LAND BRANDENBURG

Ministerium des Innern
und für Kommunales

Ministerium des Innern und für Kommunales des Landes Brandenburg
Postfach 601165 | 14411 Potsdam
Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
[redacted]
Stahnsdorfer Damm 77
14532 Kleinmachnow

Henning-von-Tresckow-Straße 9-13
14467 Potsdam

Bearb.: [redacted]
Gesch.Z.: 45-420-00
Hausruf: 0331 866-[redacted]
Fax: 0331 866-2860
Internet: www.mik.brandenburg.de
[redacted]

Bus und Straßenbahn: Alter Markt/Landtag
Bahn und S-Bahn: Potsdam Hauptbahnhof

Potsdam, 5. Juli 2018

Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes

Sehr geehrte[redacted]

in der Anlage übermittle ich Ihnen den Entwurf des Zwölften Gesetzes zur Änderung des Brandenburgischen Polizeigesetzes zur Kenntnis sowie mit der Bitte um Prüfung und Rückmeldung.

Der Gesetzentwurf hat Ihnen in einer früheren Fassung bereits auf Arbeitsebene vorgelegen. Seither haben sich im Zuge der weiteren Bearbeitung Änderungen ergeben. Diese sind aus der anliegenden Synopse ersichtlich.

Parallel erfolgt derzeit die förmliche Ressortabstimmung zu diesem Gesetzesvorhaben.

Aufgrund der Eilbedürftigkeit wäre ich für Ihre Antwort bis zum 1. August 2018 dankbar.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Hinweis: Dieses Dokument wurde am 5. Juli 2018 durch [redacted] elektronisch schlussgezeichnet.

E-Mails mit qualifiziert elektronisch signierten Dokumenten und/oder Verschlüsselung sind an die folgende Adresse zu richten: Poststelle@mik.brandenburg.de

Dok.-Nr.: 2018/105756

Zertifikat seit 2013
audit berufundfamilie

Die Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht
Dagmar Hartge

LDA Bbg. • Stahnsdorfer Damm 77 • Haus 2 • 14532 Kleinmachnow

LAND BRANDENBURG
LDA
Schutz der
- *Persönlichkeitsrechte*
- *Informationsfreiheit*

Ministerium des Innern und für Kommunales
des Landes Brandenburg
[redacted]
Henning-von-Tresckow-Str. 9-13
14467 Potsdam

Ministerium des Innern und für Kommunales
des Landes Brandenburg
Poststelle - Eingang
01. AUG. 2018
Abt. 1 No. 110

Datum: 31. Juli 2018
Bearbeiter/in: [redacted]
Telefon: 033203 356-0
Telefax: 033203 356-49
Geschäftszeichen: So/110/17/0203
(bei Antwortschreiben bitte angeben)

vorab per E-Mail:
Kriminalitaetsangelegenheiten@mik.brandenburg.de
cc an: [redacted]

Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes (BbgPolG-E)
- Ihr Schreiben vom 5. Juli 2018, Gesch.Z.: 45-420-00

Sehr geehrte[redacted]

für die Übersendung des o. g. Gesetzentwurfs zur Änderung des Brandenburgischen Polizeigesetzes und der beigefügten Synopse bedanke ich mich. Die Gelegenheit zur Stellungnahme nehme ich gerne wahr.

Vorbemerkung
Der vorliegende Gesetzentwurf enthält eine deutliche Ausweitung polizeilicher Datenverarbeitungsbefugnisse und wirft erhebliche freiheits- und datenschutzrechtliche Bedenken auf. Um das Ausmaß anschaulich zu machen, erlaube ich mir eine kurze Aufzählung. Der Entwurf schafft zahlreiche neue Eingriffsbefugnisse für die Polizei: die molekulargenetische Untersuchung zur Identitätsfeststellung (§ 12a) , die Meldeauflage (§ 15a), spezielle Möglichkeiten der Identitätsfeststellung, erkennungsdienstliche Behandlung, anlassbezogene Kennzeichenfahndung, Ausschreibung und verdeckte Registrierung zur Abwehr von Terrorgefahr (§ 28b), Aufenthaltsvorgaben und Kontaktverbote (§ 28c), elektronische Aufenthaltsüberwachung (§ 28d), Gewahrsam zur Verhinderung einer Straftat (§ 28e), Einsatz von Körperkameras im öffentlich zugänglichen Raum (§ 31a) sowie die verdeckte Datenerhebung durch Eingriffe in informationstechnische Systeme, die sowohl eine Telekommunikationsüberwachung als auch eine Durchsuchung des Systems umfasst (§ 33d), und die Anwendung von Sprengmitteln gegen Personen (§ 69). Schwerwiegend ist der neue Abschnitt 1a,

der explizit die Abwehr von Gefahren des Terrorismus als Aufgabe der Polizei festlegt (§ 28a) und damit zusammenhängend einen „nicht konkretisierten Gefahrenbegriff" als Eingriffsschwelle für polizeiliches Handeln einführt. Darüber hinaus sollen bestehende Befugnisse verschärft werden, etwa durch die räumliche Ausweitung von Identitätsfeststellungen zur Bekämpfung der grenzüberschreitenden Kriminalität (§ 12), durch die Verlängerung von Speicherfristen bei Videoüberwachungen im öffentlichen Raum (§ 31) und Bild- und Tonaufzeichnungen zur Eigensicherung (§ 31a). Auch die maximale Dauer bei kurzfristigen Observationen (§ 32) wird verlängert.

Eine Reihe von Befugnissen greifen massiv in Freiheitsrechte ein, wie etwa die Möglichkeit, im Vorfeld von feststellbaren konkreten Gefahren Aufenthaltsvorgaben und Kontaktverbote zu verhängen, und bei Zuwiderhandlungen eine vorsorgliche Ingewahrsamsnahme für bis zu 2 Wochen zu ermöglichen. Diese Regelungen stellen jedoch im Kern keine Verletzungen des informationellen Selbstbestimmungsrechts dar und sind daher meiner Beurteilung entzogen.

