpfend noch abschließend sein könne. Vielmehr bringe er in knapper Form nur einige Aspekte ein.

Zu der Frage nach dem Verhältnis zwischen Informationsfreiheit und Opferschutz sei festzuhalten, dass die Informationsfreiheit keineswegs unbegrenzt sei. Es handle sich nicht um einen Schlüssel für einen Zugang zu den gesamten Aktenbeständen öffentlicher Stellen. Für die Informationsfreiheit gebe es vielmehr auch Grenzen. Gerade als Datenschutzbeauftragter weise er darauf hin, dass das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger durch die Informationsfreiheit nicht übergangen werden dürfe. Selbstverständlich könne jeder auf der Grundlage des Informationsfreiheitsgesetzes beispielsweise das Sozialamt aufsuchen und nach der Sozialakte seines Nachbarn fragen; doch müsse das Sozialamt dann den Nachbarn fragen, ob er mit einer Informationsweitergabe einverstanden sei. Eine Informationsweitergabe sei nur auf freiwilliger Basis möglich; alles andere wäre mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar.

Mit dem Opferschutz sei ein großes Problem verbunden. Denn häufig reiche es nicht aus, Akten zu anonymisieren, indem Teile davon geschwärzt würden, weil in bestimmten Konstellationen derjenige, der Anträge nach dem IFG stelle, über Zusatzinformationen verfüge, die der Behörde gar nicht notwendigerweise vorliegen müssten, sodass eine reine Schwärzung dazu führen würde, dass derjenige, der mit diesem Vorwissen seine Anfrage stelle, die Anonymisierung unmittelbar wieder rückgängig machen könne. In öffentlichen Verwaltungen sei also ein umfassendes Verständnis von Anonymisierung erforderlich. Dies werde auch in Schulungen vermittelt. Anonymisierung bedeute nicht, Namen zu schwärzen. Anonymisierung bedeute vielmehr, sich zu fragen, ob die Informationen, die letztlich herausgegeben würden, unter Einbeziehung möglicher Vorkenntnisse oder anderer Informationen, die beispielsweise über Suchmaschinen gewonnen werden könnten, irgendeiner Person zugeordnet werden könnten, wodurch die erhaltenen Informationen wieder deanonymisiert werden könnten. Dies sei ein Problem, das in vielen Bereichen dazu führe, dass von bestimmten Aktenbeständen gar nichts mehr herausgegeben werden könne, weil die Behörde selbst durch größte Anstrengung und durch weitestgehende Schwärzung die Herstellung eines Personenbezugs nicht sicher ausschließen könne. In einem solchen Fall dürfe sie die Akten auch nicht herausgeben.

Opferschutz heiße in diesem Kontext, dass sich die Behörde ganz sicher sein müsse, dass sie keine Informationen herausgebe, die im Nachhinein wieder einer Person zugeordnet werden könnten.

Abg. Wilhelm Halder GRÜNE merkte an, ihm liege ein akuter Fall vor. Ihn interessiere, wo er intervenieren könne.

LfDI Dr. Brink teilte mit, damit könne er sich gern an seine Behörde wenden. Sie führe eine Klärung herbei, gehe auf die jeweiligen Behörden zu und informiere sie auch entsprechend. Dies gehöre zu den Aufgaben seiner Behörde.

Weiter äußerte er, das Notrufsystem eCall sei der Einstieg in das personalisierte Fahren und den Bereich Connected Car durch eine europarechtliche Vorgabe. Diese werde umgesetzt. In der Folge seien viele weitere Konzepte zur Nutzung von Fahrer- und Halterdaten aufgesetzt worden. Spannend sei beim Thema Connected Car, dass die Zahl derer, die sich für Daten interessierten, schlagartig unüberschaubar groß werde. An den Fahrerdaten seien nicht nur Hersteller und Werkstatt interessiert, sondern beispielsweise auch die Versicherungen, um das Fahrverhalten der Nutzer besser einschätzen zu können, um die Solidargemeinschaft von Kosten zu entlasten, die durch rücksichtsloses Verhalten einzelner Versicherter hervorgerufen würden. Es sei nicht beabsichtigt, diese Entwicklung mit den Mitteln des Datenschutzes aufzuhalten; selbst wenn es gewollt wäre, wäre dies auch nicht möglich.

Stellv. Vorsitzender Jürgen Filius bedankte sich für die Tätigkeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit sowie seine Ausführungen in der laufenden Sitzung.

Anschließend verlas er einen Vorschlag für eine Beschlussempfehlung an das Plenum (*Anlage 2*).

Der Ausschuss stimmte dieser Beschlussempfehlung ohne förmliche Abstimmung zu.

19. 06. 2017

Hans-Ulrich Sckerl

Anlage 1

Baden-Württemberg
INNENMINISTERIUM
DER MINISTER

LANDTAG
von Baden-Württemberg
Eing. 28. April 2016

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

Datum 27.04.2016
Durchwahl 0711 231-3254
Aktenzeichen 2-0557-6/9
(Bitte bei Antwort angeben)

Präsidenten des Landtages
von Baden-Württemberg
Herrn Wilfried Klenk MdL
Haus des Landtags
Konrad-Adenauer-Str. 3
70173 Stuttgart

Stellungnahme der Landesregierung zum 32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (LT-Drs. 15/7990)

Anlagen
Stellungnahme der Landesregierung
Synopse

Sehr geehrter Herr Landtagspräsident,

die Landesregierung hat in der Kabinettssitzung vom 26. April 2016 die Stellungnahme zum 32. 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

Reinhold Gall MdL

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

Willy-Brandt-Str. 41 • 70173 Stuttgart • Telefon 0711 231-4 • Telefax 0711 231-3019

Baden-Württemberg
INNENMINISTERIUM

Stellungnahme der Landesregierung

zum

32. Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz
in Baden-Württemberg (LT-Drs. 15/7990)

Dienstgebäude Willy-Brandt-Str. 41 • 70173 Stuttgart • Telefon 0711 231-4 • Telefax 0711 231-5000
E-Mail: poststelle@im.bwl.de • Internet: www.im.baden-wuerttemberg.de • www.service-bw.de

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

Da die Landesregierung keine Möglichkeit hat, auf die Einhaltung datenschutzrechtlicher Vorschriften durch nicht-öffentliche Stellen hinzuwirken, äußert sie sich zu den Ausführungen des Landesbeauftragten für den Datenschutz in diesem Bereich nur, soweit es um Fragen der Gesetzgebung oder das Verhalten der Landesregierung geht und eine Erwiderung erforderlich ist. Dasselbe gilt für sonstige Bereiche des Datenschutzes, soweit das Land Baden-Württemberg nicht zuständig ist.

1. Zur Situation

1.2 Die Europäische Datenschutzreform – zum Stand der Datenschutz-Grundverordnung

Das **Innenministerium** begrüßt die europäische Datenschutzreform, die ein einheitliches Datenschutzrecht in Europa einführen und damit insbesondere die Rechte der Bürgerinnen und Bürger stärken wird. Nach der im Sommer 2016 zu erwartenden Veröffentlichung der Datenschutz-Grundverordnung im europäischen Amtsblatt bleiben dem Land zwei Jahre Zeit, die Datenschutzregelungen in allen Landesgesetzen auf ihre Vereinbarkeit mit dieser zu prüfen und gegebenenfalls gesetzgeberisch anzupassen. Die vorbereitenden Arbeiten hierzu wurden im Innenministerium begonnen. Das Landesdatenschutzgesetz wird voraussichtlich in seiner jetzigen Form bis auf wenige Ausnahmen obsolet und durch die unmittelbar geltende EU-Datenschutz-Grundverordnung ersetzt werden. Auf den Landesbeauftragten für den Datenschutz kommen in diesem Zusammenhang ebenfalls neue Aufgaben zu, die einer Neuregelung bedürfen.

1.3 Die EU-Datenschutzrichtlinie für Polizei und Justiz – Flickenteppich statt Regenschirm?

Die Kritik des Landesbeauftragten für den Datenschutz an der EU-Datenschutz-Richtlinie für Polizei und Justiz (JI-Richtlinie), dass sich diese an vielen Stellen in allgemeinen Ausführungen erschöpfe und wesentliche Entscheidungen den nationalen Gesetzgebern und deren innerstaatlichem Recht überlasse, wird vom **Innenministerium** in dieser Form nicht geteilt. Aus Sicht des Innenministeriums ist die JI-Richtlinie als Teil der EU-Datenschutzreform grundsätzlich positiv zu bewerten, da damit ein Rahmen vorgegeben wird, wie und wann Behörden, Gerichte und andere Organisationen personenbezogene Daten zur Strafverfolgung erheben und nutzen können, den Mitgliedstaaten aber dennoch einen gewissen Freiraum bei der nationalen Umsetzung belässt. Das Innenministerium bedauert es jedoch, dass die Forderung eines erweiterten Anwendungsbereiches der JI-Richtlinie, der auch den Bereich der nicht auf Straftaten bezogenen polizeilichen Gefahrenabwehr erfasst, im Rahmen der Trilog-Verhandlungen nicht durchsetzbar war. Die nicht straftatenbezogene Gefahrenabwehr der Polizei wird daher künftig dem Anwendungsbereich der EU-Datenschutz-Grundverordnung unterfallen. Durch die Geltung beider Rechtsakte wird sich sowohl die Umsetzung in nationales Recht als auch die spätere praktische Anwendung schwierig gestalten.

1.6 Aus der Dienststelle

Das **Innenministerium** vertritt die Auffassung, dass die Übertragung der Zuständigkeit für die Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten auf den Landesbeauftragten für den Datenschutz dann erfolgen soll, wenn die EU-Datenschutz-Grundverordnung dies verbindlich vorgibt und hierfür eine sichere Rechtsgrundlage schafft.

2. Innere Sicherheit

2.1.2 Automatische Kennzeichenlesesysteme der Polizei

Das **Innenministerium** weist darauf hin, dass von der im Jahr 2008 eingeführten Regelung des § 22a PolG, der den Einsatz automatischer Kennzeichenlesesysteme erlaubt, aufgrund der dagegen eingelegten Verfassungsbeschwerde bislang kein Gebrauch gemacht wurde. Der Landesbeauftragte für den Datenschutz führt zutreffend aus, dass das Bundesverfassungsgericht noch keinen Termin zur mündlichen Verhandlung der Beschwerde bestimmt hat. Es ist derzeit auch offen, ob durch Urteil oder – ohne mündliche Verhandlung – durch Beschluss entschieden wird. Die Entscheidung des Bundesverfassungsgerichts bleibt abzuwarten.

2.1.4 Quod non legitur, non creditur

Wird im Rahmen von Auskunftsbegehren festgestellt, dass für bestimmte Daten die Voraussetzungen für eine Speicherung nicht mehr gegeben sind, wird künftig laut **Innenministerium** in Abstimmung mit dem Landesbeauftragten für den Datenschutz wie folgt verfahren: Die entsprechenden Daten werden zwar nach wie vor in den polizeilichen Dateien gelöscht. Durch einen vollständigen Dateiausdruck wird jedoch für einen begrenzten Zeitraum ein Aktenrückhalt erstellt, so dass die endgültige Löschung gemäß § 46 Abs. 1 Satz 2 PolG i.V.m. § 23 Abs. 4 Nr. 1 LDSG zunächst unterbleibt. Die betreffenden Daten werden gemäß § 24 Abs. 1 Nr. 2 LDSG gesperrt, gemäß § 24 Abs. 3 LDSG gesondert aufbewahrt und mit – soweit wie organisatorisch möglich – beschränkten Zugriffsrechten versehen. Dem Betroffenen wird sodann umfassend Auskunft zu allen über ihn gespeicherten Daten erteilt. Gleichzeitig erfolgt der Hinweis, dass die unrechtmäßig gespeicherten Daten aus den elektronischen Dateien gelöscht wurden, jedoch gesperrt als Dateiausdruck für weitere drei Monate aufbewahrt werden. Die Mitteilung erfolgt schriftlich und wird dem Betroffenen gemäß den Vorschriften des Landesverwaltungszustellungsgesetzes förmlich zugestellt. Wird keine Überprüfung durch ein Gericht oder durch den Landesbeauftragten für den Datenschutz eingeleitet und wird ferner kein Einwand gegen die Löschung der betroffenen Daten vorgebracht, werden diese nach Ablauf der genannten Frist endgültig vernichtet. Auch darauf wird der Betroffene bereits im Rahmen der förmlich zuzustellenden Mitteilung ausdrücklich hingewiesen. Dadurch wird sowohl der Löschverpflichtung als auch dem möglichen Interesse des Betroffenen an einer nachträglichen Rechtsprüfung Rechnung getragen.

2.1.5 Wie man sich irren kann!

Der Landesbeauftragte für den Datenschutz beruft sich auf ein rechtskräftiges Urteil des Verwaltungsgerichts Karlsruhe über den Einsatz eines Verdeckten Ermittlers durch die ehemalige Polizeidirektion Heidelberg. Aus Sicht des Verwaltungsgerichts Karlsruhe waren die an die Anordnung des Einsatzes eines Verdeckten Ermittlers zu stellenden formellen Voraussetzungen nicht erfüllt und lagen auch die materiellen Voraussetzungen für den Einsatz eines Verdeckten Ermittlers gegen den Kläger nicht vor. Aus Sicht des **Innenministeriums** handelt es sich um einen Einzelfall. Entgegen der Auffassung des Verwaltungsgerichts besteht keine Notwendigkeit, in präventivpolizeiliche Einsatzanordnungen nach § 22 Abs. 6 PolG künftig einen ausdrücklichen Hinweis aufzunehmen, dass der eingesetzte Verdeckte Ermittler Polizeibeamter ist. Dieser Umstand ergibt sich bereits aus § 22 Abs. 1 Nr. 4 PolG. Einsatzanordnungen im Bereich des Staatsschutzes werden nach der Auslegung des Urteils des Verwaltungsgerichts Karlsruhe durch das Innenministerium jedoch künftig eine Höchstzahl möglicher eingesetzter Verdeckter Ermittler und den ihnen für den Einsatz zugewiesenen Tarnnamen enthalten. Das Innenministerium wird die Bewertung des Verwaltungsgerichts Karlsruhe bei künftigen Anordnungen bedenken.

