Anwaltsverband Baden-Württemberg
im Deutschen **Anwalt**Verein e. V.

Anwaltsverband Baden-Württemberg – Postfach 1221 – 70808 Korntal-Münchingen

Ministerium für Inneres, Digitalisierung und Migration BW
Herrn Ministerialdirigent Dr. Lehr
Frau Dr. Maximiliane Friederich
Willy-Brandt-Str. 41

70173 Stuttgart

Hasenbergsteige 5
70178 Stuttgart

Geschäftsstelle:
Johannes-Daur-Straße 10
70825 Korntal-Münchingen

Postfach 1221
70808 Korntal-Münchingen

Telefon 0711 / 2 36 59 63
Telefax 0711 / 2 55 26 55

www.av-bw.de
info@av-bw.de

07. September 2018

Per E-Mail (poststelle@im.bwl.de)!

Az. 4-1080/439-1
Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes (LVSG) und anderer Gesetze - Stellungnahme des Anwaltsverbandes BW im DAV e. V.

Sehr geehrter Herr Doktor Lehr,
sehr geehrte Frau Doktor Friederich,

für die Übermittlung der Anhörungsunterlagen zum Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes und anderer Gesetze mit Schreiben vom 26. Juli 2018 danken wir Ihnen. Der Anwaltsverband nimmt die Gelegenheit zur Stellungnahme gern wahr.

Der Anwaltsverband Baden-Württemberg e. V. ist der freiwillige Zusammenschluss der 25 örtlichen Anwaltvereine in Baden-Württemberg, die Mitglied im Deutschen Anwaltverein (DAV) sind. Er repräsentiert damit mehr als die Hälfte aller Kolleginnen und Kollegen in Baden-Württemberg und vertritt so als größte Anwaltsorganisation dieses Bundeslandes die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem DAV – auch auf nationaler und internationaler Ebene.

1. Allgemeine Bewertung

Der Anwaltsverband begrüßt es, dass mit dem vorliegenden Gesetzentwurf die Anpassung der Rechtslage an das neue europaweit und bundesweit geltende Datenschutzrecht für den speziellen Bereich für den Landesverfassungsschutz in Angriff genommen wird.

Mit den Regelungen, die redaktionellen Verbesserungen und der Anpassung an das neue Datenschutzniveau dienen, ist der Anwaltsverband weitestgehend einverstanden.

Mit Blick auf die Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung vom 27.02.2008, in dem das sog. IT-Grundrecht (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausfluss von Art. 2 GG) festgeschrieben wurde, hält der Anwaltsverband die Regelungen im LVSG BW zum Einsatz von IMSI-Catchern für unverhältnismäßig und damit rechtswidrig.

Darüber hinaus vermissen wir Schutzvorkehrungen zugunsten unabhängiger Dritter, die mit den Verdächtigen nicht in einer relevanten Verbindung stehen, sowie Schutznormen zugunsten von Berufsgeheimnisträgern.

2. Im Einzelnen

a) Zu Art. 1 – Landesverfassungsschutzgesetz BW – neu

Gegen die redaktionellen Verbesserungen in der Gliederung sowie in den §§ 4 und 5 LVSG BW-neu bestehen keine Bedenken.

Die Ergänzungen um die „*personenbezogenen Daten*“ sowie „*soweit nicht besondere Regelungen entgegenstehen*“ und „*die Einwilligung der betroffenen Person*“ erscheinen vor dem Hintergrund des neuen Datenschutzrechts und dessen Terminologie sachgerecht.

b) § 5a LVSG BW – neu

Durch diese Norm wird das Landesamt zur Erhebung personenbezogener Daten mit nachrichtendienstlichen Mitteln ermächtigt. Dies ist grundsätzlich nicht zu beanstanden, weil diese Rechtsgrundlage eine sachgerechte Aufgabenerfüllung durch das Landesamt gewährleistet.

Abzulehnen ist jedoch, dass diese Ermächtigung keinerlei Einschränkungen, insbesondere auch nicht zugunsten berufsverschwiegener Personen kennt. Wir erinnern insoweit zunächst an unsere Stellungnahme vom 14.08.2017, in der wir die – beibehaltene – in § 5c Abs. 3 LVSG (nunmehr: § 5d Abs. 3 LVSG neu, der zufolge

> „§ 3b des Artikel-10-Gesetzes mit der Maßgabe anzuwenden ist, dass sich Absatz 1 auch auf Rechtsanwälte erstreckt, die in anderen Mandatsverhältnissen als der Strafverteidigung tätig sind“

ausdrücklich befürwortet hatten. Nachdem nun aber personenbezogene Daten mit nachrichtendienstlichen Mitteln ohne Einschränkung erhoben werden sollen, wiederholen wir unsere Bedenken, die wir schon in Bezug auf § 9a PolG a. F. seit 2008 geltend gemacht hatten und denen im Ergebnis Rechnung getragen wurde.

