



Baden-Württemberg

MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

Stellungnahme der Landesregierung

zum

34. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Baden-Württemberg (LT-Drs. 16/5000)

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 und die Informationsfreiheit (LfDI) 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 LfDI 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. Schwerpunkte

1.7 G20-Gipfel 2017

Zuverlässigkeitsüberprüfungen sind angesichts der heutigen Bedrohungslage und des besonderen Gefährdungspotentials von Großveranstaltungen, zu denen unzweifelhaft auch der G20-Gipfel zählte, unerlässlich. Mit seinem Bericht hat der LfDI zwar Mängel benannt, die aus seiner Sicht bei der Praxis polizeilicher Datenspeicherungen oder der fehlenden Dokumentation der Entscheidungsgründe durch Polizei und Verfassungsschutz bestehen. Allerdings hat sich gerade nicht der Vorwurf bestätigt, dass den Journalisten zu Unrecht die Akkreditierung entzogen worden wäre.

In das Landesverfassungsschutzgesetz (LVSG) wurde im Dezember 2017 eine Rechtsgrundlage für die Mitwirkung des Landesamtes für Verfassungsschutz bei Zuverlässigkeitsüberprüfungen im Rahmen von Großveranstaltungen aufgenommen (vgl. § 3 Absatz 3 Satz 1 Nr. 11 LVSG). Damit soll gerade in Fällen wie den hier in Rede stehenden für mehr Rechtssicherheit gesorgt werden.

Bezüglich der Speicherung bestimmter Daten der Betroffenen in den polizeilichen Dateien hat der LfDI keine durchgreifenden datenschutzrechtlichen Bedenken vorgebracht. Er bemängelt lediglich die unvollständige Dokumentation von Speichervoraussetzungen, etwa bei der Prognose zur Wiederholungsgefahr oder bei der für die Speicherung in der Verbunddatei des Bundes und der Länder erforderlichen länderübergreifenden Bedeutung einer Straftat.

Soweit an der Dokumentation Kritik geäußert wurde, wird das Innenministerium im Zuge der anstehenden Novellierung des Polizeigesetzes und der laufenden Verbesserungen der technischen Systeme die Speicherpraxis selbstkritisch überprüfen und eventuell erforderliche Anpassungen vornehmen.

1.9 Technisch-organisatorische Maßnahmen

Die aktuell in Umsetzung befindlichen, vom Innenministerium gesteuerten Projekte im Bereich der Informationssicherheit decken sich in hohem Maße mit den im Tätigkeitsbericht 2018 des LfDI benannten Anforderungen, die die Datenschutz-Grundverordnung in Form von „technisch-organisatorischen Maßnahmen“ an die Informationssicherheit stellt.

Dies betrifft beispielsweise die flächendeckende Anwendung der Standards des Bundesamts für Sicherheit in der Informationstechnik (IT-Grundschutz) in allen Ressorts der Landesverwaltung ebenso wie die durchgängige Verschlüsselung des Landesverwaltungsnetzes oder die aktuelle Konzipierung und Durchführung von zielgruppengerechten Schulungs- und Sensibilisierungsveranstaltungen für alle Mitarbeiterinnen und Mitarbeiter der Landesverwaltung.

1.12 Die telemedizinische Sprechstunde DocDirekt – Modellversuch „im Ländle“ als Vorbild fürs ganze Land?

Im Rahmen der Strategie Digitalisierung in Medizin und Pflege fördert das Ministerium für Soziales und Integration das Modellprojekt der Kassenärztlichen Vereinigung Baden-Württemberg (KVBW) „DocDirekt“ mit 100.000 Euro, nicht – wie im Tätigkeitsbericht ausgeführt – mit rund 1 Million Euro. Mit diesem telemedizinischen Pilotprojekt soll eine schnelle und unkomplizierte telemedizinische Fernberatung und Fernbehandlung ähnlich dem Schweizer Modell „Medgate“ erprobt werden. DocDirekt ging im April 2018 an den Start und stand zunächst den gesetzlich Versicherten in der Landeshauptstadt Stuttgart und im Landkreis Tuttlingen zur Verfügung. Seit dem 1. Oktober 2018 ist das Projekt landesweit verfügbar.