2.2.2 Precogs oder Precobs – Die Zukunft der Verbrechensverhinderung?

Das Landeskriminalamt hat den Pilotbetrieb von precobs, der Prognosesoftware für den Bereich Wohnungseinbruchdiebstahl, von Beginn an eng mit dem Landesbeauftragten für den Datenschutz abgestimmt. Die Projektgruppe des Landeskriminalamts ist mit der konstruktiven Zusammenarbeit äußerst zufrieden. Die frühe Einbindung des Landesbeauftragten für den Datenschutz während der Projektvorbereitung wurde als zwingend erforderlich angesehen und hat sich bewährt. Durch den Verzicht auf personenbezogene Daten bei der Vorhersagesoftware precobs hat das Landeskriminalamt eine Vorreiterfunktion für die gesamte Bundesrepublik eingenommen. Die anonymisierten Tatorte schränken die Auswerter („Operatoren“) bei ihren qualitativen Analysen mittels precobs nicht ein. Sollte es zu einer Verstetigung des Einsatzes von Predictive Policing kommen, werden die aktuell berücksichtigten datenschutzrechtlichen Vorgaben weiterhin Anwendung finden. Zu Recht weist der Landesbeauftragte für den Datenschutz nach Auffassung des **Innenministeriums** daher darauf hin, dass precobs in der aktualisierten Version daher insgesamt gesehen datenschutzrechtlich unbedenklich erscheint.

2.2.3 Gut gemeint ist nicht immer gut

Vor dem Hintergrund des Urteils des Verwaltungsgerichtshofs Baden-Württemberg vom 15. Mai 2014 zum Begriff der vorbeugenden Bekämpfung von Straftaten in § 22 Abs. 2 und 3 PolG sowie eines zwischenzeitlich eingestellten Projekts des Landeskriminalamts hält der Landesbeauftragte für den Datenschutz eine Novellierung des Polizeigesetzes für erforderlich. Nach Auffassung des **Innenministeriums** kann die Entscheidung des Verwaltungsgerichtshofs, dass der Begriff der vorbeugenden Bekämpfung von Straftaten nur die Verhütung von Straftaten (Verhinderungsvorsorge), nicht aber die Strafverfolgungsvorsorge umfasst, nicht verallgemeinert werden und ist nicht zwingend auf andere Vorschriften des Polizeigesetzes zu übertragen. Bei der voraussichtlich in der nächsten Legislaturperiode zur Umsetzung der EU-Datenschutz-Grundverordnung und der EU-Datenschutz-Richtlinie für Polizei und Justiz notwendigen Änderung des Polizeigesetzes wird das Innenministerium diese Frage allerdings noch vertieft prüfen.

Die im Zusammenhang mit der Forderung nach Novellierung des Polizeigesetzes geäußerte Kritik, dass auch das Landesverfassungsschutzgesetz (LVSG) nicht den verfassungsrechtlichen Anforderungen entspricht, ist wiederholt vom Landesbeauftragten für den Datenschutz geltend gemacht worden. Dem Anliegen – Regelungen zum Kernbereich privater Lebensführung – soll in einer künftigen Novellierung entsprochen werden. Auch der Abschlussbericht des Untersuchungsausschusses NSU BW enthält entsprechende Empfehlungen und Prüfbitten.

2.2.4 Der Kriminalaktennachweis – Gehören Daten aus Ermittlungsverfahren wegen des Verdachts der exhibitionistischen Handlung in diese bundesweite Datei?

Den Handlungsbedarf, den der Landesbeauftragte für den Datenschutz bezüglich der Datenspeicherung von Ermittlungsverfahren wegen des Verdachts exhibitionistischer Handlungen gemäß § 183 StGB in der beim BKA geführten Verbunddatei „Kriminalaktennachweis (KAN)“ nennt, sieht das **Innenministerium** nicht in gleicher Weise.

Das Innenministerium teilt nicht die Auffassung des Landesbeauftragten für den Datenschutz, dass eine exhibitionistische Handlung nicht den Zugangskriterien gemäß den KAN-Rahmenrichtlinien entspricht und die KAN-Relevanz in diesen Fällen deshalb zu Unrecht bejaht wird. Aus Sicht des Innenministeriums kommt für die KAN-Speicherung neben dem ausführlich behandelten Punkt 4.2 der KAN-Richtlinien durchaus auch der Punkt 4.3 als Zugangskriterium für die Straftat in Betracht. Punkt 4.3 spricht im Bereich der Triebtäterschaft lediglich von der Stärke der Triebfähigkeit, unabhängig vom Delikt. Entgegen den Voraussetzungen der Nr. 4.2 und der möglicherweise im Einzelfall fragwürdigen DNA-Probenentnahme bzw. Musterspeicherung ist bei Punkt 4.3 gerade keine Steigerung zu einem schwereren Delikt gefordert. Die Stellung einer Wiederholungsprognose ist bei einem Exhibitionisten bezüglich weiterer Taten allein durch seine Triebhaftigkeit möglich, da eben keine Steigerung der Deliktsqualität Voraussetzung ist, sondern lediglich eine Tatwiederholung.

Fehl geht aus Sicht des Innenministeriums auch der generelle Vorwurf übermäßiger DNA-Probenentnahmen nach § 81g StPO aufgrund der „Balanced Scorecard“ (BSC) der Landespolizei. Es kann zwar nicht ausgeschlossen werden, dass in Einzelfällen unrechtmäßige DNA-Probenentnahmen erfolgt sind. Bei Exhibitionisten handelt es sich aus kriminologischer Sicht aber um triebhaft gesteuerte Täter mit besonderer sexueller Veranlagung. Die kriminalistische Erfahrung zeigt, dass bei diesen Tätern künftig durchaus auch mit der

Begehung schwerwiegender Sexual- oder Gewaltstraftaten gerechnet werden muss, die gegebenenfalls durch DNA-Material aufgeklärt werden können. Deshalb strebt die Polizei in geeigneten Einzelfällen eine Probenentnahme nach § 81g StPO an, die dann auch eine Speicherung der personenbezogenen Daten mit KAN-Relevanz rechtfertigt.

Insoweit der Landesbeauftragte für den Datenschutz ferner die Voreinstellung langer Standard-Speicherfristen bemängelt, ist zu bemerken, dass die Beibehaltung der Voreinstellung der Speicherdauer KAN-Sex für eine Einzelfallentscheidung nicht relevant ist. Das Ereignis, das die Voreinstellung der Speicherfrist definiert, ist nicht deliktsgebunden, sondern frei wählbar. Somit kann bereits hier als Einzelfallentscheidung von der KAN-Sex-Speicherung abgewichen werden. Innerhalb der KAN-Speicherung kann die vorgegebene Speicherfrist manuell verkürzt werden.

Wird die KAN-Relevanz ausgewählt, besteht bereits jetzt die vom Landesbeauftragten für den Datenschutz ferner geforderte Möglichkeit der Dokumentation der Gründe im System. Der Landesteil der KAN-Richtlinien wird dementsprechend angepasst. Grundsätzlich schreibt die Dienstanweisung POLAS die Dokumentation der zur Speicherung führenden Gründe vor, insbesondere bei Abweichungen nach oben in Fällen geringer Bedeutung gemäß § 5 Abs. 3 DVO PolG. Die Dokumentation ist derzeit revisionssicher nur im Papieraktenrückhalt möglich, auch im Falle der Speicherung der Begründung im System. Eine unzureichende Dokumentation der Entscheidungsgründe kann aber jeweils nur einzelfallbezogen betrachtet werden. Entsprechende Regelungen in der Dienstanweisung POLAS sind vorhanden und wurden auch geschult.

2.2.5 Steht der Datenschutz sich selbst im Wege?

Vorgänge werden im Vorgangsbearbeitungssystem ComVor gemäß den Vorgaben der Ziffer 12 der Dienstanweisung ComVor sowie der Ziffer 3.4 des Fachkonzepts Datenschutz für ComVor zum Zwecke der Dokumentation polizeilicher Aufgabenwahrnehmung mindestens zwölf Monate gespeichert und spätestens mit Erreichen der Verfolgungsverjährung automatisiert gelöscht. Daneben ist eine Funktion eingerichtet, um personenbezogene Daten in Vorgängen manuell zu löschen, wenn deren weitere Speicherung nach Ablauf der Mindestspeicherfrist, jedoch vor Erreichen der Verfolgungsverjährung, nicht mehr erforderlich ist. Das ist insbesondere dann der Fall, wenn von der zuständigen Verfolgungsbehörde eine Mitteilung über den Ausgang des Verfahrens eingeht.

Das **Innenministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz, dass dies auch in den Fällen gilt, in denen z.B. aufgrund des Steuergeheimnisses nicht mit einer Mitteilung über den Ausgang des Verfahrens zu rechnen ist. Die technische Umsetzung hierzu ist im Detail noch zu prüfen.

2.2.6 Ende gut, alles gut?

Das **Innenministerium** teilt grundsätzlich die Auffassung des Landesbeauftragten für den Datenschutz, dass die Einstellung eines Verfahrens durch die Staatsanwaltschaft nach § 170 Abs. 2 StPO die Polizei nicht generell von ihrer Verpflichtung zur eigenverantwortlichen Prüfung eines Resttatverdachts als Voraussetzung für die weitere Datenspeicherung entbindet. Allerdings sind nach Auffassung des Innenministeriums im Handbuch Elektronische Mitteilung über den Ausgang des Verfahrens des Landeskriminalamtes Baden-Württemberg die verschiedenen Gründe für eine Einstellung durch die Justiz und ihre Auswirkung auf das Vorliegen eines Tat- bzw. Restverdachts ausreichend differenziert.

In der Folge trifft der Vorwurf im vom Landesbeauftragten für den Datenschutz geschilderten konkreten Fall nach Auffassung des Innenministeriums nicht zu. Der Betroffene hatte sich mit Schreiben vom 4. November 2014 an das Polizeipräsidium Ulm gewandt und die Löschung seiner im polizeilichen Auskunftssystem POLAS Baden-Württemberg gespeicherten personenbezogenen Daten beantragt. Mit Verfügung des Polizeipräsidiums Ulm vom 19. November 2014 wurde dem Betroffenen mitgeteilt, dass seinem Antrag nicht entsprochen werden kann. Die Speicherung der personenbezogenen Daten wurde mit § 38 Abs. 2 PolG begründet. Der dafür erforderliche (Rest-)Tatverdacht wurde insbesondere aufgrund des Schreibens der Staatsanwaltschaft Ulm vom 31.Oktober 2014 angenommen, die das Ermittlungsverfahren gegen den Betroffenen mangels öffentlichen Interesses eingestellt und den Antragsteller auf den Privatklageweg verwiesen hatte. Gemäß Ziffer 3.1.2 des Handbuches Elektronische Mitteilung über den Ausgang des Verfahrens des Landeskriminalamtes Baden-Württemberg wird bei Einstellungen gemäß § 170 Abs. 2 der Strafprozessordnung für die Tatverdachtsprüfung nach den Gründen der Einstellung differenziert. So wird ein Tat- bzw. Restverdacht z. B. verneint, wenn das Verfahren eingestellt wurde, weil das angezeigte Verhalten keinen Straftatbestand erfüllt. Bei Einstellungen wegen Verneinung des öffentlichen Interesses und Verweisung auf den Privatklageweg gemäß §§ 374 ff. StPO wird der Tat- bzw. Restverdacht jedoch bejaht. Das Handbuch Elektronische Mitteilung über den Ausgang des Verfahrens des Landeskriminalamtes Baden-Württemberg ist mit der Dienstanweisung POLAS-BW, Anhang 3, inhaltsgleich. Im konkreten Fall wurde in die Prüfung des Resttatverdachts neben dem konkreten Einstellungsgrund nach Aktenlage noch die Aussage eines Zeugen einbezogen, der aussagte, die Straftat beobachtet zu haben. Nach Auffassung des Innenministeriums hat das Polizeipräsidium Ulm den Restverdacht damit entsprechend der datenschutzrechtlichen Verantwortung eingehend geprüft. Die erst später vom Betroffenen vorgelegten Zeugenaussagen lagen zu diesem Prüfungszeitpunkt noch nicht vor und konnten daher in die Bewertung auch noch nicht einbezogen werden. Denn erst mit Schreiben vom 21. Dezember 2014 wandte sich der Betroffene erneut an das Polizeipräsidium Ulm und legte drei ihn entlastende schriftliche Zeugenaussagen vor. Erst jetzt ergab sich ein deutlicher Widerspruch zwischen der Aussage des Zeugen und der Ermittlungsakten hinsichtlich des Tatverdachts. Aufgrund dieser Widersprüche der Zeugenaussagen und dem Grundsatz „in dubio pro reo“ folgend wurde daraufhin die Löschung der beim Polizeipräsidium Ulm gespeicherten personenbezogenen Daten des Betroffenen veranlasst.

2.2.7 Warum darf die Polizei die Daten von Fußballfans in verschiedenen Sportdateien speichern?

Zu Recht weist der Landesbeauftragte für den Datenschutz darauf hin, dass Daten von Personen, die im Zusammenhang mit Sportveranstaltungen strafrechtlich aufgefallen sind oder Teilnehmer an Ausschreitungen bzw. Störungen waren, in zwei Dateien gespeichert werden – in der Verbunddatei „Gewalttäter Sport“ (GEWA SPORT) und in der „Arbeitsdatei Szenekundige Beamte“ (SKB-Datenbank). Der Landesbeauftragte für den Datenschutz kritisiert, dass eine Löschung von Daten in der in Baden-Württemberg geführten SKB-Datenbank nicht zu einer Überprüfung der Speicherung der betroffenen Personen in der Datei GEWA SPORT führt.

Die beiden Datenbanken unterscheiden sich jedoch, worauf das **Innenministerium** hinweist, in wesentlichen Punkten. Die SKB-Datenbank hat eine präventivpolizeiliche Ausrichtung mit dem Schwerpunkt der Anreiseverhinderung von Fußballstörern (z. B. Verfügung von Aufenthaltsverboten bzw. Meldeauflagen). Dagegen entfaltet die Datei GEWA SPORT gewaltpräventive Wirkung, die der Polizei Anhaltspunkte und Erkenntnisse für Eingriffsmaßnahmen auf Reisewegen und am Spielort liefert (z. B. nach einer Personenkontrolle). Auch der zugriffsberechtigte Personenkreis und die festgesetzten Löschfristen unterscheiden sich wesentlich.

Der „Unterausschuss Führung, Einsatz und Kriminalitätsbekämpfung“ (UA FEK) hat eine Bund-Länder-Arbeitsgruppe (BLAG GEWA SPORT) mit dem Auftrag zur Überprüfung und Anpassung der Datei GEWA SPORT eingesetzt. In der BLAG wurde auch der vom Landesbeauftragten für den Datenschutz angesprochene Wechsel des Datenerfassungsprinzips (vom Tatortprinzip zum Vereinsortprinzip) diskutiert. Aus rechtlichen Gründen (Verantwortlichkeit der datenerhebenden Stelle) kann dieser Ansatz aber keine Berücksichtigung finden. Der favorisierte Lösungsansatz der BLAG ist ein polizeiübergreifender personenbezogener Informationsaustausch, der die datenerfassende Stelle vor einer Datenspeicherung zur Kontaktaufnahme mit der Fachdienststelle am Vereinsort (Vereinsdienststelle) verpflichtet. Die Vereinsdienststelle (verantwortlich für die Speicherungen in der SKB-Datenbank) erlangt somit von einem Eintrag in die Datei GEWA SPORT Kenntnis und kann dadurch der datenerfassenden Tatortdienststelle prognoseunterstützende Informationen übermitteln, um sie in die Lage zu versetzen, die Erforderlichkeit einer Speicherung jederzeit zu überprüfen.