Im Bereich der Gefahrenabwehr nach Polizeirecht hat der Landesgesetzgeber anerkannt, dass der Berufsgeheimnisschutz nicht den Berufsträgern dient, sondern dem rechtssuchenden Bürger als Vertrauensgarantie im Rechtsstaat. Auf unsere Stellungnahme zur seinerzeitigen Änderung des Landespolizeigesetzes vom 08.08.2017 nehmen wir Bezug.

Der in § 9a PolG vorgesehene Schutz der Berufsgeheimnisträger vor Maßnahmen nach §§ 20 bis 27, 29 bis 33, 35 und 36 PolG muss im Landesverfassungsschutzgesetz seine Entsprechung finden, d. h. außer in § 5c Abs. 3 LVSG bzw. § 5d Abs. 3 LVSG neu auch gegenüber der Ermächtigungsgrundlage des § 5a LVSG neu.

c) § 5 b und c LVSG BW – neu

Die Regelung in § 5c Abs. 3 LVSG neu ermöglicht dem Landesamt eine Kontostammdatenabfrage. In der Tat dürften – wie in der Entwurfsbegründung erwähnt – die in der Entscheidung

> BVerfG, Beschluss vom 13.06.2007 – 1 BvR 1550/03 u. a. –, BVerfGE 118, 168 (Rdnr. 98),

genannten **Mindestanforderungen an die Bestimmtheit** erfüllt sein. Nicht beantwortet ist damit freilich die Frage nach der Erforderlichkeit einer solchen Regelung. Die Entwurfsbegründung stellt insoweit ausdrücklich auf die Ermittlung von Sachverhalten zu Finanztransaktionen im Rahmen der **Vorfeldaufklärung bei der Terrorismusbekämpfung** ab. Die Terrorismusbekämpfung ist jedoch infolge der schon Vorbereitungshandlungen unter Strafe stellenden Vorschriften des Strafgesetzbuches (§§ 129, 129a, 129 b StGB) weitestgehend den Strafverfolgungsbehörden zugewiesen. Es dürfte leider unstreitig sein, dass radikalisierte Einzeltäter mit Mitteln der Gefahrenabwehr kaum zu

fassen sind. Es ist deshalb zu vermuten, dass mit der Ermächtigung zur Kontostammdatenabfrage weitere, in der Begründung nicht genannte Ziele verfolgt werden. Gewiss nicht ohne Grund nennt § 3 Abs. 2 Satz 1 Nr. 2 LVSG beispielsweise „sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht".

Aus diesem Grund erscheint es unverzichtbar, in § 5c Abs. 3 LVSG neu nicht nur § 3 Abs. 2 Satz 1 LVSG, sondern auch **§ 3 Abs. 2 Satz 2 LVSG** einzubeziehen. Wir schlagen deshalb vor, die Regelung wie folgt zu formulieren:

> „Soweit es zur Erfüllung seiner Aufgaben nach **§ 3 Absatz 2** erforderlich ist, darf das Landesamt für Verfassungsschutz im Einzelfall beim Bundeszentralamt für Steuern Auskünfte über die in § 93b Absatz 1 der Abgabenordnung bezeichneten Daten einholen."

Auf diese Weise ist gewährleistet, dass auch für die Kontostammdatenabfrage das Vorliegen tatsächlicher Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 2 Satz 1 LVSG erforderlich ist.

Mit der Kontostammdatenabfrage korrespondiert die Regelung in § 5b Abs. 1 Nr. 1 LVSG; danach soll das Landesamt unter bestimmten Voraussetzungen befugt sein,

> „Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen,"

einzuholen. Nach § 5b Abs. 4 LVSG sollen derartige Auskünfte nur auf Antrag eingeholt werden dürfen. Der Antrag ist durch den Leiter des Landesamtes für Verfassungsschutz oder seinen Vertreter schriftlich zu stellen und zu begründen. Über den Antrag entscheidet das Innenministerium.