Im 34. Tätigkeitsbericht werden verschiedene Aspekte des Projekts kritisch gesehen. Zum einen habe das Projekt „DocDirekt“ zwei Datenschutzerklärungen. Die erste Datenschutzerklärung gelte nur für die Website www.docdirekt.de. Eine weitere Website, die eine abweichende IP-Adresse verwendet und zum Adressbereich der Fa. Cloudflare, Inc.

mit Hauptsitz in San Francisco gehört, verfüge über eine weitere Datenschutzerklärung. Hierüber werde die Nutzerin bzw. der Nutzer nicht direkt aufgeklärt. Darüber hinaus sei auch bei der Nutzung der Smartphone-App die Verwendung von Tracking- und Analysemodulen festzustellen. Der LfDI verweist daher auf den Nachbesserungsbedarf des Modellvorhabens.

Im Rahmen der Projektförderung durch das Ministerium für Soziales und Integration sind sämtliche Projektverantwortliche – ebenso die KVBW – auf die Einhaltung der datenschutzrechtlichen Vorgaben hingewiesen worden. Die Einhaltung dieser Vorgaben obliegt dem jeweiligen Projektträger. Die KVBW steht nach Kenntnis des Ministeriums für Soziales und Integration bereits seit Projektbeginn in engem Austausch mit dem LfDI.

Des Weiteren fehlt es nach Ansicht des LfDI an einer Rechtsgrundlage für die Datenerhebung. Gegenwärtig gebe es keine gesetzliche Ermächtigungsgrundlage aus dem Aufgabenkatalog des § 285 SGB V. Auf eine Einwilligung könne sich die KVBW als Körperschaft des öffentlichen Rechts nicht stützen.

Im Rahmen des von der KVBW angebotenen Services nimmt eine bei der KVBW angestellte Medizinisch-technische Assistentin (MTA) bzw. ein Medizinisch-technischer Assistent den Telefon-, Chat- oder Video-Anruf der bzw. des Versicherten entgegen und fragt zunächst das Beschwerdebild ab. Die KVBW selbst verarbeitet in dem Moment, in dem die KVBW-zugehörigen MTA das Beschwerdebild des Versicherten am Telefon aufnehmen und schriftlich erfassen, Sozialdaten der bzw. des Versicherten, die oftmals auch gleichzeitig Gesundheitsdaten sind. Bei diesen Kategorien handelt es sich jeweils um besonders sensible Daten, denen der deutsche sowie der europäische Gesetzgeber jeweils ein besonders hohes Schutzniveau zugeordnet hat. An die Verarbeitung von Gesundheitsdaten und deren Schutz werden dementsprechend hohe Ansprüche gestellt. Die Versicherten stimmen im Vorhinein einer Verarbeitung der Daten zu.

Um der geschilderten Rechtsunsicherheit abzuwehren und die Zweifel des LfDI zu beseitigen, hatte das Ministerium für Soziales und Integration im Rahmen des Gesetzgebungsverfahrens zum Terminservice- und Versorgungsgesetz einen mit dem LfDI abgestimmten Antrag eingebracht, der im Bundesrat im November 2018 auch eine Mehrheit fand.

Die Bundesregierung lehnte die Schaffung einer gesetzlichen Regelung jedoch ab. Nach Ansicht des Bundes bedürfe es keiner Gesetzesänderung. Die Verarbeitung personenbezogener Daten für Zwecke der unmittelbaren medizinischen Versorgung der Versicherten

im Rahmen des Behandlungsvertrages durch Ärztinnen und Ärzte – auch für mobile und telemedizinische Versorgungsangebote – sei auf der Grundlage der bestehenden Regelungen der Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes und des SGB V bereits zulässig, weshalb es keiner gesonderten Einwilligung hierfür bedürfe.

Bei einem persönlichen Gespräch mit Herrn Bundesminister Spahn hat Herr Minister Lucha diese Problematik nochmals thematisiert. Ziel war es, die Bundesebene zu sensibilisieren und das Anliegen erneut zu prüfen. Da Herr Bundesminister Spahn eine Gesetzesänderung abgelehnt hat, hat das Ministerium für Soziales und Integration von der Stellung eines identischen Antrags im Rahmen des Bundesratsverfahrens zum Gesetz für mehr Sicherheit in der Arzneimittelversorgung wegen fehlender Erfolgsaussichten abgesehen.

2. Polizei und Kommunen

2.1 Kontrolle der Vergabe des ermittlungsunterstützenden Hinweises „HWA0“

Aus der Überprüfung zur Vergabepraxis des ermittlungsunterstützenden Hinweises „wechselt häufig Aufenthaltsort (HWA0)“ haben sich keinerlei Anhaltspunkte ergeben, dass eine zielgerichtete Speicherung bestimmter Volksgruppen durch die Polizei Baden-Württemberg vorgenommen wird. Der LfDI weist in seinem Tätigkeitsbericht ausdrücklich auf diese Tatsache hin.