Mit fast jedem Änderungsgesetz wurden Datenverarbeitungsbefugnisse der brandenburgischen Polizei erweitert, niemals reduziert. Die Kumulation neuer Befugnisse und das Herabsenken der Einschreitschwellen auf einen Zeitpunkt, in dem (noch) keine konkrete Gefahr vorliegt, erhöhen die Datenmengen und haben inzwischen ein Ausmaß erreicht, das mir Sorge bereitet. Gerade letzteres wirft die Frage auf, ob Brandenburg mit dem Gesetzentwurf nicht bereits nahe an eine flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten herankommt. Einer darauf zielenden Absicht hat das Bundesverfassungsgericht bereits 2010 in der Entscheidung zur Vorratsdatenspeicherung (BVerfG Urteil vom 02.03.2010, 1 BvR 256/08 Rnr. 218) eine Absage erteilt.

Der Gesetzgeber hat Vorsorge dafür zu tragen, dass nicht alle Aktivitäten der Bürger erfasst werden können, und muss gerade beim Einsatz moderner Technik, die dem Betroffenen verborgen bleibt, mittels besondere Verfahrensanforderungen der Gefährdung durch „additive Grundrechtseingriffe" begegnen (BVerfG Urteil vom 12.04.2005, 2 BvR 581/01 Rn. 60). 2016 äußerte sich das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz erneut deutlich: „Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können." (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, Rn.130). Ich mahne daher eine Gesamtbetrachtung aller polizeilichen - insbesondere heimlicher - Überwachungsmaßnahmen an.

Positiv ist anzumerken, dass der vorliegende Gesetzentwurf gemessen an dem Referentenentwurf von mir geäußerte Kritik aufgenommen und einige Befugnisse eingeschränkt bzw. bei einer Abwägung zugunsten des Persönlichkeitsschutzes verworfen hat.

Ich bedauere, dass das Ministerium die zeitliche Dringlichkeit, materiellrechtliche Änderungen des Polizeigesetzes der genannten Art herbeizuführen höher einschätzt als die seit dem 5. Mai 2016 bestehende Verpflichtung zur inhaltlichen Umsetzung der Richtlinie EU 2016/680. Die anvisierte gesonderte Umsetzung (Fristablauf war am 6. Mai 2018) sollte unverzüglich erfolgen.

Zu den Maßnahmen im Einzelnen:

1. § 12 BbgPolG-E: Identitätsfeststellung

Mit der Änderung des § 12 Abs. 1 Nr. 6 BbgPolG-E soll es der Polizei ermöglicht werden, unter den dort genannten Voraussetzungen zusätzlich zu dem Gebiet der Bundesgrenze bis zu einer Tiefe von 30 Kilometern auch auf den Durchgangsstraßen (Bundesautobahnen, Europastraßen und anderen Straßen von erheblicher Bedeutung für den grenzüberschreitendenden Verkehr) und in öffentlichen Einrichtungen des internationalen Verkehrs die Identität einer Person in Brandenburg festzustellen. Dies wird damit begründet, dass der 30-Kilometer-Korridor allein der aktuellen Lage im Zusammenhang mit der Mobilität der Bevölkerung und potenzieller Straftäter nicht gerecht werde und dass eine effektive Gefahrenabwehr der Polizei nur sehr eingeschränkt möglich sei.

Ich halte im Wesentlichen an meiner bereits mit Stellungnahme vom 9. August 2017 geäußerten Rechtsauffassung fest, in der ich das damals anvisierte Entfallenlassen des 30-Kilometer-Korridors und damit eine Ausweitung auf das gesamte Land Brandenburg bemängelt habe. Denn durch die geplante Ausweitung wäre eine Vielzahl von Personen grundsätzlich ereignis- und verdachtsunabhängig kontrolliert und damit in ihrem Recht auf informationelle Selbstbestimmung massiv beeinträchtigt worden. Die neue Regelung wird unter anderem damit begründet, dass die grenzüberschreitende Kriminalität dort bekämpft werden soll, wo sie weitestgehend geschieht, nämlich gerade auf den genannten Straßen und in den öffentlichen Einrichtungen des internationalen Verkehrs. Leider fehlen aber auch in dem vorliegenden Gesetzentwurf konkrete Zahlen oder Beispiele, die untermauern, inwieweit eine derart weitreichende örtliche Ausdehnung der Befugnisse der Polizei notwendig ist, um die grenzüberschreitende Kriminalität zu bekämpfen. Ebenso wurde erneut die Wirksamkeit anderer Mittel, wie die schon bestehende automatisierten Kennzeichenfahndung oder der Einsatz zusätzlichen Personals, in Bezug auf die Bekämpfung der grenzüberschreitenden Kriminalität als möglicherweise milderes Mittel nicht beleuchtet.

Im Übrigen ist die geplante Einschränkung auf die genannten Straßen und öffentlichen Einrichtungen des internationalen Verkehrs anstatt auf das gesamte Landesgebiet Brandenburg nur marginal. Denn auch bei der Befugnis, auf dem gesamten Landesgebiet Identitätsfeststellungen vorzunehmen, hätte sich die tatsächliche Ausübung wohl auf Straßen und nahegelegene Autohöfe bzw. Flughäfen außerhalb des 30-Kilometer-Korridors konzentriert, da

eine zwingende Voraussetzung der Identitätsfeststellung ist, dass polizeiliche Erkenntnisse vorliegen, wonach am Ort der Maßnahme derartige grenzüberschreitende Kriminalität stattfindet. Dies ist abseits der Straßen oder öffentlichen Einrichtungen des internationalen Verkehrs außerhalb des 30-Kilometer-Korridors eher schwer denkbar.

In der Gesetzesbegründung wird weiter angeführt, dass außerhalb des Grenzgebiets, also außerhalb des 30-Kilometer-Korridors, der Kontrollraum verfassungswahrend auf wenige räumliche Bereiche eingeschränkt werde, die abstrakte Kontrollwahrscheinlichkeit erheblich herabgesetzt sei und etwaige Maßnahmen für den potenziell Betroffenen hinreichend berechenbar seien. Dies steht aber im Widerspruch zu der Befugnis der Polizei im Normtext, auf anderen Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr Identitätsfeststellungen durchführen zu können. Welche dieser Straßen im Land Brandenburg von erheblicher Bedeutung sind, bemisst sich jeweils nach den polizeilichen Erkenntnissen und ist flexibel, um die Polizei nicht vom Zufall des Verlaufens der Verkehrsströme abhängig zu machen. Das bedeutet für den potenziell zu Unrecht von der Maßnahme Betroffenen, dass er gerade nicht hinreichend berechnen kann, wann er sich ohne Einschränkungen auf welchen Straßen oder in welchen öffentlichen Einrichtungen des internationalen Verkehrs bewegen kann.