Hier vermissen wir – wie auch an anderen Stellen – eine Zuständigkeitsregelung innerhalb des Innenministeriums, die eine eindeutige Verantwortungszurechnung erlaubt. Die weiteren Regelungen betreffend u. a. die Zweckbindung und den Datenschutz, vor allem die für den Auskunftsgeber geltenden Verbote und die verpflichtenden Hinweise auf diese Verbote, erscheinen mit einer Ausnahme angemessen und ausreichend: Der vollständige Ausschluss jeglicher Benachrichtigung des Betroffenen ist mit dem Datenschutz, genauer: seinem Grundrecht auf informationelle Selbstbestimmung und dem Gebot effektiven Rechtsschutzes, nicht vereinbar. Wir schlagen deshalb eine Benachrichtigungspflicht folgenden Inhalts vor, die an geeigneter Stelle, vorzugsweise in § 5b Abs. 5 LVSG, zu ergänzen ist:

> „Maßnahmen nach Abs. 1 Satz 2 und Absatz 2 sind der betroffenen Person nach Erteilung der Auskunft mitzuteilen, sobald und soweit der Zweck der Maßnahme hierdurch nicht

> gefährdet wird. Spätestens sechs Monate nach Beendigung der Maßnahme ist zu überprüfen, ob eine Benachrichtigung erfolgen kann. Bei einer Ablehnung ist diese unter Angabe von Gründen aktenkundig zu machen. Zugleich ist der Zeitpunkt für eine erneute Überprüfung spätestens nach Ablauf von sechs weiteren Monaten zu bestimmen."

Alternativ kann eine der Bestimmung § 5 c Abs. 5 LVSG neu entsprechende Regelung auch in § 5b LVSG neu eingefügt werden.

d) § 6 LVSG BW – neu

Zu den besondere nachrichtendienstlichen Mitteln, zu deren Gebrauch § 6 Abs. 2 LVSG neu in erweitertem Umfang ermächtigt zählen auch sog. IMSI-Catcher. Diese Regelung begegnet aus zweierlei Gründen Bedenken:

Das Bundesverfassungsgericht hat in seiner Entscheidung

> BVerfG, Nichtannahmebeschluss vom 22.08.2006 – 2 BvR 1345/03 –, NJW 2007, 351,

den Einsatz der IMSI-Catcher vor allem deshalb nicht beanstandet, weil bei deren Einsatz ausschließlich technische Geräte miteinander „kommunizierten". Die Feststellung einer Geräte- oder Kartennummer im Bereich einer simulierten Funkzelle befindlichen Mobiltelefons durch den Einsatz eines "IMSI-Catchers" erfolge unabhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen. Wörtlich führte das Gericht aus:

> „Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhalte bezieht. Das Aussenden der Daten erfolgt unabhängig von einem konkreten Kommunikationsvorgang oder dem Aufbau einer Kommunikationsverbindung, die einen personalen Bezug hat; der Datenaustausch ist ausschließlich zur Sicherung der Betriebsbereitschaft nötig, trägt aber keine individuellen und kommunikativen Züge. Die erfassten Daten fallen nicht anlässlich eines Kommunikationsvorgangs an, sondern im Bereitschaftszustand eines Mobiltelefons, der erst technische Voraussetzung eines Kommunikationsvorgangs ist. Die bloße technische Eignung eines Geräts, als Kommunikationsmittel zu dienen, sowie die von dem Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft stellen noch keine Kommunikation dar. Sie ermöglichen – anders als Kommunikationsumstände - keinen Rückschluss auf Kommunikationsbeziehungen und –inhalte, sondern lediglich über die Position eines Endgeräts auf den Standort einer Person."
>
> BVerfG, Nichtannahmebeschluss vom 22.08.2006 – 2 BvR 1345/03 –, NJW 2007, 351 (353 f.; Rdnr. 57)

Nichtannahmeentscheidungen nach § 93b Satz 1 BVerfGG sind „Nichtentscheidungen“, die der Verfassungsbeschwerde eine Entscheidung über ihre Zulässigkeit und Begründetheit gerade versagen. Nichtannahmebeschlüsse sind deshalb keine Entscheidungen in der Sache. Als bloße Prozessentscheidungen erwachsen sie weder in materielle Rechtskraft noch entfalten sie - anders etwa als stattgebende Kammerentscheidungen nach § 93c Abs. 1 BVerfGG - Bindungswirkung i. S. des § 31 Abs. 1 BVerfGG. Auch eine noch so ausführliche Begründung kann an diesem Befund nichts ändern. Die dem Nichtannahmebeschluss **fakultativ** beigefügten „Gründe” haben in erster Linie den Zweck, dem Beschwerdeführer die Nichtannahme seiner Verfassungsbeschwerde im Interesse größerer Akzeptanz nachvollziehbar zu machen. Eine wie auch immer geartete normative Verbindlichkeit kommt ihnen nicht zu, vielmehr sind sie als „Aussagen zur materiellen Verfassungsrechtslage **rechtlich bedeutungslos**”,

so auch Nachbaur, NJW 2007, 335:

Größeres Gewicht ist deshalb den vorangegangenen Entscheidungen des Bundesgerichtshofs beizumessen, der diesen Ansatz gerade **nicht** teilte. Er vertrat die Auffassung, es sei

> „… heute auch unstreitig, dass das **Grundrecht des Fernmeldegeheimnisses** nicht nur den Kommunikationsinhalt, sondern ebenso die **Kommunikationsumstände** umfasst; hierzu gehört insbesondere, ob und gegebenenfalls wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist.“ *(Hervorhebung vom Unterzeichner)*
>
> BGH, Beschluss vom 21.02.2001 – 2 BGs 42/01 –, NJW 2001, 1587.

Aus diesem Grund

> „…sind etwa von einem Funktelefon an die nächstgelegene Funkzelle eines Mobilnetzes übermittelte Standortdaten auch dann Gegenstand von Telekommunikation, wenn der Benutzer des aussendenden Endgeräts im Einzelfall kein aktuelles Bewusstsein von dem Vorgang hat; dasselbe gilt bei automatisierten Übertragungen. Telekommunikation im Sinne von § 100 a Abs. 1 StPO liegt jedenfalls dann vor, wenn der von einer Überwachungsanordnung Betroffene ein von ihm benutztes Mobiltelefon zum Aussenden von Nachrichten in Betrieb setzt oder wenn eine betriebsbereit gehaltene Telekommunikationsanlage Nachrichten Dritter empfängt.“
>
> BGH, Urteil vom 14.03.2003 – 2 StR 341/02 –, NJW 2003, 2034 (2035).

Die Bedenken gegen die verfassungsrechtliche Zulässigkeit des Einsatzes von IMSI-Catchern bestehen somit unvermindert fort.

Zu bedenken ist außerdem, dass alle drei vorgenannten Entscheidungen den Bereich der Strafverfolgung betrafen, nicht aber den hier interessierenden Bereich der Gefahrenabwehr, d. h. insbesondere die präventive Tätigkeit des Landeamtes.

Zwar soll der Einsatz der besonderen nachrichtendienstlichen Mittel weiterhin nur „unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes“ erlaubt sein, verzichtet werden soll aber auf die Einschränkung, der zufolge „die dort genannten Bestrebungen durch Anwendung von Gewalt oder darauf ausgerichtete Vorbereitungshandlungen verfolgt werden“ müssen. Hierfür bestehe – so die Begründung auf S. 26 - kein Anlass, weil der Straftatenkatalog des § 3 Abs. 1 des Art. 10 Gesetzes bereits für sich genommen hinreichend eng sei.

Noch vor wenigen Jahren hat der Landesgesetzgeber die Situation deutlich anders beurteilt. Zwar ist die Zulässigkeit des Einsatzes von IMSI-Catchern bereits seit dem Jahr 2005 im bisherigen § 6 Abs. 4 LVSG vorgesehen. Noch in der Begründung zum damaligen Gesetzentwurf,

> LT-Drucks. 13/4524, S. 30,

wurde ausdrücklich ausgeführt, dass der Einsatz des IMSI-Catchers nur zulässig sei, wenn es sich um Bestrebungen handele,

> „die durch die **Anwendung von Gewalt** oder darauf gerichtete Vorbereitungshandlungen“ gerichtet seien. *(Hervorhebung vom Unterzeichner)*

Die Erkenntnisse würden nähere Umstände der Kommunikation berühren, die dem Schutz von Art. 10 GG unterlägen. Was sich an dieser Einschätzung des Landesgesetzgebers seit 2005 geändert haben soll, wird in der aktuellen Gesetzesbegründung weder dargelegt noch erschließt es sich aus anderen Gründen. Der in der Begründung (S. 16 f., 25 f.) enthaltene Verweis auf die vorgebliche Rechtsprechung des Bundesverfassungsgerichts geht ersichtlich fehl, weil es eine verbindliche Feststellung der Zulässigkeit des Einsatzes von IMSI-Catchern – wie zuvor dargelegt – gerade nicht gibt. Die Begründung erweckt insoweit einen bewusst unzutreffenden Eindruck.

Nach wie vor fehlt eine nachvollziehbare Begründung, weshalb heute – anders als 2005 - in Fällen des Inlandsextremismus auf die Beschränkung auf Fälle mit Gewaltbezug verzichtet werden können soll. In der vorliegenden Fassung vermag die Begründung deshalb nicht zu überzeugen.