Diese geplante Verfahrensweise könnte ein Lösungsvorschlag für die nachvollziehbare Kritik des Landesbeauftragten für den Datenschutz sein. Aufgrund der dennoch weiterhin unterschiedlichen Zielrichtungen und Rahmenbedingungen der beiden Datenbanken muss die Löschung eines Betroffenen in der einen Datei aber auch künftig nicht zwangsläufig Auswirkungen auf die Speicherung dieser Person in der anderen Datei haben.

2.2.8 Stadionverbote – Was passiert, wenn die Polizei sich geirrt hat?

Nach Bekanntwerden des vom Landesbeauftragten für den Datenschutz geschilderten Falles, bei dem ein Stadionverbot unrechtmäßigerweise bestehen blieb, weil verfahrensrelevante Daten des Betroffenen (Statuswechsel vom Beschuldigten zum Zeugen) durch die Polizei nicht zeitgerecht übermittelt bzw. berichtigt wurden, hat sich das **Innenministerium** eingehend mit dieser Problematik befasst. Die Kritik des Landesbeauftragten für den Datenschutz ist nachvollziehbar, ein Lösungsvorschlag wurde daher bereits erarbeitet. Ein neuer Passus in der „Führungs- und Einsatzanordnung Fußball Baden-Württemberg (FEA Fußball)“ greift den Statuswechsel der betroffenen Person auf und schreibt vor, dass eine solche Änderung dem Verband bzw. dem Verein zeitgerecht mitgeteilt werden muss. Zudem wurden die Polizeiführer bei Fußballspielen und die Szenekundigen Beamten hinsichtlich dieser Problematik sensibilisiert.

2.2.9 Das Nationale Waffenregister – Kontrollbesuche bei den Waffenbehörden

Bei den Verwaltungsverfahren in den vier kontrollierten Waffenbehörden wurden durch die Mitarbeiter des Landesbeauftragten für den Datenschutz keine Abweichungen von dem gesetzlich vorgegebenen Rahmen erkannt. Dieses Ergebnis ist nach Auffassung des **Innenministeriums** sehr erfreulich.

Die Empfehlungen des Landesbeauftragten für den Datenschutz, die lediglich kleinere Verbesserungsvorschläge bei technischen und organisatorischen Maßnahmen aufzeigen, wurden mit Schreiben vom 3. Februar 2016 allen Waffenbehörden zur Kenntnis gegeben. Gleichzeitig wurden die Waffenbehörden gebeten, die Empfehlungen des Landesbeauftragten für den Datenschutz umzusetzen.

Erste Rückmeldungen zeigen, dass die Waffenbehörden zwischenzeitlich teilweise bereits entsprechende Maßnahmen eingeleitet haben. Dabei werden auch Überlegungen angestellt, die allgemeinen Empfehlungen des Landesbeauftragten für den Datenschutz z.B. zum Umgang mit elektronischem Schriftgut nicht nur für den Bereich der Waffenbehörde umzusetzen, sondern auch für weitere ebenfalls betroffene Fachbereiche innerhalb der jeweiligen Behörde.

2.2.10 Glückssache!

Der Sachverhalt wird im Tätigkeitsbericht korrekt dargestellt.

Das **Innenministerium** hat gemeinsam mit dem für Spielhallen zuständigen Ministerium für Finanzen und Wirtschaft sowie der Staatlichen Toto Lotto GmbH (STLG) Gespräche mit dem Landesbeauftragten für den Datenschutz geführt, um eine sachgerechte Lösung für die bereits in OASIS eingepflegten Spielersperren aus dem Bereich der Spielhallen zu finden.

Dabei erfolgte eine Abschichtung entsprechend der von den Spielhallen verwandten Sperrantragsformulare und der Angaben, die von dem Betroffenen in diesen gemacht wurden. Bezüglich der über die Spielhallen an die STLG geleiteten Sperranträge wird geprüft, in welcher Weise dem Vorschlag des Landesbeauftragten für den Datenschutz entsprochen wird, alle Gesperrten in einem Schreiben darauf hinzuweisen, dass der laufende Spielersperrantrag gelöscht wird, wenn sie keinen erneuten Sperrantrag stellen. Bezüglich der Sperranträge, für die das Sperrantragsformular der STLG genutzt wurde, gibt es bislang noch keine abschließende Regelung.

In den Fällen, in denen der Antragsteller selbst angibt, spielsüchtig zu sein, könnte diese Angabe als ein Anhaltspunkt gewertet werden, der die Verhängung einer Fremdsperre gemäß § 8 Abs. 2 GlüStV rechtfertigt. In diesem Zusammenhang ist die Frage aufgeworfen worden, ob das von der STLG verwandte Sperrantragsformular den datenschutzrechtlichen Anforderungen entspricht. Aus Sicht des Innenministeriums ist dies der Fall. Sofern sich im Laufe der weiteren Prüfung und Abstimmung zwischen dem Landesbeauftragten für den Datenschutz und der STLG eine Lösung zur Gestaltung der Sperrantragsformulare abzeichnen wird, die den datenschutzrechtlichen Anforderungen an eine informierte Einwilligung in die Datenverarbeitung noch besser Rechnung trägt, soll diese umgesetzt werden.

2.3 Die Verfassungsschutzreform

Der Landesbeauftragte für den Datenschutz kritisiert das von der Bundesregierung eingebrachte „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“, das am 21. November 2015 in Kraft getreten ist, weil es seiner Auffassung nach wesentliche Forderungen des Datenschutzes unberücksichtigt lässt. Zusätzlich wird Kritik am Bundesgesetzgebungsverfahren (fehlende Berücksichtigung der Einwände im Anhörungsverfahren sowie Absehen vom Anrufen des Vermittlungsausschusses) geäußert.

Die inhaltliche Kritik betrifft u.a. das Nachrichtendienstliche Informationssystem (NADIS) der Verfassungsschutzbehörden. Hier sind vor allem die erweiterten Auswertungs- und Analysekompetenzen des Bundesamts für Verfassungsschutz sowie die neue Datenbankstruktur („vertiefte softwaregestützte Analyse unstrukturierter Daten“) zu nennen. NADIS musste, worauf das **Innenministerium** hinweist, angesichts der gestiegenen Herausforderungen an die Sicherheitsbehörden und die gewachsenen Informationsbedürfnisse der Verfassungsschutzbehörden untereinander angepasst werden. Die Neugestaltung trägt dem Umstand Rechnung, dass zur umfassenden Erfüllung der gegenseitigen Unterrichtungspflichten der Verfassungsschutzämter ein reines Aktenhinweissystem künftig nicht mehr ausreicht, sondern hierzu in verstärktem Maße auch gemeinsame Text-, Bild- und multimediale Informationen erforderlich sind. Nur so lassen sich die Verflechtungen zwischen den unterschiedlichen Beobachtungsobjekten des Verfassungsschutzes erkennen.

Die zeitnahe Verfügbarkeit von Erkenntnissen dient der Verbesserung der Zusammenarbeit im Verfassungsschutzverbund. Der Gesetzgebungsbedarf ist nicht zuletzt durch die Beschlüsse der Innenministerkonferenz und die Empfehlungen der Bund-Länder-Kommission Rechtsterrorismus sowie des NSU-Untersuchungsausschusses des Deutschen Bundestags hinreichend aufgezeigt worden. Dabei hatte der Gesetzgeber die datenschutzrechtlichen Belange im Blick, was sich u.a. aus der Beschränkung des Kreises der Abfrageberechtigten in § 6 Absatz 2 Satz 7 und 8 BVerfSchG ableiten lässt.

3. Justiz

3.3 Öffentlichkeitsfahndung in sozialen Netzwerken

In der Anlage B „Richtlinien über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren“ zu den „Richtlinien für das Straf- und Bußgeldverfahren (RiStBV)“, die in Baden-Württemberg als gemeinsame Verwaltungsvorschrift von Justiz- und Innenministerium vom 8. April 2005 umgesetzt ist, ist derzeit vorgesehen, dass Öffentlichkeitsfahndungen der Strafverfolgungsbehörden im Internet grundsätzlich nicht unter Einschaltung privater Internetanbieter erfolgen sollen.

Um in geeigneten Fällen auch Fahndungen in sozialen Netzwerken zu ermöglichen, wurden von einer Arbeitsgruppe der Justizministerkonferenz Empfehlungen für eine Änderung der Anlage B erarbeitet, die zwischenzeitlich von den zuständigen Gremien der Justizminister- und der Innenministerkonferenz gebilligt wurden. In Baden-Württemberg – wie auch in den übrigen Bundesländern – sollen diese Änderungen in den kommenden Wochen durch eine Änderung der Verwaltungsvorschrift vom 8. April 2005 umgesetzt werden.

Die vorgesehenen Änderungen erfüllen nach Auffassung des **Innen-** und des **Justizministeriums** im Wesentlichen die vom Landesbeauftragten für den Datenschutz als erforderlich erachteten, im Tätigkeitsbericht nochmals dargestellten Vorgaben für eine strafprozessuale Öffentlichkeitsfahndung im Internet. Dies gilt zum einen in inhaltlicher Hinsicht, da die insoweit im Regelungsentwurf vorgesehene Einzelfallprüfung, das Erfordernis des Vorliegens einer „schwerwiegenden Straftat“ und die Subsidiaritätsklausel ebenso wie das Begründungserfordernis im Rahmen der staatsanwaltschaftlichen Antragstellung geeignete rechtliche Vorkehrungen sind, um den Anwendungsbereich der künftigen Regelung angemessen zu beschränken. Zum anderen zielen die verfahrensrechtlichen und technischen Vorgaben des Regelungsentwurfs darauf ab, die Wahrung der berechtigten persönlichkeits- und datenschutzrechtlichen Belange Betroffener sowie Dritter umfassend zu gewährleisten.

Der Regelungsentwurf sieht keine obligatorische Deaktivierung der Kommentierungsfunktion bei Öffentlichkeitsfahndungen vor. Unabhängig von der Frage einer technischen Realisierbarkeit ist dies nach Auffassung der Landesjustiz- und Landesinnenverwaltungen insbesondere deshalb nicht erforderlich, da im Falle der Freischaltung der Funktion vorgesehen ist, dass die Seite von den Strafverfolgungsbehörden rund um die Uhr zu überwachen ist und unangemessene Kommentare von Nutzern unverzüglich zu entfernen sind. Nicht zuletzt die anlässlich von Pilotprojekten in anderen Bundesländern gewonnenen Erfahrungen haben gezeigt, dass es bei einer 24/7-Überwachung des Internetauftritts zuverlässig möglich ist, Nutzerkommentare mit unangemessenem Inhalten umgehend zu identifizieren und unverzüglich von der Seite zu entfernen.

Das Innenministerium hat für die auch in Baden-Württemberg geplante Öffentlichkeitsfahndung in sozialen Netzwerken und das dafür zu erstellende Datenschutzkonzept den Landesbeauftragten für den Datenschutz frühzeitig eingebunden.

3.5 Neuordnung des Notariatswesens

Der Tätigkeitsbericht weist auf den immensen Regelungs- und Organisationsbedarf im Zusammenhang mit der Umsetzung der Notariatsreform hin, bei der sicherzustellen sei, dass die Übergabe und Fortführung von laufenden Vorgängen durch die ab 1. Januar 2018 zuständigen Stellen und die Verwahrung von abgeschlossenen Vorgängen datenschutzrechtlichen Anforderungen genüge.

Diese Einschätzung wird vom **Justizministerium** geteilt.

Das Justizministerium ist sich der mit der Umsetzung der Notariatsreform zum Stichtag 1. Januar 2018 verbundenen Herausforderungen bewusst. Den datenschutzrechtlichen Anforderungen wird namentlich bei der Übernahme notarieller Akten durch die zur Fortführung bzw. Abwicklung der zugrunde liegenden notariellen Geschäfte zuständigen Personen und bei der Verbringung notarieller Akten zu den für deren Aufbewahrung zuständigen Amtsgerichten Rechnung getragen werden.

Des Weiteren erwähnt der Tätigkeitsbericht die Arbeiten der von der 81. Konferenz der Justizministerinnen und Justizminister am 23./24. Oktober 2010 in Hamburg beauftragten Bund-Länder-Arbeitsgruppe „Aufbewahrung von Notariatsunterlagen“, in der das Justizministerium unter der Federführung Niedersachsens mitwirkt. Diese Arbeitsgruppe soll einen Gesetzentwurf für eine Neuordnung der Aufbewahrung von Notariatsunterlagen und die Errichtung eines Elektronischen Urkundenarchivs erstellen. Die Arbeitsgruppe setzt sich aus Vertretern der Landesjustizverwaltungen, des Bundesministeriums für Justiz und Verbraucherschutz sowie der Bundesnotarkammer und der Landesarchivverwaltungen zusammen.

Das Justizministerium hatte den Landesbeauftragten für den Datenschutz zu den Zwischenergebnissen der Arbeitsgruppe angehört und dessen Stellungnahme vom 12. März 2015 unverändert in die Beratungen der Arbeitsgruppe eingebracht.

Den darin erhobenen Bedenken gegen den Wegfall der Kontrollbefugnisse der Landesbeauftragten für den Datenschutz über die Notare wurde seitens der Arbeitsgruppe entsprochen, da die Bundesnotarkammer an ihrem entsprechenden Regelungsvorschlag nicht festhält.

Soweit der Tätigkeitsbericht darüber hinaus Bedenken wegen des Auseinanderfallens der Führung des elektronischen Urkundenverzeichnisses durch die Bundesnotarkammer einerseits und der Verantwortung der Notare für die darin gespeicherten personenbezogenen Daten andererseits sowie wegen der nicht immer eindeutigen Regelung der Verantwortlichkeit für einzelne Datenverarbeitungsvorgänge erhoben hat, wird das Justizministerium dies bei den weiteren Beratungen in der Arbeitsgruppe einbringen; über den Fortgang der Beratungen wird das Justizministerium den Landesbeauftragten für den Datenschutz – wie bereits zugesagt – informieren.