Zwar haben mittlerweile auch andere Länder mit einer Außengrenze zu osteuropäischen Ländern ähnliche Vorschriften geschaffen. So sehen das Bayerische Polizeiaufgabengesetz und der Gesetzentwurf zum Sächsischen Polizeivollzugsdienstgesetz ebenfalls eine Ausweitung des 30-Kilometer-Korridors auf bestimmte Straßen und öffentliche Einrichtungen (etc.) des internationalen Verkehrs im Landesgebiet vor. Allerdings wird zumindest im Sächsischen Entwurf die grundsätzlich ereignis- und verdachtsunabhängige Identitätsfeststellung nur dann für zulässig erachtet, soweit die Polizei die erhebliche Bedeutung für die grenzüberschreitende Kriminalität vor der Durchführung der Maßnahme durch dokumentierte Erkenntnisse dargelegt hat. Der Brandenburgische Entwurf spricht im Normtext nur von polizeilichen Erkenntnissen; lediglich aus der Begründung ist ersichtlich, dass es sich um nachweisbare Erkenntnisse handeln muss.
Unabhängig davon, dass ich die Ausweitung der Befugnisse auf Straßen und öffentliche Einrichtungen des internationalen Verkehrs außerhalb des 30-Kilometer-Korridors für nicht ausreichend begründet und für unverhältnismäßig halte, empfehle ich aus Klarstellungsgründen, die Nachweisbarkeit der Erkenntnisse und die zeitliche Komponente in den Normtext mit aufzunehmen, um der restriktiven Auslegung des Gesetzes zu mehr Geltung zu verhelfen und insofern den Belangen des Datenschutzes Rechnung zu tragen.

2. § 12a BbgPolG-E: Molekulargenetische Untersuchungen zur Identitätsfeststellung

Die in § 12a neu gefasste Befugnis zu molekulargenetischen Untersuchungen von Körperzellen greift erfreulicherweise meine Kritik auf und beschränkt den Anwendungsbereich er-

heblich. Während in der ersten Entwurfsfassung diese Methode auf alle gem. § 12 oder § 28b Abs. 2 BbgPolG zulässigen Identitätsfeststellungen anwendbar sein sollte, wird sie nunmehr auf zwei Einsatzvarianten beschränkt: die Feststellung der Identität bei unbekannten Toten und bei hilflosen Personen, wenn eine Identifizierung auf andere Weise nur unter erheblichen Schwierigkeiten möglich wäre. Damit wird der Anwendungsbereich nach sachlichen Kriterien festgelegt, die angesichts der Schwierigkeiten, Leichen oder Hilfsbedürftige zuverlässig zu identifizieren, nachvollziehbar sind. Die Analyse ist zudem gem. § 12a Abs.1 S.3 BbgPolG-E auf das DNA-Identifizierungsmuster (sog. genetischer Fingerabdruck, der nur nicht kodierter Teile der DNA umfasst) und die Feststellung des Geschlechts begrenzt. Dies entspricht dem Untersuchungsumfang des § 81e StPO. Ich ziehe daher die ursprünglich geäußerten Bedenken gegen diese Befugnis zurück.

3. § 15a BbgPolG-E: Meldeauflage

Mit der Einführung des § 15a BbgPolG-E wird eine eigenständige Rechtsgrundlage für Meldeauflagen geschaffen, sodass diese nicht mehr unter die Generalklausel fallen, was ich im Sinne der Normenklarheit für Bürger begrüße. Darüber hinaus wurde der Begriff der Straftat, wie in meiner Stellungnahme vom 9. August 2017 angeregt, in der jetzigen Fassung konkretisiert. Im Verhältnis zum ersten Entwurf, in dem eine Meldeauflage ergehen konnte, wenn Tatsachen die Annahme rechtfertigten, dass die Person eine Straftat begehen wird und die Meldeauflage zur vorbeugenden Bekämpfung der Straftat erforderlich ist, sind jetzt nur noch Straftaten gegen Leib oder Leben oder eine Straftat nach den §§ 125, 125a des Strafgesetzbuches oder nach den §§ 26, 27 oder 28 des Versammlungsgesetzes von der Vorschrift erfasst. Dies stellt meines Erachtens hinreichend sicher, dass nicht jede beliebige Straftat dazu führen kann, dass eine Person meldepflichtig wird, ihren Aufenthaltsort zu vorgegebenen Zeiten der Polizei mitteilen muss und somit in ihrem Recht auf informationelle Selbstbestimmung in unverhältnismäßiger Weise beeinträchtigt wird. Ich begrüße zudem, dass die Ermächtigung keine Meldeauflagen bereits im Vorfeld einer Gefahr zulässt, sondern eine auf Tatsachen beruhende Prognose voraussetzt, dass die betroffene Person eine Straftat begehen wird.

4. Abschnitt 1a (§§ 28a ff BbgPolG-E): Besondere Befugnisse zur Abwehr von Gefahren des Terrorismus

Mit dem neu eingefügten Abschnitt 1a wird als besondere Aufgabe der Polizei die Abwehr von Gefahren des Terrorismus festgelegt. Welche Tathandlungen darunter zu verstehen sind, legt § 28a Abs. 1 BbgPolG-E fest, der bis auf den in Brandenburg nicht vorhandenen Begriff „international" wortgleich der Definition in § 5 Abs.1 Bundeskriminalamtgesetz entspricht. Neben den in den nachfolgenden Paragrafen geregelten neuen polizeilichen Befug-

nissen besteht eine wesentliche Verschärfung darin, dass die polizeiliche Eingriffsschwelle bei diesen Straftatbeständen massiv herabgesetzt wird.

In den Befugnissen nach §§ 28b, c, d, e, g und h BbgPolG-E werden polizeiliche Eingriffe, u. a. Datenerhebungen, bereits im Vorfeld einer konkreten Rechtsgutgefährdung erlaubt, wenn

- bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Rechtsgutschädigung begehen wird oder
- ihr individuelles Verhalten die konkrete Wahrscheinlichkeit einer Rechtsgutschädigung in übersehbarem Zeitraum begründet.