Allerdings wird die Speicherpraxis innerhalb des polizeilichen Auskunftssystems POLAS in anderen Punkten kritisiert. Hierzu ist vorzuschicken: Aufgrund enger Auswahlkriterien wurden bei der Prüfung durch den LfDI viele atypische Fälle erfasst. So bezog sich der Adressatenkreis ausschließlich auf Personen, die als Ersttäter mit dem Hinweis HWA0 gespeichert waren. Weiteres Kriterium war eine Speicherung von mindestens fünf Jahren in POLAS BW. Die 49 Überprüfungsfälle spiegeln daher keinesfalls die tatsächliche Datenqualität innerhalb POLAS BW wider.

Das Innenministerium erkennt die aufgezeigten Mängel jedoch grundsätzlich an. Die Bereinigung bzw. Löschung der gerügten Datensätze innerhalb POLAS BW war demnach zu veranlassen. Die Prognose „Wiederholungsgefahr“ bedarf einer Einzelfallentscheidung, die mit nachvollziehbar begründeten Tatsachen zu belegen ist. Innerhalb der Einzelfallbegründung sollten Katalogbegriffe nur dann verwendet werden, wenn sich Erkenntnisse aus der Akte belegen lassen und entsprechend dokumentiert werden. Das Innenministerium

wird gemeinsam mit dem Landeskriminalamt Baden-Württemberg die Bemühungen um die Datenqualität und Sensibilisierung der Sachbearbeiterinnen und Sachbearbeiter fortführen.

Des Weiteren trägt der LfDI vor, dass bei einer Vielzahl an Vorgängen die POLAS-Speicherfristen bereits abgelaufen waren. Dies wird mit der Vergabe von zu langen Speicherfristen begründet. Teilweise wurde bei der Kontrolle des LfDI festgestellt, dass festgesetzte Speicherfristen nicht beachtet wurden. Diese Thematik wurde bereits aufgegriffen. Die überarbeitete Fassung des Handbuches Bereinigung INPOL-Version 8.0 vom 6. November 2018 enthält Neuregelungen, die sich unmittelbar auf das praktizierte Lösungsverfahren innerhalb POLAS BW auswirken und an einigen Stellen bereits eine unmittelbare Veränderung des Speicherbestandes bewirkt haben. Gleiches gilt für zukünftige Speicherungen. Die neu eingeführte Version unterstützt nunmehr die automatische Überwachung und Bearbeitung fristgebundener Abläufe im Änderungsdienst. Dadurch konnte eine erhebliche Qualitätsverbesserung erzielt werden.

Kritisch betrachtet wird von Seiten des LfDI ferner die praktizierte Verfahrensweise zur Erfassung von Vorgängen in der Verbunddatei „Kriminalaktennachweis“ (KAN). In den beiden von Seiten des LfDI aufgeführten Fällen ist festzustellen, dass es sich bei den Grunddelikten (Hausfriedensbruch sowie Diebstahl) um Delikte handelt, die gemäß § 38 PolG in Verbindung mit § 5 Absatz 3 DVO PolG als „Fälle von geringer Bedeutung“ grundsätzlich auch eine Überprüfungsfrist von drei Jahren haben könnten. Im ersten Fall bejahte der Sachbearbeiter aber Bezüge in ein anderes Land und im zweiten Fall die gewerbsmäßige Begehung. Die Einstufung, ob eine Straftat unter Berücksichtigung der „Rahmenrichtlinien für den Kriminalaktennachweis“ (RL-KAN) überregional bedeutsam ist, nimmt der Sachbearbeiter beim Erfassen einer Straftat vor. Bejaht der Sachbearbeiter ein KAN-Kriterium, richtet sich die Überprüfungsfrist auch landesrechtlich nicht mehr nach § 38 PolG in Verbindung mit § 5 Absatz 3 DVO PolG, sondern nach § 38 PolG in Verbindung mit § 5 Absatz 2 Nummer 3 DVO PolG (überregional bedeutsame Straftat, insbesondere gewerbsmäßige Begehung) und beträgt folglich bei Erwachsenen 10 Jahre.