3.6 Kontrollen bei Notariaten

Die festgestellten Datenschutzverstöße seitens der Notariate betreffend die Aufbewahrung des datenschutzrelevanten Altpapiers bis zur Übergabe an die entsorgungspflichtige Gemeinde haben nach Auskunft des **Justizministeriums** stattgefunden. Eines der Notariate war nach Auskunft des dienstaufsichtsführenden Notars bereits von sich aus vor dem Kontrollbesuch der Mitarbeiter des Landesbeauftragten für den Datenschutz aktiv geworden. Der Kontrollbesuch fand statt, während Maßnahmen zur datenschutzgerechten Aufbewahrung von Altpapier geprüft und mit der Gemeinde besprochen wurden, und konnte dazu beitragen, dass die zuständige Gemeinde Datencontainer zur Verfügung stellt. Auch bei dem anderen angesprochenen Notariat wurden Datencontainer angeschafft, so dass der Datenschutzverstoß in beiden Notariaten inzwischen beseitigt ist und sich nicht wiederholen wird.

Auch der Datenschutzverstoß eines Notariats betreffend die unzureichende Hinwirkung auf eine den datenschutzrechtlichen Anforderungen genügende räumliche Ausstattung und Möblierung des Notariats seitens der Gemeinde hat stattgefunden. Die nicht den datenschutzrechtlichen Anforderungen genügende, kaputte, nur provisorisch reparierte Stockwerkstür wurde zwischenzeitlich in Stand gesetzt. Der Datenschutzverstoß seitens des Notars wird sich, wie das Justizministerium mitteilt, nicht wiederholen.

3.7 Kaputte Schlösser am Aktenschrank

Die Ausführungen in dem Tätigkeitsbericht sind korrekt. Der Datenschutzverstoß hat stattgefunden, dauerte allerdings nur kurze Zeit an, wurde abgestellt und wird sich nach dem Hinweis des **Justizministeriums** nicht wiederholen.

3.8 Unberechtigte Informationsweitergabe zwischen Gerichtsvollziehern

Die nach Erhalt der Beanstandungen des Landesbeauftragten für den Datenschutz durch das **Justizministerium** durchgeführten Prüfungen haben ergeben, dass die Feststellungen des Landesbeauftragten sowohl in tatsächlicher als auch in rechtlicher Hinsicht bestätigt werden können. Hierauf hat das Justizministerium u.a. die bereits in dem Tätigkeitsbericht angesprochenen Maßnahmen ergriffen, um vergleichbare Verletzungen der Vorgaben des Datenschutzrechts wirksam auszuschließen. Die Maßnahmen zielen zum einen darauf, den Gerichtsvollzieherinnen und Gerichtsvollziehern des Landes die datenschutzrechtliche Relevanz bestimmter Übermittlungsvorgänge und die in diesem Zusammenhang zu beachtenden Prüfungsmaßstäbe deutlich vor Augen zu führen; die Präsidenten der Oberlandesgerichte sind umgehend der Bitte des Justizministeriums nachgekommen, allen Gerichtsvollzieherinnen und Gerichtsvollziehern die hierzu erforderlichen Informationen zuzuleiten. Zum anderen soll dem Thema Datenschutz in der Aus- und Fortbildung noch mehr Raum gegeben werden; zu diesem Zweck wird der Studienplan des Bachelorstudiengangs für Gerichtsvollzieherinnen und Gerichtsvollzieher einer Überprüfung unterzogen. Außerdem hat die Aufbereitung des Vorgangs zu dem Vorhaben des Deutschen

Gerichtsvollzieher Bundes – Landesverband Baden-Württemberg e.V. – geführt, den Datenschutz zu einem Thema der Jahrestagung 2016 des Landesverbandsvorstands mit den Leiterinnen und Leitern der Bezirksgruppen sowie der sich anschließenden Versammlungen der Gerichtsvollzieherinnen und Gerichtsvollzieher in den Landgerichtsbezirken zu machen.

4. Steuern und Statistik

Zensus 2011 – und kein Ende!

Wie das **Ministerium für Finanzen und Wirtschaft** mitteilt, sind die Gerichtsverfahren, aufgrund derer – wie im Tätigkeitsbericht dargestellt – auf die Löschung vorläufig verzichtet wurde, weiter anhängig. Die vom Bundesverfassungsgericht angeordnete Außervollzugsetzung der Löschungsvorschrift im Zensusgesetz 2011 ist für alle Behörden und Gerichte bindend. Das Statistische Landesamt ist daher, worauf das Ministerium für Finanzen und Wirtschaft hinweist, verpflichtet, bis auf weiteres von der Löschung der noch vorhandenen Datenbestände abzusehen.

Der Beschluss des VGH Baden-Württemberg vom 7. August 2015 bezüglich der Herausgabe von E-Mails an den Untersuchungsausschuss Schlossgarten II des Landtags von Baden-Württemberg wird vom **Umweltministerium** positiv bewertet. Die Rechtsposition von Untersuchungsausschüssen wird gestärkt, ohne dass datenschutzrechtliche Belange in den Hintergrund treten. Die genannten Sicherungskopien wurden am 27. November 2015 gelöscht und die entsprechenden Datenträger zerstört.

5. Kommunales und andere Verwaltungsbereiche

5.4.1 Datenübermittlungen an externe Energieberater

Das **Umweltministerium** hat das Projekt „Energiekarawane“ der Metropolregion Rhein-Neckar in den Jahren 2011 und 2012 gefördert. In den Nebenbestimmungen wurde dabei u.a. aufgenommen, dass die Bestimmungen des Landesdatenschutzgesetzes in der Fassung vom 18. September 2000 zu beachten sind. Die Diskussion des Landesbeauftragten für den Datenschutz mit der in seinem Bericht erwähnten Gemeinde war dem Umweltministerium nicht bekannt.

Nach § 8 Absatz 2 des Klimaschutzgesetzes Baden-Württemberg obliegt es einer Gemeinde, ihre Gemeindemitglieder über Maßnahmen, die dem Klimaschutz in der Gemeinde dienen, zu informieren; dabei können auch Vorschläge für einzelne Maßnahmen enthalten sein. Zu entsprechenden Maßnahmen gehört auch die energetische Sanierung von Gebäuden. Wie im Bericht des Landesbeauftragten für den Datenschutz ausgeführt, ist im Einzelfall zu prüfen, ob die datenschutzrechtlichen Voraussetzungen für eine Nutzung damit zusammenhängender personenbezogener Daten vorliegen.

Die Darstellung des Sachverhalts durch den Landesbeauftragten für den Datenschutz ist nach Auskunft des **Innenministeriums** zutreffend, die rechtliche Beurteilung wird vom Innenministerium geteilt. Die Gemeinde hat sich auf Grund der Beanstandungen des Landesbeauftragten für den Datenschutz intensiv durch dessen Behörde beraten lassen und ihr fehlerhaftes Vorgehen eingesehen. Es ist geplant, gemeinsam mit zwei Nachbarkommunen einen Beauftragten für den Datenschutz zu bestellen, um künftig den Datenschutz in der Gemeindeverwaltung zu gewährleisten.

5.4.2 Notwendigkeit der Vermittlung datenschutzrechtlicher Grundlagen und
5.4.4 Datenschutzrechtliches Verbot mit Erlaubnisvorbehalt

Das **Innenministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz, dass umfassende Schulungsangebote für die Kommunen im Datenschutzrecht wünschenswert sind und begrüßt es daher, dass der Landesbeauftragte für den Datenschutz auf Anfrage einzelner Kommunen entsprechende Schulungen durchgeführt hat. Allerdings kann das Innenministerium dem Anliegen des Landesbeauftragten für den Datenschutz, die Vermittlung datenschutzrechtlicher Grundlagen (auch) den kommunalen Aufsichtsbehörden zu übertragen und entsprechende Schulungsangebote für die Kommunen zu unterbreiten, nicht näher treten. Die kommunalen Aufsichtsbehörden haben eine Vielzahl von Aufgaben zu erfüllen und sind in Anbetracht ständiger Einsparungen im Personalbereich nicht in der Lage, zusätzliche Aufgaben zu übernehmen. In dieser Hinsicht sind seit dem letzten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz keine Änderungen eingetreten. Ergänzend weist das Innenministerium darauf hin, dass konkrete datenschutzrechtliche Einzelfragen der Kommunen im Rahmen der Rechtsaufsicht geprüft werden können.

5.4.3 Behördliche Datenschutzbeauftragte

Nach § 10 Abs. 1 Satz 1 LDSG ist es in das Ermessen der Kommunen in Baden-Württemberg gestellt, ob sie einen behördlichen Datenschutzbeauftragten bestellen. Diese Regelung trägt dem Umstand Rechnung, dass die Kommunen im Rahmen ihrer Selbstverwaltungshoheit selbst entscheiden und verantworten können, ob sie einen Datenschutzbeauftragten bestellen und ggf. welche Strukturen sie insoweit als sinnvoll erachten (vgl. § 10 Abs. 2 LDSG). Die vom Landesbeauftragten für den Datenschutz geforderte Verpflichtung für die Kommunen, einen Datenschutzbeauftragten zu bestellen, wird vor diesem Hintergrund vom **Innenministerium** abgelehnt. Die geltende Ermessensregelung für die Bestellung eines Datenschutzbeauftragten trägt nach Auffassung des Innenministeriums der kommunalen Selbstverwaltung und dem Subsidiaritätsgedanken Rechnung und ist daher beizubehalten.

6. Verkehr

6.1 Datenschutz um das Kraftfahrzeug: Automatisches und vernetztes Fahren, Elektromobilität und Pkw-Maut

In Umsetzung der Richtlinie 2010/40/EU zur Einführung Intelligenter Verkehrssysteme müssen einige Dienste installiert werden, die aber, worauf das **Ministerium für Verkehr und Infrastruktur** hinweist, nicht immer zur Erfassung personenbezogener Daten führen.

Dies gilt z.B. für die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lkw und andere gewerbliche Fahrzeuge (Delegierte Verordnung EU Nr. 885/2013) sowie für die Bereitstellung eines Mindestniveaus allgemeiner, für die Straßenverkehrssicherheit relevanter Verkehrsinformationen (Delegierte Verordnung EU Nr. 886/2013). Bezüglich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationen (Delegierte Verordnung EU Nr. 962/2015) können im Rahmen der Generierung von Echtzeit-Verkehrsinformationen in Abhängigkeit von der eingesetzten Technik personenbezogene Daten erfasst und verarbeitet werden (z.B. Bluetooth-Technologie). Die Straßenbauverwaltung Baden-Württemberg erfasst und verarbeitet derzeit keine personenbezogenen Daten zur Ermittlung von Reisezeiten. Eine Ausnahme hiervon stellt die Reisezeitermittlung für die Netzbeeinflussungsanlage Rhein-Neckar dar. Hierauf wird bei den Ausführungen zu Kapitel 6.5 näher eingegangen.

Die Umsetzung von „Baustellenwarnern“ und „Verkehrslageerfassung“ im Rahmen der Einführung Kooperativer Systeme in Deutschland im Korridor Rotterdam – Frankfurt a.M. –

Wien erfolgt unter der Federführung des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI). Das BMVI ist neben der technischen, organisatorischen und finanziellen Umsetzung auch für den Datenschutz und die Datensicherheit der beiden Projekte verantwortlich. Hierzu steht das BMVI mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Kontakt und nimmt die notwendigen Abstimmungen vor.

Zum autonomen Fahren teilt das Ministerium für Verkehr und Infrastruktur die Auffassung des Landesbeauftragten und setzt sich für Datenschutz ein. Mit Ausschreibung des Landes Baden-Württemberg zu einem eigenen „Testfeld autonomes Fahren“ adressiert das Ministerium für Verkehr und Infrastruktur in einem zweiten Schritt auch die Untersuchung zu rechtlichen Fragen und dem Datenschutz.

Des Weiteren ist das Ministerium für Verkehr und Infrastruktur seit dem Jahr 2016 am „Runden Tisch Autonomes Fahren“ (RTAF) vertreten, ebenso in dessen Unterarbeitsgruppe „Gesellschaftliche Akzeptanz“.

6.2 Projekt TwoGO

Für nahezu alle Lebenslagen und Interessen werden heute Apps (*applications*) für mobile Endgeräte angeboten. Die Verbreitung von Mitfahr-Apps haben sich Unternehmen zunutze gemacht und bieten in der Nische zwischen gewerbsmäßiger Personenbeförderung und privatem Mitfahrangebot neue Mobilitätsdienstleistungen an. Für das **Ministerium für Verkehr und Infrastruktur** lag es nahe, das Potenzial von Mitfahr-Apps für eine nachhaltigere Mobilität der Landesbeschäftigten zu erkunden und nutzbar machen. Denn die Landesverwaltung ist einerseits gesetzlich verpflichtet, beim Klimaschutz mit gutem Beispiel voran zu gehen (§ 7 Klimaschutzgesetz Baden-Württemberg). Andererseits erhöhen bei der Luftreinhaltung aktuell zwei EU-Vertragsverletzungsverfahren zur Luftreinhaltung den Handlungsdruck auf die Landesregierung – insbesondere an ihrem Sitz in Stuttgart – zur Entlastung von Pendlerverkehren auf den Straßen und zur Lösung der Feinstaubproblematik beizutragen.

In einem Ausschreibungs- und Vergabeverfahren wählte das Ministerium für Verkehr und Infrastruktur die am Markt eingeführte Lösung TwoGo aus, die das Software-Unternehmen SAP für seine eigene Belegschaft entwickelt hatte, aber in einer offenen Version jedermann zur kostenlosen Nutzung anbot. Für das Ministerium für Verkehr und Infrastruktur kam es dabei auf einen hohen Datenschutzstandard für die geschlossene Benutzergruppe aus den Beschäftigten der Landesministerien und der Landeshauptstadt Stuttgart an, da Medienberichte über den geringen Datenschutzstandard ausländischer Diensteanbieter und spektakuläre Verletzungen der Privatsphäre von Mitfahrerinnen und Mitfahrern die neuen informationstechnischen Lösungen auch hierzulande in Misskredit zu bringen drohten.

Dank der engagierten und wertvollen Beratung durch den Landesbeauftragten für den Datenschutz gelang es, denjenigen Beschäftigen von Ministerien und Landeshauptstadt, die für ihren Weg zum Arbeitsplatz auf motorisierte Individualverkehrsmittel nicht verzichten können oder wollen, mit der App TwoGo eine umweltfreundliche und kostengünstige Alternative zum Alleinfahren anzubieten, noch vor Auslösung des ersten Feinstaubalarms in Stuttgart im Januar 2016. SAP konnte sein Produkt TwoGo am Standard des baden-württembergischen Datenschutzes messen und so noch weiter verbessern.