Diese Formulierungen übernehmen den Wortlaut aus dem Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz vom 20. April 2016, auf dessen Umsetzung auch in der Begründung des Gesetzentwurfs Bezug genommen wird. Zwar hat das Bundesverfassungsgericht in dem Urteil zum Zweck der Straftatenverhütung unter bestimmten Voraussetzungen reduzierte Vorhersehbarkeitsanforderungen für Kausalverläufe, die zu Gefahren führen können, für verfassungsgemäß erklärt, dabei aber auch die äußerste Grenze verfassungskonformer Grundrechtseingriffe zur Gefahrenabwehr formuliert.

Wie bereits in meiner Stellungnahme vom 9. August 2017 aufgezeigt, führt die Einführung des Abschnitts 1a mit den geplanten besonderen Befugnissen zur Abwehr von Gefahren des Terrorismus dazu, dass polizeiliche Eingriffe und dadurch ggf. auch Datenerhebungen bereits im Vorfeld einer konkreten Rechtsgutsgefährdung erlaubt werden. Ich habe erhebliche Zweifel, dass diese Änderung noch verfassungsmäßig ist. Es entsteht der Eindruck, dass das Polizeirecht immer weiter dem Recht des Verfassungsschutzes angeglichen werden soll. Leider wurden trotz meiner datenschutzrechtlichen Bedenken, dass mit der zeitlichen Vorverlagerung der Eingriffsbefugnisse eine enorme Ausweitung des betroffenen Personenkreises erfolgt, bisher keine relevanten Änderungen an der Eingriffsschwelle vorgenommen, sondern die Begriffe weiterhin wortwörtlich, ohne konkrete Ausfüllung oder Definitionen, aus dem Urteil des Bundesverfassungsgerichts zum BKA-Gesetz übernommen. Insofern halte ich in weiten Teilen an meiner bereits geäußerten Kritik fest.

Das Bundesverfassungsgericht hat in seinem Urteil zum BKA-Gesetz zwar dargelegt, dass der Gesetzgeber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt ist, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Für bestimmte Bereiche, die schon die Straftatenverhütung bezwecken, können die Grenzen auch weiter gezogen werden, indem die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert werden (Rn. 112 d. Urteils). Allerdings bedarf es auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen

ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (Rn. 164 d. Urteils, vgl. auch BVerfGE 110, 33 <56 f., 61>; 113, 348 <377 f.>; 120, 274 <328 f.>; 125, 260 <330>). Bei terroristischen Straftaten kann stattdessen aber auch darauf abgestellt werden, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Die Anforderungen hierfür sind in einem Gesetz normenklar zu regeln.

Die durch das Bundesverfassungsgericht entwickelten Voraussetzungen stellen die Maximalgrenze der Eingriffsbefugnis dar. Wie bereits in meiner Stellungnahme vom 9. August 2017 ausgeführt, erschließt es sich mir nicht, warum der Gesetzentwurf automatisch die äußerste Grenze in nahezu allen Vorschriften zur Abwehr der Gefahren des Terrorismus als Eingriffsbefugnis ausgestaltet, anstatt die gesamte Bandbreite zu nutzen. Aus der Gesetzesbegründung ergibt sich hierfür keine Erklärung. Es wird lediglich darauf abgestellt, dass es der Polizei ermöglicht werden solle, auf die gestiegenen Gefahren des Terrorismus angemessen zu reagieren, und dass aus Gründen der Vereinheitlichung der Regelungen in Bund und Ländern eine Anlehnung an die entsprechenden Regelungen des BKA-Gesetzes erfolgen solle. Daraus scheint geschlossen zu werden, dass es zur vorbeugenden Terrorismusbekämpfung unerlässlich sei, eine derart zeitlich vorverlagerte Eingriffsbefugnis zu besitzen. Ich widerspreche ausdrücklich der Annahme auf Seite 2 der Gesetzesbegründung, dass sich die neu eingeführten Maßnahmen auf einen eng abgegrenzten Personenkreis beziehen würden. Vielmehr geraten durch die zeitliche Ausdehnung viel mehr Personen in den polizeilichen Fokus, als dies bisher der Fall war.

Die Voraussetzungen des Bundesverfassungsgerichts sind zudem ausfüllungsbedürftig, um dem Gebot der Normenklarheit zu genügen. Zwar ist es prinzipiell mit dem Bestimmtheitsgebot vereinbar, wenn eine Norm ausgelegt werden muss. Dies muss mit den juristischen Auslegungsmethoden möglich sein. Der Betroffene muss ab- bzw. vorhersehen können, wann der Anwendungsbereich der Norm eröffnet ist. Im aktuellen Gesetzentwurf des Brandenburgischen Polizeigesetzes werden die Voraussetzungen aus dem Urteil lediglich wortwörtlich übernommen, sodass dem Bürger eine Beurteilung, wann die Schwelle des polizeilichen Einschreitens zulässigerweise erreicht ist, nicht möglich ist. Im Übrigen stellen die unklaren und ausfüllungsbedürftigen gesetzlichen Begriffe meines Erachtens auch eine Schwierigkeit in der praktischen Anwendung sowohl durch die Polizei als auch durch die zuständige Datenschutzaufsicht dar. Denn es ist nicht definiert, wann beispielsweise ein „übersehbarer Zeitraum", eine „konkrete Wahrscheinlichkeit" oder ein „individuelles Verhalten" vorliegen. Dies kann auch nicht mithilfe juristischer Auslegungsmethoden bestimmt werden, da die Begriffe zu schwammig sind. In der Gesetzesbegründung findet sich zu der Frage eines übersehbaren Zeitraumes die Aussage, dass dessen Umfang lageabhängig sei und in der Regel „nicht mehr als Tage bis maximal Wochen" umfasse. Das ist keine ausreichende Konkretisierung.

Weiter führt die Gesetzesbegründung aus, dass, da die Formulierungen damit den Anforderungen des Bundesverfassungsgerichts an eine hinreichende Bestimmtheit genügten, eine weitere Konkretisierung nicht erforderlich sei, sodass durch die Regelung eine notwendige flexible polizeiliche Reaktion auf entsprechende Anhaltspunkte ermöglicht werde.