2.2. Gebrochene Zusage

Im vorliegenden Fall handelt es sich um einen Auskunfts- und Lösungsantrag einer sog. „Umweltaktivistin“ beim Landeskriminalamt Baden-Württemberg (LKA) vom 20. Januar 2015, die sich auch an den LfDI gewandt hat. Wie vom LfDI vorgetragen, wird die Petentin seit fast 20 Jahren in regelmäßigen Abständen wiederkehrend in den polizeilichen Dateien

mit szenetypischen Straftaten gespeichert. Bei diesen handelt es sich zwar überwiegend um Fälle mit geringer Bedeutung im Sinne von § 38 Absatz 2 PolG in Verbindung mit § 5 Absatz 3 DVO PolG, für die in einer Einzelbetrachtung eine verkürzte Überprüfungsfrist gelten würde. Die Straftaten wurden jedoch gewohnheitsmäßig und überregional begangen, weshalb sie vorliegend nicht als Fälle von geringer Bedeutung einzustufen sind (vgl. § 5 Absatz 4 DVO PolG).

Konkret hat das LKA dem LfDI mit Schreiben vom 23. Januar 2017 mitgeteilt, dass die Überprüfung der Löschung der zur Petentin in POLAS BW gespeicherten Daten und die Vernichtung der Unterlagen – soweit keine neuen Erkenntnisse gespeichert werden müssen – zum 31. Juli 2017 vorgesehen ist. Bei dieser Formulierung handelte es sich um die Mitteilung des Aussonderungsprüfdatums im Bestand von POLAS BW und um keine verbindliche Aussage zur tatsächlichen Löschung. Jeweils vier Monate vor Erreichen des maßgeblichen Aussonderungsprüfdatums werden Datensätze auf einer Prüfliste an die datenbesitzende Dienststelle ausgegeben, damit diese prüfen kann, ob eine Verlängerung der Speicherdauer in Betracht kommt. Neue Straftaten sowie eine Speicherung im Bundesbestand können sich gemäß § 38 Absatz 5 Satz 2 PolG auf die Speicherdauer im Landesbestand POLAS BW auswirken. Die Aussage, dass die Daten zur Löschung anstehen, war daher ausdrücklich an die Bedingung geknüpft, dass keine weiteren Erkenntnisse hinzukommen, also weder eine Neuspeicherung in POLAS BW noch eine relevante Speicherung in den Verbunddateien – wie vorliegend.

Bei einem erneuten Auskunftsantrag der Petentin gegenüber dem LKA wurde mit Schreiben vom 7. Dezember 2017 mitgeteilt, dass „auf Grund des Bundesbestandes die Daten voraussichtlich am 12.03.2023 gelöscht werden“. Ausschlaggebend für die Verlängerung der ursprünglichen Speicherfrist war ein Ermittlungsverfahren gegen die Petentin in Bayern, welches in INPOL gespeichert war.

Nach erneuter Kontaktaufnahme des LfDI mit dem LKA unter Verweis auf das ursprünglich übermittelte Datum (31. Juli 2017) erfolgte wiederum eine intensive Prüfung der Rechtslage im Hinblick auf den ausgelösten „Mitzieheffekt“ des Ermittlungsverfahrens in Bayern. Gleichfalls wurde unmittelbar nach Bekanntwerden der Fristenübernahme Kontakt zu den zuständigen Polizeipräsidien als Datenbesitzer aufgenommen, verbunden mit dem Prüfungsauftrag einer etwaigen Löschung der gespeicherten Datenbestände der Petentin in POLAS BW. Der LfDI wurde darüber schriftlich in Kenntnis gesetzt. Lediglich aufgrund des entstandenen Missverständnisses bezüglich der Löschung wurden die Daten im vorliegenden Fall ausnahmsweise ohne rechtliche Notwendigkeit gelöscht.

Der „Mitzieheffekt“ ist seit dem Jahr 2012 gesetzlich in § 38 Absatz 5 Satz 2 PolG geregelt. Die Intention des Gesetzgebers bei der Einführung dieser Regelung war, die kriminelle Karriere eines Straftäters innerhalb der polizeilichen Informationssysteme abzubilden (vgl. LT-Drucks. 15/2434, Seite 35). Davon ausgenommen werden sollte auch nicht die sog. „Kleinstkriminalität“, insbesondere wenn diese gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen wird.

Für die Polizei Baden-Württemberg ist es von besonderem Interesse, dass die kriminelle Karriere einer Person innerhalb der polizeilichen Auskunftssysteme umfassend abgebildet wird. Eine historische Betrachtung, die Rückschlüsse auf das zukünftige Folgeverhalten zulässt, ist bedeutsam, insbesondere wenn die Person aufgrund ihres Wohnsitzes oder ihres privaten und beruflichen Umfeldes einen festen Bezug zu Baden-Württemberg hat.