6.3 PolyGO: Eine für alles, alles auf einer?

Das **Ministerium für Verkehr und Infrastruktur** misst der Einführung von elektronischem Ticketing im ÖPNV im Hinblick auf die Kundenorientierung und die Erleichterung der Nutzung entsprechender Verkehrsmittel hohe Bedeutung zu. Im Rahmen des Landesgemeindeverkehrsfinanzierungsgesetzes (LGVFG) ist deshalb zukünftig eine Förderung von elektronischem Ticketing vorgesehen. Der Landesbeauftragte für den Datenschutz wurde im Rahmen dieser Gesetzesnovellierung beteiligt. Auf seine Empfehlung hin werden im Rahmen der Neuaufstellung der Verwaltungsvorschrift zum LGVFG bzw. in den entsprechenden Richtlinien datenschutzrechtliche Aspekte aufgegriffen. Die Gesetzesbegründung selbst wurde entsprechend ergänzt. Die derzeit in der Erstellung befindliche Verwaltungsvorschrift sieht vor, dass Vorhaben des LGVFG, die die Verarbeitung personenbezogener Daten umfassen (z.B. durch den Einsatz von datenverarbeitenden Technologien), die Anforderungen des Datenschutzrechts einzuhalten haben bzw. der zuständige Datenschutzbeauftragte im Vorfeld der Vorhaben zu beteiligen ist. Damit soll sichergestellt werden, dass zukünftig beim Einsatz von E-Ticketing die entsprechenden Rechtsgrundlagen beachtet werden. Es ist darauf hinzuweisen, dass die Kernapplikation (der sogenannte VDV-KA Standard) als sehr sichere Technologie betrachtet werden muss.

Der Landesbeauftragte für den Datenschutz hat eine Ausprägung der Mobilitätskarte geprüft, bei der eine Anwendung das elektronische Ticketing für den ÖPNV ist. Hierbei stellt er fest, dass die Aufdeckung von Missbrauchsfällen ein grundsätzlich berechtigtes Interesse für die entsprechende Datenverarbeitung darstellt und der Schwerpunkt vielmehr darauf gelegt werden muss, die hierfür erforderlichen Verarbeitungen abzugrenzen und sicherzustellen, dass personenbezogene Daten nicht zu lange gespeichert werden. Das Ministerium für Verkehr und Infrastruktur teilt diese Rechtsauffassung.

6.5 Reisezeitermittlung

Die Steuerung von Netzbeeinflussungsanlagen (NBA) erfolgt derzeit im Sinne eines reagierenden Systems, wobei im Fall einer Störung auf der Normalroute eine entsprechende Umlenkungsempfehlung angezeigt wird. Diese wird automatisch vom Steueralgorithmus der NBA generiert. Als Grundlage dienen die erfassten lokalen Verkehrsdaten. Durch diese lokale Verkehrsdatenerfassung und modellhafte Berechnung der Störfallausprägungen ergeben sich jedoch Schwachpunkte bei der Reisezeitermittlung. Verbesserungen in der Reisezeitermittlung können vor allem durch das Einbinden von tatsächlich aktuell gemessenen strecken- und relationsbezogenen Daten in den Steueralgorithmus erzielt werden. Ein entsprechendes System zur videobasierten Reisezeitermittlung wurde bereits durch ein Konsortium entwickelt.

Für die Ermittlung von Reisezeiten sollen an relevanten Standorten im Bereich der NBA Rhein-Neckar insgesamt 19 Kameras installiert und die Kennzeichen der vorbeifahrenden Fahrzeuge erfasst werden. Über die Wiedererkennung an einem anderen Standort kann die aktuelle Reisezeit zwischen den beiden Standorten ermittelt werden. Da dies aus datenschutzrechtlichen Gründen nicht direkt über einen Kennzeichenvergleich erfolgen darf, wurde ein entsprechendes Datenschutz- und Sicherheitskonzept entwickelt und im Vorfeld dem Landesbeauftragten für den Datenschutz zur Prüfung und Zustimmung vorgelegt. Die vom Landesbeauftragten für den Datenschutz als Auflage genannten technischen Änderungen im Konzept wurden zwischenzeitlich durch die Landesstelle für Straßentechnik aufgenommen und ausgearbeitet. Das überarbeitete Konzept wurde dem Landesbeauftragten für den Datenschutz erneut übersandt. Dies hat sich mit der Veröffentlichung des 32. Tätigkeitsberichtes überschnitten.

7. Gesundheit und Soziales

7.1 Das Gesetz über den öffentlichen Gesundheitsdienst (Gesundheitsdienstgesetz)

Im Rahmen der Erarbeitung des Referentenentwurfs zur Novellierung des Gesundheitsdienstgesetzes hat das **Sozialministerium** den Landesbeauftragten für den Datenschutz gemäß den Vorgaben der zu diesem Zeitpunkt geltenden Verwaltungsvorschrift der Landesregierung und Ministerien zur Erarbeitung von Regelungen vom 1. Januar 2011 (Nummer 5.2.4) zeitgleich mit den anderen Ministerien, dem Beauftragten der Landesregierung für Bürokratieabbau sowie dem Rechnungshof Baden-Württemberg beteiligt. Die Frist von zwölf Werktagen war aus Sicht des Sozialministeriums vor dem Hintergrund der begrenzt verfügbaren Kabinettstermine für die Einbringung der Kabinettsvorlage noch vor der Sommerpause angemessen. Schließlich konnten in der Zeit der Durchführung der öffentlichen Anhörung zum Entwurf des Gesundheitsdienstgesetzes von Ende Juli bis Anfang September 2015 die datenschutzrechtlichen Bedenken des Landesbeauftragten für den Datenschutz im Verlauf eines ausführlichen Erörterungsgesprächs auf Arbeitsebene beraten werden.

Die Anmerkungen und Hinweise führten zur Klärung der datenschutzrechtlichen Bedenken sowie der Präzisierung und Korrektur der noch im Referentenentwurf enthaltenen Vorschriften. Mit den nachgearbeiteten Formulierungen wurde der dann fortgeschriebene Gesetzentwurf als Gesetzesinitiative der Landesregierung dem Landtag zugeleitet und schließlich am 16. Dezember 2015 vom Landtag beschlossen.

7.3.1 Dauerpatient Krankenhaus und
7.3.2 Umsetzung Orientierungshilfe – Krankenhausinformationssysteme und
7.3.3. Auskünfte gegenüber Strafverfolgungsbehörden und
7.10.1. Datenlecks in Krankenhäusern

Vor dem Hintergrund der im Tätigkeitsbericht enthaltenen Darstellung wird die rechtliche Beurteilung des Landesbeauftragten für den Datenschutz vom **Sozialministerium** geteilt.

Der 7. Abschnitt des Landeskrankenhausgesetzes Baden-Württemberg (LKHG) enthält umfassende Bestimmungen zum Datenschutz im Krankenhaus. Das Sozialministerium ist jedoch nicht aufsichtsberechtigt bezüglich der Einhaltung datenschutzrechtlicher Vorschriften. Dementsprechend beschränken sich seine Möglichkeiten auf allgemeine Hinweise gegenüber Krankenhausträgern.

Das Sozialministerium hält es für geboten, die Krankenhäuser im Land darauf hinzuweisen, dass im Hinblick auf den Umgang mit sensiblen Patientendaten datenschutzrechtliche

Bestimmungen genauestens zu beachten sind. Das Ministerium hat daher die Baden-Württembergische Krankenhausgesellschaft (BWKG) angeschrieben und darum gebeten, dass diese ihre Mitgliedskrankenhäuser auf den Tätigkeitsbericht des Landesbeauftragten für den Datenschutz aufmerksam macht und an die Einhaltung des Datenschutzes im Krankenhaus erinnert.

Explizit hingewiesen wurde auf die Notwendigkeit einer verbesserten Umsetzung der Orientierungshilfe Krankenhausinformationssysteme (OH KIS), außerdem auf die mit dem Einsatz externer Dienstleister für die Datenverarbeitung verbundenen datenschutzrechtlichen Gefahren. Das Ministerium hat gebeten, bei der im Auftrag der Krankenhäuser erfolgenden Datenverarbeitung durch externe Stellen ein datenschutzrechtlich korrektes Verfahren zu gewährleisten.

7.6.1 Hausbesuche bei fehlgeleiteten Arbeitsunfähigkeitsbescheinigungen und
7.6.2 Krankengeldfallmanagement der Krankenkassen

Das **Sozialministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz. Es wird die unter den hiesigen Zuständigkeitsbereich fallenden landesunmittelbaren Krankenkassen sowie deren Verbände über die monierten Sachverhalte informieren und um Beachtung bitten.

7.6.3 Bekanntgabe von Reha-Entlassungsberichten an die Deutsche Rentenversicherung

Das **Sozialministerium** weist darauf hin, dass das o.g. Thema in den zuständigen Gremien der Deutschen Rentenversicherung ausführlich beraten und rechtlich bewertet wurde. Im Ergebnis ist festzustellen, dass seit dem 19. März 2014 in der Deutschen Rentenversicherung bezüglich der Bekanntgabe von Reha-Entlassungsberichten eine einheitliche Rechtslage gilt.

Die Deutsche Rentenversicherung Baden-Württemberg stuft – wie die im Tätigkeitsbericht positiv hervorgehobene Deutsche Rentenversicherung Bund – die Weitergabe von Reha-Entlassungsberichten durch private Rehabilitationseinrichtungen als Datenübermittlung und nicht mehr als interne Weitergabe bzw. Nutzung ein. Damit besteht die gewünschte Rechtsklarheit.

7.7.1 Kontrollbesuch beim Medizinischen Dienst der Krankenversicherung und

7.7.2 Ende des Umschlagverfahrens und
7.10.3 Medizinischer Dienst der Krankenversicherung (MDK)

Das **Sozialministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz. Es wird den Medizinischen Dienst der Krankenversicherung Baden-Württemberg über die monierten Sachverhalte informieren und um Beachtung bitten.

7.8.1 Datenerhebung durch Hilfsmittelerbringer in Pflegeeinrichtungen

Das **Sozialministerium** teilt die Auffassung des Landesbeauftragten für den Datenschutz. Es wird die unter den hiesigen Zuständigkeitsbereich fallenden landesunmittelbaren Krankenkassen sowie deren Verbände über den monierten Sachverhalt informieren und um Beachtung bitten.

Der im Tätigkeitsbericht angesprochene Vorgang wurde beim **Regierungspräsidium Karlsruhe** mit Schreiben des Landesbeauftragten für den Datenschutz vom 4. November 2015 angezeigt. Da jedoch von Seiten der Betroffenen vorgetragen wurde, dass sie die hier gegenständliche Tätigkeit als Hilfsmittelerbringer/Leistungserbringer im Sinne von § 294 SGB V auf vertraglicher Grundlage mit den Krankenkassen vorgenommen habe, handelt es sich nach derzeitigen Erkenntnissen nicht um eine Ordnungswidrigkeit nach dem Bundesdatenschutzgesetz, sondern es kommt eine Ordnungswidrigkeit nach den spezielleren Vorschriften des Sozialgesetzbuchs (hier: § 85 SGB X) in Betracht. Für deren Verfolgung ist nicht das Regierungspräsidium Karlsruhe, sondern gemäß § 2 Abs. 1 OWiZuVO die untere Verwaltungsbehörde zuständig. Nach Rücksprache beim Landesbeauftragten für den Datenschutz prüft man dort derzeit, ob das von Seiten der Betroffenen vorgebrachte Vertragsverhältnis tatsächlich besteht. Sobald diese Erkenntnisse vorliegen, kann abschließend über die Bußgeldzuständigkeit entschieden und der Vorgang entsprechend weitergeleitet werden.

7.8.2 Fotoaufnahmen von Pflegeheimbewohnern für Notfall- und Evakuierungspläne

Dem **Sozialministerium** liegen keine Erkenntnisse darüber vor, ob und inwieweit die Fotodokumentation für Fälle der Evakuierung von Gebäuden gängige Praxis in Pflegeheimen ist. Es wird aber den geschilderten Sachverhalt zum Anlass nehmen, die Heimaufsichtsbehörden zu gegebener Zeit über die Problematik zu informieren und zu bitten, die Betreiber von Pflegeheimen entsprechend zu sensibilisieren.

7.11.2 Formulare

Soweit der Landesbeauftragte für den Datenschutz zunächst rügt, dass Leistungsberechtigte aufgefordert wurden, ihren Antrag über ihr Bürgermeisteramt beim Jobcenter einzureichen, wird seine Auffassung vom **Sozialministerium** geteilt. Anträge sind grundsätzlich beim zuständigen Leistungsträger – hier die Jobcenter – zu stellen. § 16 Abs. 1 Satz 2 Erstes Buch Sozialgesetzbuch (SGB I) schafft hiervon lediglich eine Ausnahme, wonach Anträge von unzuständigen Stellen entgegenzunehmen sind. Auch soweit gerügt wurde, dass die Wohnsitzgemeinde aufgefordert worden sei, die Angaben des Antragstellers zu bestätigen, stimmt das Sozialministerium mit der Auffassung des Landesbeauftragten für Datenschutz überein. Es ist in beiden Fällen beabsichtigt, die Träger über die gemeinsame Auffassung zu informieren.

Soweit der Landesbeauftragte für den Datenschutz darüber hinaus den Personenkreis, von welchem Angaben zu Einkommen und Vermögen gefordert wird, als zu weit erachtet, gibt das Sozialministerium Folgendes zu bedenken:

Leben Hilfebedürftige in Haushaltsgemeinschaft mit Verwandten oder Verschwägerten, so wird nach § 9 Abs. 5 Zweites Buch Sozialgesetzbuch (SGB II) vermutet, dass sie von ihnen Leistungen erhalten, soweit dies nach deren Einkommen und Vermögen erwartet werden kann. Der Eintritt der Vermutung ist dabei an zwei Voraussetzungen geknüpft: Zum einen ist das Zusammenleben in einer Haushaltsgemeinschaft mit Verwandten oder Verschwägerten erforderlich, zum anderen muss von diesen ganz oder teilweise erwartet werden dürfen, dass sie für den Hilfebedürftigen Leistungen zum Lebensunterhalt erbringen. Eine Haushaltsgemeinschaft liegt vor, wenn die Personen mit dem Erwerbsfähigen in einem gemeinsamen Haushalt zusammen leben und „aus einem Topf“ wirtschaften (BT-Drs. 15/1516, S. 53). Damit ist der Begriff der Haushaltsgemeinschaft weiter als der der Bedarfsgemeinschaft.