Dies steht im Widerspruch zum Urteil des Bundesverfassungsgerichts, wonach die Anforderungen an ein Abweichen von den tradierten sicherheitsrechtlichen Gefahrenabwehrkategorien normenklar zu regeln sind. Es ist nicht erkennbar, wie viele Tage oder Wochen ein übersehbarer Zeitraum maximal beinhalten darf. Im Extremfall könnte dieser Zeitraum unerträglich weit ausgedehnt werden, sodass ggf. unbeteiligte Personen wochenlang einer polizeilichen, eventuell sogar verdeckten Maßnahme ausgesetzt sind. Dies stellt einen massiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG dar.

Im ersten Entwurf waren von den jeweiligen Eingriffsnormen auch Personen umfasst, bei denen Tatsachen die Annahme rechtfertigen bzw. die konkrete Wahrscheinlichkeit begründet ist, dass sie unter den oben genannten Voraussetzungen zu einer Straftat nach § 28a Abs. 1 PolGBbg-E anstiften oder Beihilfe leisten werden. Ich habe in meiner Stellungnahme vom 9. August 2017 dargelegt, dass dies Schwierigkeiten in der praktischen Rechtsanwendung nach sich ziehen könnte, insbesondere, weil die Gesetzesbegründung keinerlei Anwendungsbeispiele oder Erklärungen enthalten hat. Daher begrüße ich es, dass nunmehr nur noch auf die Begehung einer entsprechenden Straftat abgestellt wird, zumal auch in anderen Landespolizeigesetzen bzw. –entwürfen die Beteiligungsformen der Beihilfe und Anstiftung nicht erfasst sind.

5. § 28d BbgPolG-E: Elektronische Aufenthaltsüberwachung (EAÜ)

Meine bereits in der Stellungnahme vom 9. August 2017 geäußerte grundsätzliche Kritik an der Einführung der elektronischen Aufenthaltsüberwachung zur Gefahrenabwehr halte ich aufrecht. Dass sich die bisher im Rahmen der Führungsaufsicht in geringer Zahl erprobte Überwachungsmaßnahme auf Personen übertragen lässt, die als sog. Gefährder eingestuft werden, ist fraglich. Angesichts der geringen Forschungserkenntnisse zur Wirksamkeit dieser Maßnahme bzw. erster ernüchternder Auswertungen der Maßnahme bei Führungsaufsicht[1] ist äußerste Zurückhaltung bei der Ausweitung des Einsatzes geboten. Die Gesetzesbegründung geht schlicht davon aus, dass die bisherige Nutzung erfolgreich war und entsprechend die EAÜ auch bei Personen, von denen in Zukunft eine Gefahr ausgehen könnte, terroristische Straftaten im Sinne des § 28a BbgPolG-E zu begehen, nutzbar wäre. Die Ge-

[1] Empirische Studie: Bräuchle/Kinzig, Die elektronische Aufenthaltsüberwachung im Rahmen der Führungsaufsicht, Kurzbericht über die wesentlichen Befunde einer bundesweiten Studie mit rechtspolitischen Schlussfolgerungen, S. 16; Bräuchle, in: Kinzig/Kerner, Tübinger Schriften und Materialien zur Kriminologie, Die elektronische Aufenthaltsüberwachung gefährlicher Straftäter im Rahmen der Führungsaufsicht, S. 164 f.

eignetheit wird mit der Möglichkeit, den Standort des Betroffenen in Echtzeit (über GPS) festzustellen und ggf. ein sofortiges Einschreiten der Polizei zu ermöglichen, begründet. Verhältnismäßig sei die Maßnahme, da es um die Gefahrenabwehr für hochrangige Rechtsgüter und die Abwehr schwerwiegender Straftaten gehe und damit einem überragenden Gemeinwohlinteresse diene. Die sog. „Fußfessel" sei auch als offene Maßnahme weniger einschneidend als die stattdessen in Betracht kommende ständige Observation eines Gefährders, da von dieser auch Dritte betroffen seien und das Persönlichkeitsbild noch umfassender beleuchtet werde.

Aus meiner Sicht wirft die elektronische Aufenthaltsüberwachung in ihrer Ausgestaltung tief greifende datenschutzrechtliche Zweifel hinsichtlich der Verfassungsgemäßheit der Maßnahme auf. Die EAÜ ist ein äußerst weitreichender Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen, der sich – obwohl offen gestaltet – in seiner Wirkung auf das Persönlichkeitsrecht mit einer heimlichen durchgeführten Überwachung bzw. Observation vergleichen lässt. Aufgrund der rund um die Uhr übermittelten Daten lässt die Maßnahme Rückschlüsse auf den Aufenthaltsort und damit auch auf das Privatleben des Trägers zu. Besuche im öffentlichen Raum werden ebenso dokumentiert wie Besuche bei Freunden, Ärzten oder anderen Berufsgeheimnisträgern. Auch der Besuch von weltanschaulichen oder religiösen Veranstaltungen und Versammlungen wird aufgezeichnet. Da Aufenthaltsdaten in einem langfristigen Zeitraum von bis zu drei Monaten erhoben werden dürfen, werden nicht nur einzelne Situationen erfasst, sondern es lässt sich ein detailliertes Bild über das Privatleben der Person zusammensetzen und ein Bewegungsprofil erstellen.

Diese Eingriffstiefe verbietet es jedenfalls, die Eingriffsvoraussetzungen der Befugnis an einen vorverlagerten Gefahrenbegriff (s. Abs. 1 S. 1 Nr. 1. und 2.) zu knüpfen. Die Unschärfe und Unbestimmtheit der in den Gesetzeswortlaut übernommenen Begrifflichkeiten (s. o. unter 4.) erlauben es nicht mehr, die Schwelle polizeilichen Eingreifens vorherzusehen. Ich begrüße, dass in der neuen Entwurfsfassung des Gesetzes die Begehungsformen der Anstiftung und Beihilfe als Tathandlungen gestrichen wurden. Ich halte jedoch angesichts der Schwere des mit der EAÜ verbundenen Grundrechtseingriffs auch bei täterschaftlichem Handeln eine Anknüpfung an den vorverlagerten Gefahrenbegriff für unverhältnismäßig. Wenn der Gesetzgeber überzeugt ist, nicht auf diese Maßnahme zur Gefahrenabwehr verzichten zu können, empfehle ich wie bei der längerfristigen Observation gemäß § 32 BbgPolG-E als Voraussetzung eine konkrete Gefahr festzuschreiben.