Das Innenministerium ist der Auffassung, dass der Mitzieheffekt des § 38 Absatz 5 Satz 2 PolG grundsätzlich auch bei Daten, die aus anderen Bundesländern in INPOL gespeichert wurden, Anwendung finden kann. Der Vorwurf einer „gebrochenen“ Zusage entbehrt vor diesem Hintergrund jeder Grundlage: Weder gab es eine (Lösch-)Zusage, noch hat sich die Polizei bei der Anwendung des Mitzieheffekts in irgendeiner Hinsicht kritikwürdig verhalten.

2.3 Datenschutz bei der Waffenbehörde

Antragsteller war ein Bewachungsunternehmen, das bei der Waffenbehörde einen Antrag nach § 28 Absatz 3 WaffG auf Erteilung einer Waffentrageberechtigung für den Betroffenen gestellt hat. Im Rahmen der Antragstellung hatte das Unternehmen darauf hingewiesen, dass es sich mit dem Betroffenen in einem Arbeitsrechtsstreit befindet, in dem dieser erreichen möchte, wieder im Bereich des bewaffneten Geld- und Werttransports beschäftigt zu werden. Aufgrund einer länger andauernden Arbeitsunfähigkeit ging das Bewachungsunternehmen aber von einer psychischen Erkrankung bei dem Betroffenen aus und äußerte Zweifel an seiner waffenrechtlichen Eignung. Bewachungsunternehmer dürfen im Rahmen einer solchen Antragstellung mögliche Zweifel an der persönlichen Eignung des Wachpersonals nicht verschweigen. Die Bitte der Waffenbehörde, die im Rahmen der Antragstellung gemachten Angaben durch das Bewachungsunternehmen zu belegen, um dessen Einschätzung verifizieren und auf ihre waffenrechtliche Relevanz hin überprüfen zu können, geschah grundsätzlich auch im Interesse des Betroffenen. Die Einholung der Daten beim Antragsteller anstelle des Betroffenen stellt in der Tat einen Verstoß gegen

den Grundsatz der Direkterhebung nach § 13 Absatz 2 LDSG in der damals geltenden Fassung dar.

Der Landrat hat das Fehlverhalten eingeräumt und die betroffenen Mitarbeiter zur zukünftigen Beachtung des Datenschutzes angewiesen. Zudem sollen die Schulungsaktivitäten in der betreffenden Behörde verstärkt werden. Darüber hinaus sind keinerlei ähnliche oder andere datenschutzrechtlich relevante Fälle bekannt geworden, auch der vorliegende Fall ist dem Innenministerium erst im Rahmen des Datenschutzberichts bekannt geworden. Es handelt sich um einen abgeschlossenen Einzelfall. Weitere Maßnahmen, wie eine generelle Sensibilisierung der Waffenbehörden im Land, erscheinen daher nicht erforderlich.

2.4 Datenschutz und Bauleitplanung

Die Ausführungen sind aus Sicht des Wirtschaftsministeriums zutreffend und entsprechen der Abstimmung.

2.5 Online-Prüfung von baden-württembergischen Behörden-Websites

Seitens des LfDI wird festgestellt, dass die Zahl der verschlüsselt betriebenen Behörden-Websites in den letzten Jahren kontinuierlich angestiegen ist. Der ermittelte Anteil von verschlüsselt betriebenen Behörden-Websites mit 19 vom Hundert wird jedoch als zu gering erachtet.

Bei der Erhebung dieser Daten durch den LfDI wurden Webauftritte aller Verwaltungsebenen untersucht, in hohem Maße auch aus dem kommunalen Umfeld. Durch aktuell in der Umsetzung befindliche Projekte ist der Anteil der verschlüsselt betriebenen Websites in der Landesverwaltung bereits angestiegen und übersteigt die vom LfDI für alle Behörden ermittelte Quote erheblich. Ein weiterer Ausbau der IT-Sicherheitsmaßnahmen für Websites und Webportale und damit der verschlüsselt betriebenen Internetauftritte erfolgt 2019.

5. Justiz und Recht

5.1 Umsetzung der Richtlinie (EU) 2016/680 im Justizbereich

5.1.1...durch Schaffung eines Landesdatenschutzgesetzes für Justiz- und Bußgeldbehörden

Das federführende Justizministerium hatte dem LfDI bereits vor Durchführung einer förmlichen Anhörung Gelegenheit gegeben, sich zu dem Referentenentwurf für ein Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 für den Geschäftsbereich des Justizministeriums zu äußern. In dieser frühen Arbeitsphase, in der Regelungsentwürfe naturgemäß noch umfangreich inhaltlich überarbeitet werden, hatte sich der LfDI kritisch zu der Rechtsgrundlage für die Videoüberwachung von Vorführbereichen in Gerichtsgebäuden geäußert. Obwohl die vom LfDI geforderte Güterabwägung zu diesem Zeitpunkt bereits durch die Ausgestaltung der Vorschrift als gebotene Ermessensausübung im ersten Referentenentwurf enthalten war, erfuhr sie anschließend zudem eine ausdrückliche Normierung im Gesetzentwurf.