In einem zweiten Schritt hat das Jobcenter sodann zu überprüfen, ob Unterstützungsleistungen seitens der Verwandten oder Verschwägerten nach deren Einkommens- und Vermögensverhältnissen erwartet werden können. Im Hinblick auf das zu berücksichtigende Einkommen ist hierfür § 1 Abs. 2 der Verordnung zur Berechnung von Einkommen sowie zur Nichtberücksichtigung von Einkommen und Vermögen beim Arbeitslosengeld II/Sozialgeld (ALGII-V) maßgeblich. Danach sind die um die Absetzbeträge nach § 11b

SGB II bereinigten Einnahmen in der Regel nicht als Einkommen zu berücksichtigen, soweit sie einen Freibetrag in Höhe des doppelten Betrags des nach § 20 Abs. 2 Satz 1 SGB II maßgebenden Regelbedarfs zuzüglich der anteiligen Aufwendungen für Unterkunft und Heizung sowie darüber hinausgehend 50 Prozent der diesen Freibetrag übersteigenden bereinigten Einnahmen nicht überschreiten. Im Einzelfall können dabei besondere Umstände Berücksichtigung finden. Hierzu gehören besondere Bedarfssituationen des Angehörigen wie z.B. ein vorhandener Mehrbedarf im Sinne von § 21 SGB II. Dabei sieht u.a. § 21 Abs. 4 SGB II einen Mehrbedarf für erwerbsfähige behinderte Leistungsberechtigte vor, denen Leistungen zur Teilhabe am Arbeitsleben nach § 33 Neuntes Buch Sozialgesetzbuch (SGB IX) oder sonstige Hilfen zur Erlangung eines geeigneten Platzes im Arbeitsleben oder Eingliederungshilfen nach § 54 Abs. 1 Satz 1 Nr. 1-3 des Zwölften Buches Sozialgesetzbuch (SGB XII) erbracht werden. Hieraus dürfte sich die Frage nach einer Behinderung erklären.

Nach alledem dürfte zwar eine Abfrage von allen Haushaltsangehörigen zu weit führen. Die Abfrage nach dem Einkommen und Vermögen der in der Haushaltsgemeinschaft lebenden verwandten und verschwägerten Personen dürfte nach hiesiger Auffassung jedoch im Hinblick auf § 9 Abs. 5 SGB II erforderlich sein. Eine Beschränkung auf die Mitglieder der Bedarfsgemeinschaft ist daher zu eng.

7.12.1 Das neue Gesetz und
7.12.2 Prüfberichte der Heimaufsicht

Der Bericht bezieht sich im Wesentlichen auf das in § 8 Wohn-, Teilhabe- und Pflegegesetz (WTPG) geregelte Transparenzgebot. Er fasst sehr klar zusammen, dass der Landesgesetzgeber den Konflikt zwischen dem Informationsbedürfnis der (künftigen) Bewohner und dem Recht auf informationelle Selbstbestimmung der im Bericht ggf. erwähnten Bewohner erkannt und deshalb eine Anonymisierungspflicht der Heimaufsichtsbehörde festgeschrieben hat. Das **Sozialministerium** als oberste Heimaufsichtsbehörde hat die Heimaufsichtsbehörden unmittelbar nach Inkrafttreten des WTPG im Rahmen einer Sonderfachtagung detailliert über ihre Pflichten im Umgang mit dem Transparenzgebot und der Erstellung eines korrekten Prüfberichts informiert. So wurden die Heimaufsichtsbehörden etwa auch darin unterrichtet, wie der Prüfbericht inhaltlich ausgestaltet werden darf bzw. welche Daten mittels welcher Methoden (Platzhalter, Schwärzen) zu anonymisieren sind.

Mit dem Landesbeauftragten für den Datenschutz ist darin übereinzustimmen, dass die Gesetzeslage im Hinblick auf den Umgang mit dem Transparenzgebot klar und eindeutig geregelt ist. Bei der Umsetzung dieser Vorgaben traten in der Tat Anfangsschwierigkeiten auf, wie dies bei neu in Kraft getretenen Gesetzen nicht selten der Fall ist. Das Sozialministerium hat die vom Landesbeauftragten für den Datenschutz erwähnten Prüfberichte umgehend zum Anlass genommen, die Heimaufsichtsbehörden im Rahmen einer erneuten Sonderfachtagung sowie anlässlich der regelmäßig stattfindenden Dienstbesprechungen mit den Heimaufsichtsbehörden intensiv im Umgang mit dem Transparenzgebot und der Anonymisierungspflicht zu schulen und zu sensibilisieren. Nach hiesigem Kenntnisstand sind seit dieser Intervention keine Verstöße mehr aufgetreten. Selbstverständlich wird dieses Thema von hier aus weiter aufmerksam beobachtet und verfolgt.

7.12.3 Zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen

Das **Sozialministerium** weist darauf hin, dass die vom Landesbeauftragten für den Datenschutz beschriebene Problematik im Umgang mit dem pauschalen Zuschlag zum Pflegegeld nach § 38a SGB XI den Ländern bekannt war. Sie hatten deshalb im Rahmen des Gesetzgebungsverfahrens zum Ersten Pflegestärkungsgesetz (PSG I) darauf hingewirkt, eindeutige Regelungen zu denjenigen Daten zu treffen, die beim Antragsteller zur Feststellung der Anspruchsvoraussetzungen erhoben werden dürfen. Der Bundesgesetzgeber hat daraus die entsprechenden gesetzestechnischen Konsequenzen gezogen und festgeschrieben, dass personenbezogene Daten von pflegebedürftigen Mitbewohnern zu diesem Zweck nicht mehr erhoben werden dürfen. Zu Missständen wie dem beschriebenen dürfte es mithin künftig nicht mehr kommen.

7.13 Wohngeld: Das Formular

Die Ausführungen des Landesbeauftragten für den Datenschutz hinsichtlich der Datenerhebung durch eine Wohngeldbehörde sind zutreffend. Aus Sicht des **Ministeriums für Finanzen und Wirtschaft** als Fachaufsichtsbehörde ist der Vorgang aus rechtlicher Sicht wie folgt zu bewerten:

Die Wohngeldbehörde hat nach § 20 Zehntes Buch Sozialgesetzbuch (SGB X) den Sachverhalt von Amts wegen zu ermitteln. Die Wohngeldbehörde darf Sozialdaten nur erheben, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist (§ 67 a Abs. 1 Satz 1 SGB X). Dieser Grundsatz schränkt daher den allgemeinen Amtsermittlungsgrundsatz nach § 20 SGB

X ein.

Nach dem Wohngeldgesetz (WoGG) gilt, dass bei der Ermittlung des Jahreseinkommens nach § 15 WoGG grundsätzlich das vom Antragsteller nachgewiesene Einkommen zugrunde zu legen ist. Liegt dieses jedoch unter dem sozialrechtlichen Bedarf, sind diese Angaben besonders sorgfältig auf Glaubhaftigkeit und Vollständigkeit zu überprüfen. In diesen Fällen wird die Wohngeldbehörde im Regelfall den Antragsteller zur Stellungnahme auffordern und ihn bitten, weitere Angaben zur Glaubhaftmachung der Einkommenssituation zu tätigen. Der Antragsteller sollte in diesen Fällen nachvollziehbar darlegen, dass der notwendige Lebensunterhalt mit den zur Verfügung stehenden Mitteln finanziert werden kann. Hierbei kommt es maßgeblich auf die individuellen Umstände an. Die Plausibilität der Einnahmen kann z.B. durch detaillierte Angaben zu den Ausgaben oder durch den Verbrauch von Vermögen dargelegt werden. Eine umfassende Offenlegung der Ausgaben zur Darlegung der Plausibilität kann jedoch die Wohngeldbehörde vom Antragsteller nicht fordern. Zudem muss der Antragsteller auf die Möglichkeit hingewiesen werden, einen Nachweis der Plausibilität auch auf andere Weise erbringen zu können. Sofern der Antragsteller bei der Feststellung der leistungserheblichen Tatsachen nicht mitwirkt, kann nach Ziff. 15.01 Abs. 2 Satz 2 der Wohngeld-Verwaltungsvorschrift (WoGVwV) die Wohngeldleistung ohne weitere Ermittlungen ganz oder teilweise versagt oder entzogen werden (§ 66 i.V.m. § 60 SGB I).

Das Ministerium für Finanzen und Wirtschaft stellt den für die Durchführung des Wohngeldgesetzes zuständigen Stellen einheitliche amtliche Vordrucke zur Verfügung. Diese wurden zuletzt durch das Gesetz zur Reform des Wohngeldrechts und zur Änderung des Wohnraumförderungsgesetzes (WoGRefG) zum 1. Januar 2016 geändert. Die Wohngeldbehörden werden vom Ministerium für Finanzen und Wirtschaft angehalten, ausschließlich diese Vordrucke zu verwenden. Der vom Landesbeauftragten für Datenschutz zwischenzeitlich beanstandete Vordruck gehört nicht dazu.

Anfragen der Wohngeldbehörden und der Regierungspräsidien zum Vollzug des Wohngeldgesetzes bei der Überprüfung der Plausibilität der Einnahmen werden mit den oben dargestellten rechtlichen Hinweisen beantwortet. In den jährlich stattfindenden Dienstbesprechungen der Regierungspräsidien mit den Wohngeldbehörden, an denen das Ministerium für Finanzen und Wirtschaft stets vertreten ist, weist das Ministerium für Finanzen und Wirtschaft bei entsprechenden Anfragen zudem auf diese Rechtsauffassung hin.

8. Datenschutz an Schulen und Hochschulen

8.1 Verwaltungsvorschrift Datenschutz an öffentlichen Schulen

Die rasante technische digitale Entwicklung macht auch weiterhin vor den Schulen und der Schulverwaltung nicht Halt.

Das **Kultusministerium** hat deshalb ein Unterstützungssystem für die Schulen auf drei Säulen aufgebaut:

- dem Fortbildungsbereich,
- den Informationsplattformen zum Datenschutz und zum Urheberrecht,
- sowie der Einzelfallberatung, die durch die Regierungspräsidien und Staatlichen Schulämter wahrgenommen wird.

Die frühere Verwaltungsvorschrift von 2009 wurde 2015 aktualisiert und mit Inhalten aus der datenschutzrechtlichen schulischen Praxis ergänzt. Fragestellungen aus der Schulleiterfortbildung und Themen, die die Lehrerfortbildner einbrachten, wurden in die neue Verwaltungsvorschrift eingearbeitet. Beispielhaft seien die Themen Löschfristen, Veröffentlichung von Fotos, Filmen und anderen digitalen Medien sowie Videoüberwachung genannt. Das Kultusministerium teilt die Auffassung des Landesbeauftragten für den Datenschutz, dass es nun für die Schulen gilt, die zur Verfügung gestellten Hilfestellungen zu nutzen und konsequent umzusetzen.

8.2 Medienbildung im Bildungsplan 2016

Aus Sicht des **Kultusministeriums** wurde ein Fach Medienbildung aus folgenden Gründen nicht realisiert:

- Medienbildung betrifft alle Unterrichtsfächer, an vielen Stellen des Bildungsplanes lassen sich die Kompetenzbereiche der Medienbildung verankern. Hätte es ein Fach Medienbildung gegeben, würden sehr wahrscheinlich dort die entsprechenden Kompetenzbereiche verortet, eine thematisch sinnvolle Verankerung im Fächerkanon wäre so dann nicht gegeben.
- Die Leitperspektive Medienbildung ist ab Klasse 1 fächerintegrativ in die Bildungspläne integriert und wird so von Anfang an spiralcurricular aufgebaut. Je-

des Fach kann dann die für seinen Bereich wichtigen Kompetenzfelder der Medienbildung an einem Thema bearbeiten.

- Derzeit entwickelt das Landesmedienzentrum ein e-Portfolio, das den spiralcurricularen Aufbau von Klasse 1-12, insbesondere auch im Bereich des Datenschutzes, aufgreift. Dieses unterstützt die Lehrkräfte bei der Strukturierung der Inhalte. Die Schülerinnen und Schüler haben dadurch einen Nachweis ihrer erworbenen Kompetenzen. Hierzu wird eine enge Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz angestrebt.
- Der Basiskurs Medienbildung in Klasse 5 dient vor allem dazu, die unterschiedlichen Leistungsstände der ehemaligen Grundschulkinder im Arbeiten mit digitalen Medien auf ein gemeinsames Niveau zu stellen. Auch soll damit vermieden werden, dass alle Lehrkräfte die gleichen Themen parallel aufgreifen, sondern dass sie davon ausgehen können, dass diese zentral im Basiskurs besprochen wurden und sie so ihre fachlichen medienbildnerischen Schwerpunkte bearbeiten können. Auch zum Basiskurs hat das Landesmedienzentrum eine Reihe von Unterstützungsangeboten entwickelt.
- Von großer Bedeutung ist das Thema Medien auch in den anderen fünf Leitperspektiven. In allen Leitperspektiven sind Themen vorgesehen, die aus ihrer jeweiligen Sichtweise die Medien aufgreifen, wobei auch datenschutzrelevante Inhalte eine Rolle spielen.

Der aus Sicht der Leitperspektive Medienbildung berechtigte Hinweis auf die Aufnahme der Funktionsweisen und Rahmenbedingungen des Internets in die Bildungspläne wird im Aufbaukurs Informatik eine große Rolle spielen, für den noch ein Fachplan erstellt werden wird. Dabei werden auch die jetzigen Ausführungen des Landesbeauftragten für den Datenschutz mit einbezogen.

Die positive Aussage des Landesbeauftragten für den Datenschutz zu den Mediencurricula des Landesmedienzentrums belegt, wie wichtig es war, sich mit ihm ganz eng abzustimmen und seine wichtigen Anregungen aufzugreifen.

8.5 Erst Verfahrensverzeichnis, dann Betrieb

Das berichtete Verhalten einer Universität im Zusammenhang mit der Inbetriebnahme eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten ist zutreffend dargestellt. Die Universität verstieß damit, wie von ihr selbst eingeräumt wurde, gegen die

Pflicht zur Führung eines vollständigen Verfahrensverzeichnisses (§ 11 LDSG) und die in § 32 LDSG geregelte Meldepflicht. Die betreffende Universität hat gegenüber dem **Wissenschaftsministerium** dargelegt, dass sie ihre Verfahrensabläufe den datenschutzrechtlichen Anforderungen angepasst hat. Sie hat zugesichert, dass sie künftig alle erforderlichen Maßnahmen ergreifen wird, um die Anforderungen des Datenschutzes vollständig zu erfüllen. Konkret wurde für den Tätigkeitsbereich, in dem der Verstoß erfolgte, eine zusätzliche Stelle von 0,25 VZÄ für den Datenschutz zur Verfügung gestellt und besetzt.