In Absatz 2 Satz 3 der Norm werden die Verwendungszwecke der erhobenen Aufenthaltsdaten aufgelistet. Daneben sollen mit Einwilligung der betroffenen Person die Daten auch für sonstige Zwecke verwendet werden dürfen. Ob eine einwilligungsbasierte Zweckänderung auch nach der noch umzusetzenden Richtlinie EU 2016/680 zulässig ist, sollte geprüft werden.

Mir sind bisher keine Fälle einer Nutzung der elektronischen Aufenthaltsüberwachung in Brandenburg bekannt. Es stellt sich daher auch prinzipiell die Frage, ob eine Befugnisnorm dieser Eingriffsintensität prophylaktisch für einen abstrakt denkbaren Anwendungsfall geschaffen werden soll.

6. § 29 BbgPolG-E: Grundsätze der Datenerhebung

Mit der Neufassung des § 29 Abs. 6 BbgPolG-E wird der Kernbereich privater Lebensgestaltung in ausreichender Weise geschützt. Es werden somit datenschutzrechtliche Belange des Betroffenen gewahrt.

Das Bundesverfassungsgericht hat in seinem Urteil zum BKA-Gesetz (Rn. 123 d. Urteils) klargestellt, dass der Kernbereich privater Lebensgestaltung gegenüber allen Überwachungsmaßnahmen Beachtung beansprucht. Wenn die Überwachungsmaßnahmen typischerweise zur Erhebung kernbereichsrelevanter Daten führen können, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten (vgl. BVerfGE 109, 279 <318 f.>; 113, 348 <390 f.>; 120, 274 <335 ff.>). Dies ist mit der dezidierten Regelung des § 29 Abs. 6 PolGBbg-E in Ausführung des oben genannten Urteils geschehen. Nach dem Bundesverfassungsgericht ist der Schutz des Kernbereichs privater Lebensgestaltung strikt und darf nicht durch Abwägung mit Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsprinzips relativiert werden (Rn. 124 d. Urteils, vgl. BVerfGE 109, 279 <314>; 120, 273 <339>; stRspr). Bei der Durchführung von Überwachungsmaßnahmen muss dem Kernbereichsschutz sowohl auf der Ebene der Datenerhebung als auch auf der Ebene der anschließenden Auswertung und Verwertung Rechnung getragen werden (Rn. 126 d. Urteils, vgl. BVerfGE 120, 274 <337 ff.>; 129, 208 <245 f.>). Wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt, muss die Überwachungsmaßnahme abgebrochen werden (Rn. 128 d. Urteils, vgl. BVerfGE 109, 279 <318, 324, 331>; 113, 348 <392>; 120, 274 <338>). Wenn die Erhebung kernbereichsrelevanter Daten nicht vermieden werden konnte, sind die Daten von einer unabhängigen Stelle zu sichten und die kernbereichsrelevanten Daten herauszufiltern, bevor die Daten von der Sicherheitsbehörde verwendet werden (Rn. 129 d. Urteils, vgl. BVerfGE 109, 279 <331 f., 333 f.>; 120, 274 <338 f.>). § 29 Abs. 6 S. 2 PolGBbg-E bestimmt, dass die Datenerhebung zu unterbrechen ist, wenn erkennbar wird, dass durch die Erhebung in den Kernbereich privater Lebensgestaltung eingedrungen wird. Damit wird der Vorgabe, dass der Kernbereichsschutz schon bei der Erhebung der Daten zu beachten ist, Rechnung getragen. Die Überprüfung der Daten durch das Amtsgericht als unabhängiger Stelle, bevor die Daten weiter verarbeitet werden dürfen, wird von § 29 Abs. 6 S. 3 BbgPolG-E umgesetzt.

Das Bundesverfassungsgericht stellt klar, dass der Gesetzgeber die sofortige Löschung von gegebenenfalls erfassten höchstpersönlichen Daten vorsehen und jegliche Verwendung ausschließen muss. Die Löschung muss so protokolliert werden, dass eine spätere Kontrolle

ermöglicht wird (Rn. 129 d. Urteils, vgl. BVerfGE 109, 279 <318 f., 332 f.>; 113, 348 <392>; 120, 274 <337, 339>). Dies wird durch § 29 Abs. 6 S. 5 und 6 PolGBbg-E erreicht. Satz 7 stellt darüber hinaus klar, dass die Protokolldaten später nur dazu verwendet werden dürfen, zu überprüfen, ob die Maßnahme rechtmäßig durchgeführt worden ist.

7. § 31 BbgPolG-E: Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie auf öffentlich zugänglichen Straßen und Plätzen

Erfreulich ist, dass im Sinne meiner Kritik aus der Stellungnahme vom 9. August 2017 die geplante zeitliche Ausdehnung der Datenerhebung aus § 31 Abs. 1 S. 1 BbgPolG-E wieder rückgängig gemacht wurde. Ursprünglich beabsichtigte der Gesetzentwurf, Bild- und Tonaufzeichnungen von Teilnehmern öffentlicher Veranstaltungen und Ansammlungen bis zu zwei Wochen im Vorfeld dieser Ereignisse erheben zu können.

Darüber hinaus regelt der aktuelle Gesetzentwurf in § 31 Abs. 2 S. 3 BbgPolG-E, dass Bildaufnahmen, die die Polizei an öffentlich zugänglichen Straßen und Plätzen anfertigen darf, innerhalb von zwei Wochen zu löschen sind, was zwar eine Verbesserung gegenüber der ursprünglich geplanten Zeitspanne von einem Monat, ist aber immer noch eine um das Siebenfache erhöhte Speicherfrist zum momentan geltenden Gesetzestext, 48 Stunden, darstellt. Auf meine Kritik hin, dass die Gesetzesbegründung für die Erweiterung der Speicherdauer zu pauschal und nicht ausreichend sei, wurde diese zwar angepasst. Allerdings überzeugen auch die nun vorliegenden Ausführungen für die Erforderlichkeit einer zweiwöchigen Speicherdauer unter Verhältnismäßigkeitsgesichtspunkten nicht. Bei der Norm handelt es sich um eine Befugnis der Polizei zur Gefahrenabwehr, also um präventives Tätigwerden in einem konkret benannten Bereich, um dort Straftaten zu verhüten. Kommt es zu einer Straftat oder Ordnungswidrigkeit, können die Bildaufnahmen zur repressiven Verfolgung von Straftaten oder Ordnungswidrigkeiten ohnehin solange gespeichert werden, wie sie für diese Zwecke benötigt werden, § 31 Abs. 2 S. 4 BbgPolG-E.