Seine grundsätzlichen Bedenken hinsichtlich des öffentlichen Vorführbereichs in Gerichtsgebäuden, in dem die Möglichkeit zur Videoüberwachung bestehen sollte, sind in der Folge ebenfalls schon bei der Erarbeitung des später veröffentlichten Anhörungsentwurfs aufgegriffen worden. Dementsprechend ist auch in dem Bericht selbst bereits ausgeführt, dass den ursprünglichen Bedenken insofern Rechnung getragen worden ist.

Die Kritik des LfDI an der Rechtsgrundlage für ein mobiles Alarmgerät mit Mithörfunktion zum Schutz der Justizbediensteten im Außendienst wurde – nach Redaktionsschluss des Tätigkeitsberichts – bei der Erarbeitung des Regierungsentwurfs teilweise berücksichtigt.

Die Kritik des LfDI wird jedoch nicht geteilt, soweit er dem mobilen Alarmgerät mit Mithörfunktion pauschal Eignung und Erforderlichkeit zum Schutz von Justizbediensteten im Außendienst abspricht und insbesondere auch eine „Heimlichkeit“ kritisiert. Die Rechtsgrundlage soll nur dem unmittelbaren Schutz von Justizbediensteten dienen, solange deren Leben, Gesundheit oder Freiheit in dringender Gefahr ist. Das in solchen Fällen zwingende Eingreifen der Polizei wird von dem Alarmgerät bereits durch das Absetzen eines Notsignals bewirkt, das aber außer dem Standort und dem Umstand, dass ein Notfall vorliegt, keine weiteren Lageinformationen übermittelt; das über eine Leitstelle sehr schnell vermittelbare Mithören des Geschehens soll es der Polizei ermöglichen, sich bis zum Eintreffen am Ort des Geschehens in Echtzeit ein besseres Lagebild von der für Justizbedienstete wie Polizistinnen und Polizisten gleichermaßen bedrohlichen Situation zu verschaffen. Die Möglichkeit, das Gerät im Einzelfall zur Vermeidung einer möglichen dringenden Gefährdung bei einem offenen Einsatz auch verdeckt einzusetzen, ist dabei unverzichtbar, gleichwohl von vornherein an den Verhältnismäßigkeitsgrundsatz, dessen Anwendung Bestandteil jeder pflichtgemäßen Ermessensausübung ist, gebunden. Der Vermutung des LfDI, der offene Einsatz sei geeigneter, weil er stets zur Deeskalation beitrage, kann nicht

gefolgt werden: Justizbedienstete wie Gerichtsvollzieherinnen und Gerichtsvollzieher und Betreuungsrichterinnen und Betreuungsrichter treffen leider immer wieder auf Menschen, die ihnen gegenüber in der belastenden Situation einer Zwangsvollstreckung oder einer Beurteilung ihrer seelischen Gesundheit enthemmt und aggressiv auftreten. Gewalttätige Übergriffe in der Vergangenheit belegen dies. Justizbedienstete werden bei ihren Amtshandlungen in aller Regel allein tätig und sind unbewaffnet; sie sind dann auf schnelle und wirksame Hilfe der Polizei angewiesen. Dass Menschen, die nicht selten psychisch krank sind und die sich in einer erheblichen Erregungssituation befinden, sich bei einem offenen Einsatz des Alarmgeräts mit Mithörfunktion beruhigen und von einer Bedrohung oder einem Angriff auf das Leben oder die Gesundheit von Justizbediensteten ablassen werden, kann nach Auffassung der Landesregierung nicht pauschal unterstellt werden – mindestens genauso wahrscheinlich ist eine weitere Eskalation der Lage. Aus diesem Grund sieht der Regierungsentwurf die Möglichkeit eines auch verdeckten Einsatzes des Alarmgeräts trotz der Einwände des LfDI im Anhörungsverfahren weiterhin vor. Um seine Bedenken dennoch so weit wie möglich aufzugreifen, wurden die Anforderungen an den Einsatz aber generell und mit Blick auf den verdeckten Einsatz besonders verschärft.