Vielmehr ist vor dem Hintergrund der Entscheidung

> BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 –, BVerfGE 120, 274

betreffend die verfassungsrechtlichen Grenzen für Online-Durchsuchungen unter Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) an der Einschränkung festzuhalten, der zufolge Fälle mit Gewaltbezug vorliegen müssen.

Sollte an dem Verzicht festgehalten werden, so ist im Einzelfall eine strenge Prüfung vorzunehmen, ob tatsächliche Anhaltspunkte dafür vorliegen, dass um schwere Straftaten oder solcher von erheblicher Bedeutung geht. Durch die Bezugnahme auf den Straftatenkatalog von **§ 3 Abs. 1 G 10-Gesetz** erscheint dies sichergestellt.

Unabhängig davon vermissen wir eine Regelung entsprechend **§ 3 Abs. 2 G 10-Gesetz**, der zufolge die Maßnahmen sich nur gegen den Verdächtigen oder gegen Personen richten dürfen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt.

Hingegen erscheint fraglich, ob die für den Einsatz vorgesehenen IMSI-Catcher diese technischen Beschränkungen erfüllen. Das Bundesverfassungsgericht verwies bereits selbst darauf, dass in der Literatur werden auch Modelle des IMSI-Catchers erwähnt würden, die es ermöglichten, sich in Echtzeit in laufende Mobilfunkgespräche einzuschalten und diese mitzuhören,

> BVerfG, Nichtannahmebeschluss vom 22.08. 2006 – 2 BvR 1345/03 –, juris (Rdnr. 18).

Über IMSI-Catcher, die Gespräche abhören können, wurde und wird seither in den Medien und einschlägigen Foren wiederholt berichtet,

> vgl. nur Zeit Online vom 21.08.2017.

Dass hierdurch der Schutzbereich des Grundrechts aus Art. 10 GG betroffen wird, bedarf keiner Vertiefung. Zum Schutz dieses Grundrechts bedarf es deshalb nicht nur einer technischen Beschränkung der Funktion der vom Landesamt eingesetzten IMSI-Catcher, sondern auch einer gesetzlichen Begrenzung der Ermächtigung zu deren Einsatz.

Dementsprechend ist eine Regelung ähnlich der des **§ 3a G 10-Gesetz** aufzunehmen, der zufolge die Maßnahme - sobald eine Kenntnisnahme des Gesprächsinhalts erfolgt - unverzüglich zu unterbrechen und die Aufzeichnung zu löschen ist.

Schließlich fehlt eine **§ 3b G 10-Gesetz** vergleichbare Regelung zum **Schutz der Berufsgeheimnisträger**.

Trotz der Bezugnahme auf die Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes bleibt § 6 LVSG neu deutlich hinter dem Schutz des G 10-Gesetzes zurück. Es bedarf insoweit dringend der Nachbesserung.

e) § 9 LVSG BW – neu

Die Ergänzungen in § 9 LVSG BW neu werden unserem Verband aus Gründen der Verhältnismäßigkeit befürwortet. Die Regelung gibt jedoch Anlass, eine weitere Ergänzung zu fordern:

So sollten nicht nur – wie § 9 Abs. 3 Satz 5 LVSG dies vorsieht – die Ersuchen als solche aktenkundig machen, sondern auch die Begründung, weshalb die angeforderten Daten für unerlässlich erachtet werden. Nur so kann die in § 17 Abs. 1 Satz 1 LVSG neu vorgesehene Kontrolle durch den Landesbeauftragten für den Datenschutz wirksam ausgeübt werden.

f) § 10 LVSG BW – neu

Der Anwaltsverband lehnt die Ersetzung der personalisierten Bezeichnung „*Innenminister oder im Verhinderungsfall durch seinen Vertreter*“ durch die sächliche Bezeichnung „*Innenministerium*“ ab. Dies geschieht nicht etwa, weil unser Verband eine andere, aber umständlichere geschlechtsneutrale Bezeichnung, d. h. eine Ergänzung um die Worte „*Innenministerin oder im Verhinderungsfall durch ihre Vertreterin“* vorziehen würde.

Die Ablehnung ist vielmehr deshalb begründet, weil die bisherige Regelung nicht nur eine Personalisierung, sondern zugleich eine Zuständigkeitsregelung umfasste. Die Übermittlung der betreffenden Daten bedurfte der ausdrücklichen Zustimmung der Behördenleitung; nur die Hausspitze war nach dem Gesetz zu einer solchen Zustimmung befugt. Diese Befugnis mag delegiert worden sein, ließ sich aber unmittelbar auf den Gesetzeswortlaut zurückführen. Daran fehlt es in der Entwurfsfassung; sie lässt nicht erkennen, wer bzw. welche Stelle innerhalb des Innenministeriums für eine solche Entscheidung, die unter Umständen für den Betroffenen von erheblicher Tragweite ist, zuständig sein soll. Die Letztverantwortung lässt sich nur über die Organisationsverantwortlichkeit rekonstruieren; dies genügt unserer Auffassung nach nicht, um dem Datenschutz hinreichend Rechnung zu tragen.