Die Gesetzesbegründung stellt allerdings darauf ab, dass durch eine generelle Verlängerung der Speicherdauer sowohl im Nachgang als auch im Vorfeld einer Straftat wichtige Erkenntnisse zum Täter erlangt werden könnten. Falls sich der Täter im Nachgang einer Straftat an einen (anderen) videoüberwachten Ort begebe, könnten dadurch beispielsweise das Fluchtverhalten und die Fluchtwege eines Attentäters/einer Attentäterin, das Aussehen oder mögliche Mittäter oder Kontaktpersonen noch nach Tagen bzw. Wochen aufgeklärt und durch die dabei erlangten Erkenntnisse weitere Folgetaten verhindern werden. Außerdem sei auch an erst nach und nach eingehende Hinweise zu denken, die den zwischenzeitlichen Aufenthalt des Täters an einem videoüberwachten Ort begründeten. Solche Aufnahmen sollten daher nicht vorschnell gelöscht werden, damit die Erkenntnisse nicht verloren gingen.

Zwar kann ich die Sorge nachvollziehen, dass Videoaufnahmen nicht vorschnell gelöscht werden sollen, wenn die Möglichkeit besteht, dass der Täter sich vor oder nach der Tat an einem videoüberwachten Ort aufgehalten hat und dort ggf. Mittäter getroffen hat. Auch ist einleuchtend, dass diese Erkenntnisse möglicherweise weitere Straftaten verhindern könnten. Dennoch sollte meines Erachtens die vorliegende Befugnis der Polizei, bestimmte Orte videoüberwachen zu dürfen, nicht dazu dienen, auf Vorrat Filmaufnahmen über einen längeren Zeitraum zu speichern, nur für die ungewisse Annahme, dass eine Person sich nach einer bereits begangenen Straftat an einen anderen videoüberwachten Ort begibt und damit dann ein Abgleich mit bereits bestehenden Aufnahmen ermöglicht werden kann. Dies gilt ebenso für den Fall, dass eine Person sich vor der Begehung einer Straftat an einem anderen videoüberwachten Ort aufgehalten hat und nach der Tat ein Abgleich ermöglicht werden soll. Die zweiwöchige Speicherfrist würde eine Vielzahl unbeteiligter Personen über einen langen Zeitraum betreffen, die sich lediglich an einem der benannten Orte aufhalten, ohne dass sie selbst eine Straftat begangen hätten. Daher ist die pauschale Erweiterung der Speicherfrist unter datenschutzrechtlichen Aspekten unverhältnismäßig und unzulässig.

Als weniger einschneidende Maßnahme wäre es denkbar, nach der Begehung einer Straftat nach § 129a StGB an allen Orten, an denen die Polizei Videoüberwachungen nach § 31 BbgPolG-E durchführt, die Speicherfrist manuell von 48 Stunden auf zwei Wochen hochzusetzen, da dann ein begründeter Anlass hierfür bestünde.

8. § 31a BbgPolG-E: Datenerhebung zur Eigensicherung (Body-Cams)

Die Änderung im Absatz 1 betrifft Bildaufnahmen sowie Bild- und Tonaufzeichnungen in Fahrzeugen der Polizei, die bereits bisher im Polizeigesetz als Befugnis normiert waren. Die Löschfrist wird jedoch von bisher einem Tag nach der Aufnahme auf zwei Wochen verlängert. Diese erhebliche Ausweitung ist nur im Zusammenhang mit der in Absatz 2 gefassten Neuregelung, die ebenfalls eine Zweiwochenfrist vorsieht, vertretbar.

Absatz 2 führt zum Zweck der Eigensicherung nun die Erlaubnis für die Polizei ein, in öffentlich zugänglichen Räumen Bildaufnahmen sowie Bild- und Tonaufzeichnungen durch körpernah getragene technische Mittel durchzuführen (sog. Body-Cams). Damit wird die bestehende Eigensicherungsmaßnahme auf sämtliche Personen- und Fahrzeugkontrollen der Polizei ausgeweitet, wenn der Einsatz einer Körperkamera nach den Umständen zum Schutz gegen eine Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Die neue Befugnis greift schon aufgrund ihrer Streubreite erheblich in das Recht auf informationelle Selbstbestimmung ein. Die Anzahl Betroffener ist bei Aufnahmen und Aufzeichnungen größer, da Einsätze räumlich nicht mehr auf das Polizeifahrzeug beschränkt sind. Betroffene sind zudem nicht nur die Zielpersonen des Einsatzes, sondern auch Dritte, die sich zufällig im öffentlichen Raum im Aufnahmebereich der Kamera befinden und erfasst werden.

Grundsätzlich ist zu begrüßen, dass für die Datenerhebung mittels körpernah getragener Kameras eine ausdrückliche Rechtsgrundlage geschaffen werden soll. Im Hinblick auf den Verhältnismäßigkeitsgrundsatz bestehen jedoch Zweifel an der Geeignetheit und Erforderlichkeit der Eingriffsbefugnis. Ob eine Kamera tatsächlich die erhofften Auswirkungen, vor allem Abschreckungseffekte hat, sollte mittels einer objektivierten Evaluierung eines Pilotprojekts ausgewertet werden. Die Begründung verweist darauf, dass der Einsatz von Körperkameras bei Pilotprojekten (z. Bsp. in Frankfurt am Main) zu einer erhöhten Kooperationsbereitschaft bei Betroffenen in Konfliktsituationen geführt, Solidarisierungseffekte von Unbeteiligten reduziert und damit insgesamt die Zahl der Übergriffe auf Einsatzkräfte verringert habe. Diese Bewertung beruht zwar auf polizeilichen Erfahrungen, entspricht aber nicht einer nach wissenschaftlichen Maßstäben ausgerichteten Wirkungsanalyse. Ob die festgestellten positiven Effekte tatsächlich auf die Wirkung der Kameras oder möglicherweise auf andere Faktoren zurückgehen, sollte untersucht werden. Ein Rückgang von Angriffen könnte mit statistischen Schwankungen oder damit zusammenhängen, dass an den ausgewählten Brennpunkten im Test ein höherer Personaleinsatz vorgehalten wurde. Zudem wurden in den Pilotprojekten auch Beamte, die erkennbar eine Body-Cam trugen, Ziel von Angriffen und Widerstandshandlungen[2]. Erstaunlicherweise enthält die Gesetzesbegründung auch keine Hinweise auf Erfahrungen, die mit der in Brandenburg bereits existierenden Regelung zur Bild- und Tondatenerhebung in Polizeifahrzeugen § 31a BbgPolG gemacht wurden.