5.1.2 ...durch Änderung des Justizvollzugsgesetzbuchs

Die Aufgaben der Justizvollzugsbehörden des Landes umfassen die gesamte Bandbreite von Lebenssituationen, in denen sich die ihnen anvertrauten Gefangenen befinden. Diese können nur sehr eingeschränkt mit Stellen außerhalb der Justizvollzugsanstalt in Kontakt treten und sind deshalb bei ihren Anliegen in vielen Lebenslagen auf die Vermittlung durch die sie betreuenden Justizvollzugsbediensteten angewiesen. Soweit es sich um Fallkonstellationen der Eingriffsverwaltung handelt oder eine Justizvollzugsanstalt zur Wahrnehmung eigener Aufgaben oder im Interesse anderer Stellen tätig wird, soll das Erste Buch des Justizvollzugsgesetzbuchs mit detaillierten datenschutzrechtlichen Regelungen teilweise neu gefasst werden. Es ist dem Gesetzgeber aber schlechterdings nicht möglich, die Vielzahl von mit dem Leben in einer Justizvollzugsanstalt verbundenen Verarbeitungssituationen vorherzusehen und gesetzlich zu regeln.

In Fällen, bei denen es sich regelmäßig um ein Tätigwerden im Interesse der oder des Gefangenen handeln wird, kann die Justizvollzugsanstalt nur auf der Grundlage einer freiwillig erteilten Einwilligung tätig werden. Die Landesregierung teilt die Auffassung des LfDI, dass die besondere Situation von Gefangenen im Justizvollzug gravierenden Einfluss auf die Freiwilligkeit ihrer Erteilung haben kann. Auch wenn die Einwilligung als Rechtsgrundlage einer Datenverarbeitung deshalb zu Recht kritisch gesehen wird, schließt die Richtli-

nie (EU) 2016/680 sie für den Strafvollzug nach Auffassung der Landesregierung generell nicht aus. Die besondere Situation der Gefangenen im Justizvollzug hat gleichwohl in Überarbeitungen des Entwurfs Berücksichtigung gefunden, nach dem die Nutzung der Einwilligung als datenschutzrechtliche Gestattung unter sehr strenge Voraussetzungen gestellt worden ist und mit ihr keinesfalls andernorts normierte hohe gesetzliche Anforderungen umgangen werden dürfen.

5.2 Datenschutz bei Rechtsanwälten

Die Landesregierung teilt die Auffassung des LfDI, dass Datenschutz und Datensicherheit bei Rechtsanwältinnen und Rechtsanwälten ein hoher Stellenwert gebührt. Der staatliche Zugriff auf dem anwaltlichen Berufsgeheimnis unterliegende Mandantenakten sollte nur in äußersten Ausnahmefällen gesetzlich zugelassen werden. Das qualifizierte Geheimhaltungsinteresse der Anwaltschaft erkennt auch die Datenschutz-Grundverordnung an, auf deren Artikel 90 die vom LfDI kritisierten Regelungen des Bundesdatenschutzgesetzes beruhen, mit denen die – im Übrigen weitreichenden – Untersuchungsbefugnisse der datenschutzrechtlichen Aufsichtsbehörden in dem sehr eng begrenzten Bereich des Zugangs zu Verfahrensakten in unionsrechtlich zulässiger Weise eingeschränkt werden.

7. Gesundheit und Soziales

7.3 Vorlage des Personalausweises und Anforderung von Kontoauszügen beim Sozialamt

Mit Schreiben vom 6. November 2018 wurde das Ministerium für Soziales und Integration durch den LfDI über die beschriebenen datenschutzrechtlichen Verstöße bei einem örtlichen Träger der Sozialhilfe in Kenntnis gesetzt.

Auf Basis der Monierungen des LfDI hat das Ministerium für Soziales und Integration mit Schreiben vom 30. November 2018 die Stadt- und Landkreise als örtliche Träger der Sozialhilfe auf die geltende Rechtslage hingewiesen sowie um Beachtung der datenschutzrechtlichen Maßgaben des LfDI gebeten.

8. Schule und Hochschulen

8.1 Datenschutzbeauftragte an öffentlichen Schulen in BW – wie „gemeinsam“ darf es denn sein?

Bereits vor Inkrafttreten der Datenschutz-Grundverordnung standen in jeder Schulaufsichtsbehörde fachkundige und fortgebildete Personen für datenschutzrechtliche Fragestellungen zur Verfügung, um bei der Beratung eine räumliche Nähe zu den Schulen zu gewährleisten. Dieser Service wird fortgeführt. Das bedeutet, dass sich Schulen auch zukünftig mit der Bitte um Beratung jeweils direkt an ihre Schulaufsichtsbehörde wenden können. Das Kultusministerium unterstützt diese Fachleute der Schulaufsicht wiederum fallbezogen oder bei Grundsatzfragen.