Im Übrigen verweisen wir auf unsere Stellungnahme vom 14.08.2017 zu der damaligen Änderung des § 10 LSVG, in der wir mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts dringenden Nachbesserungsbedarf anmahnten. Wörtlich führten wir aus:

> „Mit der beabsichtigten Neuregelung wird der bisherige § 10 Abs. 1 LVSG vollständig neu gestaltet. Die Gesetzesbegründung führt auf S. 25 f. an, dass damit die Vorgaben des Bundesverfassungsgerichts zur sog. Antiterrordatei umgesetzt werden sollen,
>
> BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277.
>
> Die neue Regelung soll sich an den schon in 2015 verabschiedeten § 19 BVerfSchG anlehnen.
>
> Erfreulich ist zunächst, dass die Behörden, an die - mit nachrichtendienstlichen Mitteln erhobenen - personenbezogenen Daten übermittelt werden dürfen, nun konkret benannt sind, wie Staatsanwaltschaften, Finanzbehörden, Polizei, Steuer- und Zollfahndungsbehörden.
>
> Des Weiteren zu begrüßen ist die Konkretisierung der Erforderlichkeit (als Ausprägung der Verhältnismäßigkeit) durch die Begrenzung der Übermittlungsbefugnis auf die eigene Aufgabenerfüllung des LfV, der Gefahrenabwehr bei entsprechendem öffentlichen Interesse, der Verhinderung von Straftaten mit erheblicher Bedeutung sowie der Verfolgung von Straftaten mit erheblicher Bedeutung.
>
> Der Anwaltsverband versteht die einschlägigen Entscheidungen des Bundesverfassungsgerichts
>
> BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277; BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220,
>
> jedoch dahin, dass aufgrund der darin entwickelten Grundsätze zur Zweckbindung und Zweckänderung – entsprechend dem Grundsatz von der hypothetischen Datenneuerhebung – eine Weitergabe von erhobenen Daten nur zum **Schutz genau solcher Rechtsgüter** und bei **Vorliegen eines ebensolchen Gefahrengrades** möglich ist, die auch die Datenerhebung gestattet haben.
>
> Dies würde im Falle von durch heimliche Wohnraumüberwachung (Art. 13 GG) oder Telekommunikationsüberwachung (Art. 10, 2 GG) erlangten Daten bedeuten, dass sie nur zum Schutz besonders gewichtiger Verfassungsgüter, wie beispielsweise in § 3 Abs. 1 G-10-Gesetz, § 129a StGB oder § 100a StPO angeführt, und bei Vorliegen eines konkreten Ermittlungsansatzes weitergegeben werden dürften,
>
> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220.
>
> Der neue § 10 Abs. 1 LVSG würde aber schon „erhebliche“ Gefahren, Schutzgüter oder Straftaten erfassen. Erheblich sein sollen nach der Gesetzesbegründung (und z. B. auch § 22 Abs. 5 PolG BW), Verbrechen nach § 12 StGB und Straftaten, die lediglich dem Bereich der mittleren Kriminalität zuzurechnen sind.
>
> Das Beispiel der mit diesem Gesetzentwurf in § 5c vorgesehenen Befugnis zur verdeckten Telekommunikationsüberwachung durch Eingriffe in informationstechnische Systeme mit Hilfe von „technischen Mitteln“ zeigt, dass die Voraussetzungen zur Datenerhebung nach dem G-10-Gesetz und zur Datenübermittlung nach dem LVSG deckungsgleich sein müssen. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 20.04.2016 mehrfach

betont, dass speziell für verdeckte Wohnraumüberwachungen und dem verdeckten Zugriff auf informationstechnische Systeme besonders hohe Anforderungen an die Datenerhebung und Datenweiternutzung zu stellen sind,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (Rdnr. 275, 294, 302).