Das Wissenschaftsministerium hat die betreffende Passage aus dem Tätigkeitsbericht des Landesbeauftragten für den Datenschutz an alle Landeshochschulen übermittelt und diese darauf hingewiesen, dass bereits bei erstmaliger Datenverarbeitung mit einem automatisierten Verfahren ein vollständiges Verfahrensverzeichnis nach § 11 Abs. 2 LDSG vorliegen muss und dass bei Verzicht auf die Bestellung eines behördlichen Datenschutzbeauftragten die Meldepflichten des § 32 LDSG zu beachten sind.

10. Datenschutz in der Wirtschaft

10.19 Intelligente Stromzähler

Grundsätzlich steht das **Umweltministerium** hinter einer breit angelegten Einführung von intelligenten Messsystemen und damit zu den Zielen des Gesetzesentwurfs der Bundesregierung zur Digitalisierung der Energiewende. Diese bestehen darin, im Interesse von Umwelt- und Klimaschutz durch den Einbau von intelligenten Messsystemen eine bessere Auslastung und Steuerung der Netze – hin zu intelligenten Netzen – zu erreichen. Weiter erhalten Letztverbraucher mittels intelligenter Messsysteme genaue Informationen über ihr Verbrauchsverhalten, was zu einem energiesparenden Verhalten führen kann. Schließlich ermöglichen erst intelligente Messsysteme die Umsetzung variabler Tarife, mit denen der Letztverbraucher wirtschaftliche Anreize zur Verbrauchsverlagerung erhält. Bürgerinnen und Bürger können damit aktiv die Energiewende vorantreiben. Prinzipiell sollte dabei gelten, dass die durch die intelligenten Messsysteme gewonnenen Daten zunächst in der Datenhoheit des jeweiligen Haushalts bleiben. Nur die Daten, die für die Energieversorgung, -verteilung und -abrechnung notwendig sind, sollten ausgelesen und übermittelt werden. Entsprechend hat sich die Landesregierung im Bundesrat dafür ausgesprochen, Letztverbrauchern mit einem Jahresstromverbrauch bis einschließlich 6.000 kWh eine Opt-Out-Variante zu ermöglichen, so dass sie die Einbindung ihres Messsystems in ein Kommunikationsnetz ablehnen können. Darüber hinaus hat sie sich auch dafür ausgesprochen, dass von Haushaltskunden mit über 6.000 kWh ebenfalls eine Zustimmung zur Ausstattung mit intelligenten Messsystemen vorliegen muss.

11. Technik und Medien

11.1.3 Videoüberwachung in öffentlichen Verkehrsmitteln

Das **Ministerium für Verkehr und Infrastruktur** bewertet die Rechtslage wie folgt:

Die Zulässigkeit einer Videoüberwachung durch nichtöffentliche Stellen richtet sich nach § 6b Bundesdatenschutzgesetz. Hiernach ist die Beobachtung öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen. Maßstab der Bewertung ist auf der einen Seite das informationelle Selbstbestimmungsrecht der Fahrgäste und Mitarbeiter als besondere Ausprägung des Persönlichkeitsrechts, auf der anderen Seite der Schutz des Eigentums oder der körperlichen Unversehrtheit. Dabei sind die Gesamtumstände jedes Einzelfalls maßgeblich. Soweit die Videoaufnahmen nicht auf einem Monitor übertragen, sondern aufgezeichnet werden sollen, ist eine diesbezügliche Abwägung mit den schutzwürdigen Interessen der Betroffenen erneut vorzunehmen.

In den Ausschreibungsverfahren des Landes für den schienengebundenen Nahverkehr (SPNV) wird lediglich die technische Ausrüstung der Fahrzeuge mit einer Videoüberwachungsanlage, die eine Aufzeichnung und Speicherung über einen gewissen Zeitraum ermöglicht, gefordert. Der konkrete Einsatz sowie der Zeitpunkt der Durchführung solcher Überwachungen liegen dagegen im Ermessen des Eisenbahnverkehrsunternehmens (EVU) als verantwortliche Stelle. Die Forderung des Landes nach der Ausrüstung mit einem Videoüberwachungssystem wird – entgegen der Darstellung im 32. Tätigkeitsbericht – nicht „pauschal“, „undifferenziert“ und „flächendeckend“ erhoben, sondern erfolgt in Abhängigkeit von dem jeweils der Ausschreibung zugrunde liegenden Verkehrsnetz und dessen Besonderheiten wie etwa dem einzusetzenden Fahrzeugmaterial. Insoweit gibt es hinsichtlich der Anforderungen an eine Überwachungstechnik netzabhängig durchaus Unterschiede.

Ist die Videoüberwachung – wie vorliegend – als reine Aufzeichnungslösung ausgestaltet (Black-Box-Lösung), so kann sie gemäß der „Orientierungshilfe Videoüberwachung in öffentlichen Verkehrsmitteln“ des Düsseldorfer Kreises vom 16. September 2015 dazu eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann oder Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z.B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist demnach stets zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Diese Aufgabe obliegt im SPNV in Baden-Württemberg den EVU.

Sämtliche Verkehrsbetriebe (EVU und Busbetreiber) haben mit Vandalismus und Sachbeschädigung zu kämpfen. Außerdem werden Straftaten gegenüber Fahrgästen verübt. Diese Fälle lassen sich in der Regel nicht einzelnen Ausschreibungsnetzen zuschreiben, sondern kommen flächendeckend mit einzelnen Schwerpunkten vor. Wegen der mangelnden Vorhersehbarkeit solcher Vorfälle erscheint aus Sicht des Ministeriums für Verkehr und Infrastruktur – entgegen der Auffassung des Landesbeauftragten für den Datenschutz – auch eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs verhältnismäßig. Die Videoüberwachung dient dazu, solche Taten aufzuklären, eine präventive Wirkung zu entfalten und den Fahrgästen mehr Sicherheit zu bieten. Um den datenschutzrechtlichen Bedenken und den schutzwürdigen Interessen der Betroffenen Rechnung zu tragen, werden die Videoaufzeichnungen in einer Blackbox gespeichert und nach 72 Stunden automatisch überschrieben. Ein Zugriff auf diese Aufnahmen ist neben der Polizei ausschließlich einzelnen (in der Regel nur eine Person im ganzen Unternehmen), besonders qualifizierten und geschulten Mitarbeitern der EVU und auch nur im Beisein der Polizei gestattet.

Nach einhelliger Aussage der in Baden-Württemberg tätigen EVU ist es der in den SPNV-Ausschreibungen enthaltenen Forderung nach der Ausstattung mit Videoüberwachungstechnik und deren Nutzung durch die EVU zu verdanken, dass sowohl die Anzahl der in und an den Fahrzeugen begangenen Sachbeschädigungen und der übrigen Vandalismusfälle als auch die Anzahl der in den Fahrzeugen begangenen sonstigen Delikte (etwa Körperverletzungen, Diebstähle etc.) seit Jahren stagniert bzw. rückläufig ist, wobei die Videoüberwachung zu einer außerordentlich hohen Aufklärungsquote begangener Straftaten beiträgt. Auch das subjektive Sicherheitsempfinden der Fahrgäste hat in den letzten Jahren parallel mit der Einführung der Videoüberwachungstechnik (unabhängig von einer tatsächlich durchgeführten Videoaufnahme) zugenommen, wie sich aus landesweit durchgeführten Qualitätsmessungen ableiten lässt.

Abschließend ist darauf hinzuweisen, dass dem Landesbeauftragten für den Datenschutz mit Schreiben vom 3. Juli 2015 ein Gesprächsangebot zum Thema Videoüberwachung im SPNV unterbreitet wurde, auf welches bis heute allerdings keine Reaktion erfolgt ist. Ein gemeinsames Gespräch im Vorfeld des 32. Tätigkeitsberichtes hätte möglicherweise zur Beseitigung bestehender Unklarheiten und Meinungsverschiedenheiten betragen können. Für die nun im 32. Tätigkeitsbericht erfolgte Ankündigung von Gesprächen ist das Ministerium für Verkehr und Infrastruktur offen.

11.1.5 Dashcams

Zur Frage der Videoaufzeichnung im Straßenverkehr durch Dashcams, d.h. private Kameras, die am Fahrzeug befestigt werden und während der Fahrt das Verkehrsgeschehen filmen, insbesondere um Fehlverhalten anderer Verkehrsteilnehmer dokumentieren zu können, gibt es bislang keine auf diese bezogene spezielle rechtliche Regelung.

Betroffen hiervon sind weniger die dem **Ministerium für Verkehr und Infrastruktur** zugeordneten Bereiche des öffentlichen Straßenverkehrsrechts wie die Straßenverkehrs-Ordnung, das Ordnungswidrigkeitenrecht, das Fahrerlaubnisrecht oder das Fahrzeug-Zulassungsrecht. Vorrangig geht es um datenschutzrechtliche Fragen, da das Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts das Recht am eigenen Bild umfasst.

Die Rechtsprechung zum Einsatz von Dashcams und der Verwertbarkeit hierdurch erlangter Daten im Gerichtsverfahren ist bisher aber uneinheitlich. So gibt es einzelne Urteile, die die Verwertbarkeit der Aufzeichnungen ablehnen, aber auch Rechtsprechung, die den gezielten, situationsgebundenen Einsatz von Dashcams zur Beweissicherung als gerechtfertigt ansieht. Die Diskussion hierzu ist bisher nicht abgeschlossen. Eingehend befasst mit diesen Fragen hat sich aktuell der 54. Deutsche Verkehrsgerichtstag vom 27. bis 29. Januar 2016 in Goslar, Arbeitskreis VI. Dort wurden folgende Empfehlungen beschlossen:

1. *Die Video-Aufzeichnung von Verkehrsvorgängen mithilfe von Dashcams kann einen Beitrag zur Aufklärung von Unfallhergängen und Straftaten leisten, aber auch zu einer erheblichen Beeinträchtigung von Persönlichkeitsrechten führen. Der Arbeitskreis beklagt, dass weder in Deutschland noch in den Nachbarländern eine klare Rechtslage zur Verwendung derartiger Kameras und zur Verwertung damit erzeugter Aufnahmen vor Gericht besteht.*

2. *Der Arbeitskreis empfiehlt daher eine gesetzliche Regelung, die auf der Basis des europäischen Datenschutzrechts möglichst ein einheitliches Schutzniveau innerhalb der EU gewährleistet.*

3. *Anstelle eines generellen Verbotes oder einer generellen Zulassung derartiger Aufzeichnungen ist ein sachgerechter Ausgleich zwischen Beweisinteresse und Persönlichkeitsrecht durch den Gesetzgeber geboten.*

4. *Dieser Ausgleich könnte darin bestehen, dass die Aufzeichnung mittels derartiger Geräte dann zulässig ist, wenn die Aufzeichnung anlassbezogen, insbesondere bei einem (drohenden) Unfall, erfolgt oder bei ausbleibendem Anlass kurzfristig überschrieben wird.*

5. *Die Verwertung von rechtswidrigen Dashcam-Aufnahmen im Gerichtsverfahren richtet sich nach den von der Rechtsprechung entwickelten Grundsätzen zu den Beweisverwertungsverboten.*

6. *Die Verfolgung von Verkehrsverstößen ohne schwerwiegende Gefährdung oder Folgen soll weiterhin nicht auf die Aufzeichnungen von Dashcams gestützt werden können.*

7. *Der Missbrauch von Aufzeichnungen mit personenbezogenen Daten, z.B. eine Veröffentlichung im Internet, sollte mit Sanktionen bedroht werden.*

Seitens der Datenschutz-Aufsichtsbehörden existiert bisher keine Stellungnahme zu Kameras, welche im sog. Loop-Verfahren ihre Aufnahmen ständig selbst überschreiben.

Beim **Regierungspräsidium Karlsruhe** wurden bisher 11 Fälle eines Dashcam-Einsatzes zur Anzeige gebracht. Anzuwenden ist nach Auffassung des Regierungspräsidiums Karlsruhe die allgemeine Vorschrift des § 6b Bundesdatenschutzgesetz zur Videoüberwachung, die eine anlasslose permanente Überwachung des Straßenverkehrs jedenfalls ausschließt. Das Regierungspräsidium Karlsruhe hat in Anbetracht der ungeklärten Rechtslage bisher nur in Fällen, in denen im Sinne der Rechtssicherheit davon ausgegangen werden konnte, dass die Betroffenen das Verbot des permanenten Einsatzes der Kamera jedenfalls kennen mussten und dennoch anlasslos Aufnahmen über einen längeren Zeitraum erstellt haben, Bußgelder verhängt. Bisher sind zwei Bußgeldbescheide wegen des Einsatzes einer Dashcam rechtskräftig geworden (Bußgelder in Höhe von jeweils 70 Euro bzw. 300 Euro).

11.1.6 Drohnen: Harmloses Spielzeug oder eine Gefahr für das Persönlichkeitsrecht?

Der Bericht beschreibt den aktuellen Boom im Bereich der Drohnen. Sowohl im gewerblichen als auch im privaten Bereich werden in den letzten Jahren immer mehr Drohnen eingesetzt. Diese sind häufig mit Kameras ausgestattet. Das Anfertigen von Foto- und Videoaufnahmen beim Überfliegen von eingezäunten und mit Blickschutz versehenen Grundstücken ist heute technisch ohne weiteres möglich. Folge dieser enormen technischen Fortschritte der letzten Jahre im Bereich der Drohnen ist eine Vielzahl luftrechtlicher und datenschutzrechtlicher Fragestellungen. Diese Entwicklung wird nach Auffassung des **Ministeriums für Verkehr und Infrastruktur** sehr gut und zutreffend beschrieben.

Ebenfalls zutreffend dargestellt ist die aktuelle Rechtslage zum Luftverkehr. Ergänzend ist darauf hinzuweisen, dass hierzu der Bund die ausschließliche Gesetzgebungskompetenz hat. Die Länder können daher grundsätzlich nur im Bereich des Gesetzesvollzugs regulierend eingreifen. In ihre Zuständigkeit fällt die Erteilung von Aufstiegserlaubnissen für zu gewerblichen Zwecken genutzte Drohnen. Um diesbezüglich möglichst einen bundeseinheitlichen Standard zu schaffen, haben der Bund und die Länder sich auf die „gemeinsamen Grundsätze des Bundes und der Länder für die Erteilung der Erlaubnis zum Aufstieg von unbemannten Luftfahrtsystemen“ geeinigt. In diesen Grundsätzen wird vom Antragsteller für eine Aufstiegserlaubnis die Abgabe einer Datenschutzerklärung gefordert. Diese hat in Baden-Württemberg folgenden Wortlaut: „*Hiermit erkläre ich, dass durch die beantragte Nutzung des Luftraums datenschutzrechtliche Bestimmungen nicht verletzt werden. Die beantragte Nutzung dient nicht der gezielten Beobachtung und/oder Aufzeichnung von Personen bzw. es liegt eine schriftliche Einwilligung der betroffenen Personen vor.*“ Durch das Erfordernis, diese Erklärung bei Beantragung der Aufstiegserlaubnis anzugeben, werden die Steuerer hinsichtlich der datenschutzrechtlichen Bestimmungen sensibilisiert.