Um die Schulen von der durch die Datenschutz-Grundverordnung verbindlich vorgegebenen Aufgabe, einen Datenschutzbeauftragten zu bestellen, zu entlasten, stellt das Kultusministerium den Schulen Personen aus der Schulaufsicht (Staatliche Schulämter und Regierungspräsidien) zur Verfügung, die von den Schulen als behördliche Datenschutzbeauftragte bestellt werden können. Auf diese Weise ist es zudem bei den durch die Datenschutz-Grundverordnung nun auch komplexeren und umfangreicheren Aufgaben des Datenschutzbeauftragten möglich, Ressourcen und Fachwissen zu bündeln. Es steht den Schulen hierbei frei, auf diese in der Schulaufsicht verorteten Personen zurückzugreifen, den behördlichen Datenschutzbeauftragten aus ihren Reihen zu benennen oder, wenn bereits ein behördlicher Datenschutzbeauftragter vorhanden ist, diesen erneut zu benennen.

Im Tätigkeitsbericht des LfDI wurde nicht erwähnt, dass es dem Kultusministerium gelungen ist, ab 2019 insgesamt 26 neue Stellen zu erhalten, 25 Stellen davon für die Schulaufsichtsbehörden, die alleine der Aufgabe Datenschutz für die Schulen gewidmet sind, und diese Personen sich gemäß der Zuständigkeit der jeweiligen Schulaufsichtsbehörde ausschließlich als Datenschutzbeauftragte für die Schulen kümmern werden. Diese Stellen werden so verteilt, dass in jeder Schulaufsichtsbehörde, also in jedem Staatlichen Schulamt und in jedem Regierungspräsidium, jeweils eine Person vor Ort ist. Die Besetzung dieser Stellen erfolgt schnellstmöglich.

Daneben hat das Kultusministerium insbesondere Schulleitungen auf vielfältige Weise unterstützt: Auf www.it.kultus-bw.de und im Intranet der Kultusverwaltung stehen umfangreiche zielgruppenorientierte Handlungsanleitungen, Informationen, Hinweise, FAQs, Vorlagen, Formulare und Erläuterungen zur Verfügung. Eine web-basierte Plattform mit vielen detaillierten und konkreten Hilfestellungen, Leitfragen und Vorlagen bzw. Mustern erleichtert den Schulen das Führen des „Verzeichnisses der Verarbeitungstätigkeiten“. Die amtliche Lehrkräftefortbildung bietet durch Juristen der Regierungspräsidien und durch technisch versierte Pädagogen Fortbildungen zum Thema Datenschutz an für Schulleiter, Da-

tenschutzbeauftragte, Moodle-Administratoren, Multimediaberater, Fachberater und Lehrkräfte, die „Datenschutz“ im Unterricht behandeln.

Nach Ansicht des Kultusministeriums liegt kein Interessenkonflikt vor, welcher die Bestellung von Personen aus der Schulaufsicht als Datenschutzbeauftragte für Schulen ausschließen würde. Es ist grundsätzlich nicht ausgeschlossen, dass ein Mitarbeiter einer Ober- oder Mittelbehörde die Aufgabe des Datenschutzbeauftragten für die nachgeordneten Behörden wahrnimmt. Ein Interessenkonflikt läge dann vor, wenn derjenige, der in großem Umfang personenbezogene Daten verarbeitet oder für die Verarbeitung verantwortlich ist, diese Datenverarbeitung selbst überwachen und damit sich selbst kontrollieren würde, dies ist hier aber nicht der Fall. Auch schließt die Wahrnehmung von Aufgaben der Rechtsaufsicht nicht von vornherein die Benennung als Datenschutzbeauftragte aus. Diese Auffassung vertritt auch das Innenministerium in Bezug auf Beamte der Regierungspräsidien, die die Aufgabe des Datenschutzbeauftragten von Schulen übernehmen sollen. Beide Aufgaben haben zum Gegenstand, die Vereinbarkeit der behördlichen Datenverarbeitung mit dem Datenschutzrecht zu gewährleisten und auf dessen Einhaltung hinzuwirken.

9. Privater Datenschutz

9.2 Der Adresshandel

Die vom LfDI vertretene Auffassung zum Adresshandel erscheint aus Sicht des Wirtschaftsministeriums im Licht der neuen Datenschutz-Grundverordnung angemessen. Gegebenenfalls bei Adresshändlern eintretende wirtschaftliche Schäden können im Zuge des Evaluationsprozesses der Datenschutz-Grundverordnung im Herbst 2020 erörtert werden.