Begründet wird die Absenkung der Eingriffsschwelle für die Übermittlung von Daten durch das LfV im hiesigen Gesetzentwurf damit, dass es nach der Datenerhebung erst noch eine Filterung vornehme, bevor es „Erkenntnisse" (nicht unbedingt alle erhobenen Daten) an die berechtigten Behörden weitergeben würde. Es seien an eine solche Datenweitergabe nicht so hohe Anforderungen zu stellen, weil sie nicht die gleiche Grundrechtseingriffsintensität hätte. Dabei wird auf die Gesetzesbegründung vom 20.04.2015 (BT-Drucks. 18/4654, S. 33) Bezug genommen. Dass die Erwägungen des Bundesverfassungsgerichts

> BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220,

in diese schlechterdings noch nicht eingeflossen sein können, bedarf keiner Vertiefung. Zum einen hat ein Betroffener nur sehr beschränkte Rechte zu erfahren, woher die über ihn erhobenen Daten stammen und wohin sie übermittelt wurden (§ 13 LVSG BW), weshalb sich für ihn die Datenweitergabe an etwa eine Polizeidienststelle, die dann über diese Informationen verfügt, als genauso schwerwiegend darstellt, als hätte die Polizei die Daten selbst erhoben. Ferner ist nicht auszuschließen, dass die vom LfV möglicherweise aus verschiedenen Datenerhebungen zusammengestellten „Erkenntnisse", die es weitergibt, sogar noch schwerwiegender wirken als hätte es nur die „Rohdaten" weitergegeben. Die Argumentation der Gesetzesbegründung vermag deshalb nicht zu überzeugen. Vielmehr ist eine Zweckänderung von der Datenerhebung zu Datenweitergabe zu unterbinden.

Auch wenn mit Blick auf die Besonderheiten der Quellen-TKÜ in § 5c Abs. LVSG BW – neu - den Besonderheiten durch Verweis auf das G-10-Gesetz Rechnung getragen wurde, bleibt festzuhalten, dass § 10 Abs. 1 LVSG BW – neu - mit Blick auf die verfassungsgerichtliche Rechtsprechung zu wenig differenziert ist und dringend der Nachbesserung bedarf."

Den seinerzeit geäußerten Bedenken wurde entsprochen, wir erhalten sie unvermindert aufrecht und haben nach wie vor verfassungsrechtliche Bedenken gegen Regelungen des § 10 LSVG.

g) § 12 LVSG BW – neu

Eine verstärkte Unterrichtung der Öffentlichkeit und Präventionsarbeit befürworten wir; damit die Regelung über die eine hiermit zusammenhängende Bekanntgabe personenbezogener Daten insoweit aber eine sachgerechte und angemessene Abwägung erlaubt, ist eine **Ergänzung** unverzichtbar. Wir schlagen vor, § 12 Satz 3 LVSG wie folgt zu formulieren:

> „Bei der Unterrichtung nach Satz 1 und den Angeboten zur Information nach Satz 2 dürfen auch personenbezogene Daten bekanntgegeben werden, wenn **und soweit** die Bekanntgabe für das Verständnis des Zusammenhangs oder der Darstellung von Organisationen oder unorganisierten Gruppierungen erforderlich ist und die Informationsinteressen der Allgemeinheit das schutzwürdige Interesse des Betroffenen überwiegen."

Auf diese Weise wird verdeutlicht, dass auch der Umfang der Bekanntgabe personenbezogener Daten der Entscheidung im Einzelfall bedarf, also nicht nur das „Ob", sondern auch das „Wie" bzw. das „Wie viel".

h) § 13 LVSG BW – neu

Die Ergänzung in § 13 Abs. 3 LVSG BW neu betreffend die Einschaltung des Landesbeauftragten für den Datenschutz in die Behandlung von Auskunftsverlangen halten wir für sinnvoll; sie entspricht dem Regelungsgehalt des § 9 Abs. 5 LDSG unter Berücksichtigung der besonderen Belange des Landesamtes für Verfassungsschutz.

i) § 14 – LVSG BW-neu – Einschränkung der Verarbeitung

Gegen die Ersetzung der „*Sperrung*" durch „*Einschränkung der Verarbeitung*" bestehen wegen § 46 Nr. 3 BDSG keine Bedenken.

j) § 15 LVSG BW – neu

Gegen die Regelungen zur Führung eines Verfahrensverzeichnisses und die Vorabkontrolle durch den (behördeninternen) Datenschutzbeauftragten bestehen keine Einwände. Sie waren – worauf in der Gesetzesbegründung zutreffend hingewiesen wird - in vergleichbarer Form im Landesdatenschutzgesetz alter Fassung enthalten.

Es erscheint uns jedoch sinnvoll, ausdrückliche Regelungen vorzusehen, denen zufolge das Landesamt für Verfassungsschutz (entsprechend §§ 5 bis 7 BDSG) behördeninterne Datenschutzbeauftragte haben muss, und deren Aufgaben und Befugnisse zu normieren.

k) § 17 LVSG BW – neu

Der Anwaltsverband begrüßt die Einführung einer unabhängigen Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz. Der vorgesehene Überprüfungszeitraum von höchstens zwei Jahren erscheint mit Blick auf die nach § 13 Abs. 3 LVSG neu vorgesehene anlassbezogene Kontrolle angemessen.