Auf Grund der ausschließlichen Gesetzgebungskompetenz des Bundes im Luftrecht hat Baden-Württemberg im Moment keine weiteren Möglichkeiten, durch gesetzliche Regelungen den Drohnenaufstieg stärker zu regulieren. Zuständig für eine stärkere gesetzliche Regulierung des Drohnenaufstiegs sind der Bund und die EU. Auf beiden Ebenen gibt es im Moment Bestrebungen, die rechtlichen Rahmenbedingungen für den Aufstieg von Drohnen neu zu regeln.

11.8 E-Government-Gesetz Baden-Württemberg

Das **Innenministerium** hat den Landesbeauftragten für den Datenschutz in den Erstellungsprozess des E-Government-Gesetzes Baden-Württemberg (EGovG BW) frühzeitig und umfassend einbezogen, was dieser auch anerkennend würdigt. Das EGovG BW stellt wirksame und praktikable Regelungen zur Gewährleistung des Datenschutzes bereit. Ein hohes Niveau des Datenschutzes ist Grundvoraussetzung für ein erfolgreiches E-Government. Daneben sind aber auch praktische Nutzbarkeit der technischen Lösungen, die Akzeptanz bei den Bürgerinnen und Bürgern sowie eine möglichst einheitliche und aufwandsarme Umsetzung für die Verwaltung Erfolgsfaktoren.

Aus diesen Gründen wurde die vom Landesbeauftragten für den Datenschutz gewünschte Verpflichtung zur Zugangseröffnung für elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, nicht in das EGovG BW übernommen. Die Gesetzeslage unterscheidet sich damit inhaltlich nicht wesentlich von der des Bundesrechts. Denn die in § 2 Absatz 1 EGovG des Bundes normierte Zugangsöffnung für die entsprechend signierten elektronischen Dokumente ist in ihrer Wirkung nur beschränkt, da eine Überprüfungspflicht durch die Behörden für die qualifiziert elektronisch signierten Dokumente nicht angeordnet ist. Ein wirksamer Schriftformersatz ist damit für die Bürgerinnen und Bürger nicht möglich. Außerdem ist für die entsprechende Nutzung der Signatur noch der Erwerb eines kostenpflichtigen Zertifikats sowie eines entsprechenden Kartenlesers für die Bürgerinnen und Bürger erforderlich. Das Innenministerium betrachtet die qualifizierte elektronische Signatur sowohl aus diesen Gründen als auch im Hinblick auf die durch die europäische Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (VO (EU) Nr. 910/2014) anstehenden Veränderungen als keine vorzugswürdige technische Lösung zum Ersatz der Schriftform.

Aus ähnlichen Gründen ist auch keine Verpflichtung zum Empfang von verschlüsselt übertragenen elektronischen Dokumenten im EGovG BW enthalten. Eine solche Regelung hätte nach Auffassung des Innenministeriums den Datenschutz in der Praxis nicht wesentlich verbessert. Denn Verschlüsselungslösungen gewährleisten zwar einen hohen Schutz, die

Vielzahl an Verschlüsselungsprogrammen sowie deren unterschiedliche Handhabung würden bei den Behörden, Bürgern und Unternehmen jedoch erheblich höhere zeitliche, personelle, technische und finanzielle Aufwände erforderlich machen und sie vor technische Herausforderungen stellen. Dies hätte nur durch die Festlegung einer spezifischen technischen Lösung vermieden werden können, die allerdings, wie das Beispiel der qualifizierten elektronischen Signatur zeigt, im Hinblick auf die rasche technische Entwicklung in diesem Bereich keine zufriedenstellenden Ergebnisse liefern dürfte. Es wurde deshalb – angelehnt an die entsprechenden, ebenfalls technikoffenen Regelungen des Landesdatenschutzgesetzes – eine technikoffene Regelung getroffen. Mit dem Dienstleistungsportal des Landes „service-bw“ steht zugleich eine technische Infrastruktur zur Verfügung, um rasch und flächendeckend für die Bürgerinnen und Bürger sowie die Behörden die sichere Kommunikation möglichst einfach zu ermöglichen. Mit der im EGovG BW zudem verankerten Hinweispflicht auf das gesicherte Verfahren wird ein weiterer Beitrag zu einer hohen Nutzung der entsprechenden technischen Verfahrenslösungen geleistet.

Die vom Landesbeauftragten für den Datenschutz geäußerten Bedenken gegen den in der Gesetzesbegründung zu § 2 Absatz 2 Satz 2 EGovG BW als möglich beschriebenen Verzicht auf die gesicherte Kommunikation durch eine ausdrückliche Einwilligung sind aus Sicht des Innenministeriums nicht begründet. Gerade durch den Hinweis auf die ausdrückliche Einwilligung werden diese Fragen geklärt. Denn bei der Einholung einer ordnungsgemäßen ausdrücklichen Einwilligung ist nicht nur die Erklärung als solche, sondern auch der Umfang der Einwilligung explizit abzufragen. Dies kann beispielsweise durch entsprechende Webformulare geschehen. Es ist richtig, dass eine Einwilligung nicht zu Lasten Dritter erfolgen kann. Dies gilt auch für die aufgrund gesetzlicher Verpflichtungen nicht disponiblen Schutzmaßnahmen. Den Behörden sind diese zusätzlichen gesetzlichen Pflichten bekannt, Umsetzungsschwierigkeiten in breitem Maße sind damit nicht zu erwarten.

Das Innenministerium wird auch die vom Landesbeauftragten für den Datenschutz angesprochenen Themen im Rahmen der Evaluierung des Gesetzes ins Blickfeld nehmen. Sofern sich dann Anzeichen für Anpassungsbedarf ergeben, können diese offen und umfassend diskutiert werden.

11.9 Die Evaluierung des Rundfunkbeitragsstaatsvertrags

Das **Staatsministerium** teilt weder die datenschutzrechtlichen Bedenken des Landesbeauftragten für den Datenschutz gegenüber dem geplanten Meldedatenabgleich im Rundfunkbeitragsstaatsvertrag, noch kann das Staatsministerium eine unzureichende Beteiligung des Landesbeauftragten für den Datenschutz im Rahmen der Erarbeitung des 19. Rundfunkänderungsstaatsvertrags, mit dem u.a. die Änderungen am Rundfunkbeitragsstaatsvertrag umgesetzt werden, erkennen.

Die Rundfunkstaatsverträge bilden ein einheitliches Rahmenrecht für den Bereich des Rundfunks im Gesetzgebungszuständigkeitsbereich der Länder. Änderungen an diesem Rahmenrecht werden daher von allen Ländern gemeinsam erarbeitet. Im Rahmen der Evaluierung des Rundfunkbeitragsstaatsvertrags wurden die Datenschutzbeauftragten der Länder frühzeitig eingebunden.

Bereits am 25. Oktober 2014 fand ein gesonderter Termin der Länder mit den Datenschutzbeauftragten der Länder statt, in dem erstmals die Frage eines weiteren vollständigen Meldedatenabgleichs erörtert wurde. Im Rahmen der förmlichen Anhörung zu den geplanten Änderungen am Rundfunkbeitragsstaatsvertrag folgte im Juli 2015 eine vierwöchige öffentliche Online-Anhörung, in deren Rahmen die geplanten Änderungen auf der Webseite der Staatskanzlei Rheinland-Pfalz als des für den Bereich der Rundfunkpolitik federführenden Bundeslandes veröffentlicht wurden und allen Betroffenen und Interessierten Gelegenheit zur Stellungnahme gegeben wurde. Abschließend fand am 5. August 2015 eine mündliche Anhörung statt, zu der auch die Datenschutzbeauftragten der Länder über den Berliner Datenschutzbeauftragten in seiner Funktion als Vorsitzender der AG Rundfunk der Datenschutzbeauftragten der Länder eingeladen wurden. Wenn – wie hier – 16 Landesbehörden betroffen sind, ist es unter dem Gesichtspunkt der Verfahrensvereinfachung üblich, zentral die für das betreffende Thema federführende Stelle anzuschreiben. Der Vorsitzende der AG war hier entsprechend gehalten, die erhaltene Information/ Einladung an seine Kolleginnen und Kollegen weiterzugeben und ggf. eine etwaige gemeinsame Stellungnahme in seinem Kreis abzustimmen.

In diesem Zusammenhang erhielt auch der baden-württembergische Datenschutzbeauftragte im August 2015 Kenntnis von den geplanten Änderungen am Rundfunkbeitragsstaatsvertrag. Darüber hinaus wurde der Landesbeauftragte für den Datenschutz vorsorglich auch unmittelbar vom Staatsministerium auf den Anhörungstermin hingewiesen. Dementsprechend war es dem Landesbeauftragten für den Datenschutz spätestens seit August 2015 und damit weit vor der Freigabe zur Durchführung des Vorunterrichtungsverfahrens in den Landtagen und der Unterzeichnung des Staatsvertrags durch die Regierungschefinnen und -chefs im Oktober bzw. im Dezember 2015 möglich, sich mit einer eigenen Stellungnahme in das Verfahren einzubringen. Im Rahmen der im November 2015 erfolgten Erarbeitung des landesinternen Gesetzes zur Umsetzung des Staatsvertrags in Landesrecht wurde der Landesbeauftragte für den Datenschutz erneut gemäß der Verwaltungsvorschrift Regelungen förmlich angehört.

Ungeachtet dessen gab der Berliner Beauftragte für den Datenschutz in seiner Funktion als Vorsitzender der AG Rundfunk der Datenschutzbeauftragten der Länder in der Anhörung im August 2015 eine schriftlich ausformulierte und nach seinen Angaben im Kreis der Datenschutzbeauftragten abgestimmte Erklärung ab, in der die Einführung eines weiteren Meldedatenabgleichs abgelehnt wurde.

Die Position der Datenschutzbeauftragten der Länder und des Landesbeauftragten für den Datenschutz war damit bekannt und wurde im weiteren Verfahren auch intensiv von den Ländern erörtert. Hierbei gelangten die Länder allerdings zu einer anderen rechtlichen Beurteilung als die Landesdatenschutzbeauftragten. Die Länder stützten sich dabei u.a. auch auf die vom Landesbeauftragten für den Datenschutz zitierte Entscheidung des Bayerischen Verfassungsgerichtshofs zum „einmaligen“ Meldedatenabgleich vom 15. Mai 2014 (Vf. 8-VII-12 und Vf. 24-VII-12). Das Gericht kommt darin zu dem Ergebnis, dass der Gesetzgeber den Gemeinwohlbelang, die Beitragsehrlichkeit durch Kontrollmöglichkeiten zu ergänzen, höher gewichten dürfe als die Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung (vgl. Rz. 164 des Urteils). Die Beeinträchtigung für die Betroffenen sei gering, da im Regelfall Daten von Beitragsschuldnern übermittelt würden, die bereits als Rundfunkteilnehmer erfasst seien. Durch die Übermittlung solcher Daten erfahre die jeweilige Landesrundfunkanstalt aber nichts wesentlich Neues. Soweit Beitragsschuldner dagegen ihrer Anzeigepflicht noch nicht nachgekommen seien, verdiene ihr Interesse, ihre Daten nicht offenbaren und den Rundfunkbeitrag nicht zahlen zu müssen, keinen Schutz. Sie sollten gerade im Interesse einer gleichmäßigen Beitragserhebung ermittelt werden. Seien schließlich Personen vom Meldedatenabgleich betroffen, die nicht der Beitragspflicht unterlägen oder später nicht als Beitragsschuldner herangezogen würden, so habe der Eingriff ihnen gegenüber geringes Gewicht. Die zu übermittelnden Daten beschränkten sich auf Informationen zur Identifizierung einer Person und ihrer Zuordnung zu einer bestimmten Wohnung und ließen keinen tieferen Einblick in die Privatsphäre zu. Die

Daten seien zudem durch eine strikte Zweckbindung und strenge Löschungspflichten hinreichend abgesichert (vgl. Rz. 165 des Urteils).

Aus Sicht des Staatsministeriums können die vom Bayerischen Verfassungsgerichtshof zugunsten des „einmaligen" Meldedatenabgleichs ins Feld geführten Argumente auf den nun geregelten weiteren Meldedatenabgleich übertragen werden, zumal das Gericht an keiner Stelle seiner Entscheidung die Rechtmäßigkeit des Meldedatenabgleichs allein an die Voraussetzung der Einmaligkeit knüpft. Dabei ist auch zu berücksichtigen, dass die Länder mit dem Staatsvertrag gleichzeitig den Ankauf von Adressdaten als alternatives Instrument zur Datenerhebung gesetzlich bis zum 31. Dezember 2020 ausgesetzt haben. Würde man, wie vom Datenschutzbeauftragten intendiert, auf beide Instrumente der Datenerhebung verzichten, wäre das Ziel der Beitragsgerechtigkeit hingegen kaum zu erreichen.

Das für das Meldewesen zuständige **Innenministerium** hatte aufgrund des fortgeschrittenen Gesetzgebungsverfahrens seine datenschutzrechtlichen Bedenken gegen eine erneute Bestandsdatenlieferung zurückgestellt. Die Mitzeichnung in der Vorunterrichtung des Landtags durch das Staatsministerium zu dem Entwurf des Neunzehnten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge (19. RÄStV) vom 9.November 2015 ist daher aber durch das Innenministerium nur unter der Maßgabe erfolgt,

„ (…) *dass im Zuge der in zwei Jahren anstehenden Evaluierung melde- und datenschutzrechtlich weniger einschneidende Maßnahmen zum Datenabgleich geprüft werden. Dabei sollten im Sinne von Datensparsamkeit nach Möglichkeit Alternativen zum Zuge kommen, die einen erneuten vollständigen Meldedatenabgleich entbehrlich machen"*.

Anlage 2

Vorschlag für eine Beschlussempfehlung

Der Landtag wolle beschließen,

von der Mitteilung des Landesbeauftragten für den Datenschutz vom 21. Januar 2016 – Drucksache 15/7990 – und der vom Innenministerium hierzu mit Schreiben vom 27. April 2016 vorgelegten Stellungnahme der Landesregierung (siehe Anlage 1 zum Ausschussbericht) Kenntnis zu nehmen.