Die Subsidiarität im Verhältnis zum den Befugnissen der Kommission nach dem Ausführungsgesetz zum Artikel 10-Gesetz und die eröffnete Möglichkeit des Zusammenwirkens der Kommission mit dem Landesbeauftragten für den Datenschutz halten wir für sachgerecht und ausgewogen.

Die Beschränkung der Unterstützungspflicht nach § 26 Abs. 1 LDSG auf ihrer Funktion nach konkret bezeichnete Personen aus der Behörde Landesdatenschutzbeauftragten erscheint sinnvoll. Umso deutlicher fällt hierbei wiederum auf, dass eine vergleichbare Konkretisierung bezogen auf die Verantwortlichen innerhalb des Innenministeriums fehlt. Wir vermissen – wie zuvor bei § 10 LVSG neu – eine konkrete Bezeichnung der für die in Rede stehende Entscheidung zuständigen und verantwortlichen Person; eine solche Konkretisierung wäre hier wie dort ohne weiteres zu leisten.

l) § 18 LVSG BW – neu

Zutreffend wurde § 25 Abs. 5 Satz 1 LDSG, dem zufolge § 29 Absatz 3 des Bundesdatenschutzgesetzes unberührt bleibt und entsprechend für die Notarinnen und Notare des Landes gilt, von der Verweisung ausgenommen, weil diese Bestimmung gerade nicht die Erfüllung der Aufgaben des Landesamtes nach § 3 LVSG BW betrifft, sondern den Schutz der Berufsgeheimnisträger.

Gerade deshalb hat aber auch das Landesamt die Berufsverschwiegenheit zu respektieren. Wir erinnern daran, dass wir die Regelung in § 5c Abs. 3 LVSG BW – nunmehr § 5d Abs. 3 LVSG BW, der zufolge

> „§ 3b des Artikel-10-Gesetzes mit der Maßgabe anzuwenden ist, dass sich Absatz 1 auch auf Rechtsanwälte erstreckt, die in anderen Mandatsverhältnissen als der Strafverteidigung tätig sind“,

seinerzeit ausdrücklich begrüßt hatten; auf unsere, Ihnen bekannte Stellungnahme vom 14.08.2017 nehmen wir Bezug.

3. Zu Art. 2 – Änderung des Landessicherheitsüberprüfungsgesetzes BW

§ 37 LSÜG neu übernimmt die bisher in § 28 Abs. 2 Satz 2 bis 4 LDSG enthaltene Regelung. Das Widerspruchsrecht der betroffenen Person im Fall einer Sicherheitsüberprüfung hat den Sinn, die betroffene Person selbst darüber entscheiden zu lassen, ob die oder der Landesbeauftragte für den Datenschutz ihre

Daten kontrollieren soll. Dies ist aus unserer Sicht nicht grundsätzlich zu beanstanden. Den nunmehr vorgesehenen Verzicht auf die Schriftform des Widerspruchs halten wir jedoch für verfehlt. Die Schriftform dient der Dokumentation der Ausübung des Widerspruchsrechts und damit der Rechtssicherheit sowohl im Interesse der betroffenen Person als auch der speichernden Stelle.

Die Beibehaltung des Schriftformerfordernisses erscheint mit Blick auf die Entscheidungsbefugnisse des Landesbeauftragten für den Datenschutz nach § 25 Abs. 4 LDSG sinnvoll. Im Sinne einer Kontrollüberlegung ist in diesem Zusammenhang auf den Entwurf des Art. 2 § 70 Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden (LDSG-JB) zu verweisen, der gerichtlichen Rechtsschutz gegen derartige Entscheidungen vorsieht. Die Praktikabilität eines solchen Rechtsschutzes erfordert eine hinreichende Dokumentation, weshalb die Schriftform als unverzichtbar angesehen wird.

4. Fazit

Wir würden uns freuen, wenn unsere Hinweise und Vorschläge Berücksichtigung finden würden. Für etwaige Rückfragen oder auch Gespräche stehen wir selbstverständlich gerne zur Verfügung. Sollte im Laufe des weiteren Verfahrens eine weitere Anhörung durchgeführt werden, so bitten wir um eine Unterrichtung und die Gelegenheit zur Äußerung.

Mit freundlichen Grüßen

Prof. Dr. Peter Kothe
Präsident