Ich empfehle, die Eingriffsbefugnis zu befristen und die Maßnahme nach Zeitablauf von max. 2 Jahren zu evaluieren. In dieser Zeit könnte ein brandenburgisches Pilotprojekt durchgeführt werden. Erst danach ist eine verantwortliche Abwägungsentscheidung zwischen den Einschränkungen des Rechts auf informationelle Selbstbestimmung und präventiven Effekten möglich.

Positiv zu bewerten ist, dass von Planungen, den Einsatz von Körperkameras auch in Wohnungen zu erlauben, Abstand genommen wurde und Bereiche, in denen Berufsgeheimnisträger ihrer Tätigkeit nachgehen, ausgeschlossen wurden.

Die Nutzung der Körperkameras schließt die Möglichkeit von Vorabaufnahmen (sog. „Pre-recording") in Absatz 2 Satz 3-5 der Vorschrift ein. Dies bedeutet, dass die von dem Beamten aktivierte Kamera permanent, auch dann, wenn keine gewalttätige Eskalation bei der Kontrolle eintritt, die Bild- und Tondaten erfasst, diese erhobenen Daten für einen vorkonfigurierten Zeitraum (hier 60 Sekunden) in einem Kurzzeitspeicher ablegt und danach überschreibt. Erst durch eine zweite Aktivierung des Beamten wird die permanente Aufzeichnung ausgelöst, die dann jedoch die vorangegangenen 60 Sekunden mitumfasst. Der Einsatz von „Pre-recording" stellt einen Grundrechtseingriff dar. Bereits in der vorangegangenen Stellungnahme habe ich deutlich gemacht, dass dadurch völlig anlasslos das gesamte Gesche-

[2] vgl. Abschlussbericht des Polizeipräsidiums Frankfurt am Main über die Erfahrungen des Einsatzes der mobilen Videoüberwachung gem. § 14 Abs. 6 HSOG im Rahmen der Maßnahmen „Alt-Sachsenhausen" sowie im Bereich des 1. Polizeireviers des Polizeipräsidiums Frankfurt am Main vom 1.10. 2014, Zf. 2.1.1

hen einer Kontrolle „auf Vorrat" aufgezeichnet wird, was ich verfassungsrechtlich für äußerst problematisch halte.

Unklar ist wie die Transparenz für Betroffene praktisch hergestellt werden soll. Das Pre-recording muss aus Transparenzgründen für den Betroffenen und ggf. Dritte deutlich erkennbar sein, damit diese ggf. gegen die Kameraüberwachung effektiv vorgehen können. Um die Body-Cam rechtmäßig nutzen zu können, müsste daher in der Praxis darüber aufgeklärt werden, dass die Kamera eingeschaltet ist, aber ein Überschreiben der Daten stattfindet, solange die Speicherungsvoraussetzungen nicht eintreten. Ob die Nutzung in diesem Fall noch eine Abschreckungswirkung entfaltet, ist fraglich. Der kameraführende Beamte dürfte jedenfalls nicht den Eindruck erwecken oder gezielt falsch informieren, dass bereits eine dauerhafte Aufnahme stattfindet, obwohl dies tatsächlich nicht der Fall ist.

Dass diese Funktion der Vorabaufzeichnung aus technischer Sicht erforderlich sei, wie die Begründung vorgibt, damit die Entstehung einer Gefahrenlage ohne Verzögerung dokumentiert werden könne, reicht aus meiner Sicht nicht. Die Beweisführung im Falle eines Übergriffs ist nicht nur mithilfe der aufgezeichneten Bildaufnahmen möglich, sondern wie bisher auch mithilfe der Aussagen der beteiligten Beamten. Andere Länder, die die Befugnis zur Datenerhebung mittels Körperkamera bereits eingeführt haben (vgl. Nordrhein-Westfalen: § 15c PolGNRW) oder einführen wollen (Niedersachsen: § 32 Abs.4 NdsSOG-E) verzichten ebenfalls auf das Pre-recording. Ich empfehle daher dringend, diese Funktion zu streichen, bzw. eine Evaluation der Maßnahme abzuwarten (s. o.). Jedenfalls sollten nur Kameras zum Einsatz kommen, bei denen technisch eine Abschaltung der Pre-recording-Funktion vorgenommen werden kann.

Neben der Bildaufzeichnung erlaubt die Vorschrift auch Tonaufzeichnungen, was nach der Gesetzesbegründung die präventive Wirkung erhöhen soll. Geht man davon aus, dass es vor tätlichen Auseinandersetzungen verbale beleidigende und aggressive Äußerungen gibt, könnte es sein, dass die Aufzeichnung der Kommunikation – vorausgesetzt der Betroffene wird darauf hingewiesen – deeskalierend wirkt. Hier könnten Erfahrungen aus der Anwendung der bereits bestehenden Befugnis (§ 31a Absatz 1), Tonaufnahmen in Fahrzeugen der Polizei aufzuzeichnen, hilfreich sein. Leider enthält die Begründung diesbezüglich keine Hinweise. Kommt es zu einem Übergriff, der mit Bild und Ton gespeichert wird, muss dieses Material sowohl der Polizei als auch der betroffenen Person zur Auswertung zur Verfügung stehen. Im Rahmen eines Pilotprojektes stimme ich daher einer Tonaufzeichnung zu. Nach einer gründlichen Auswertung der Erfahrungen sollte geprüft werden, ob der Zweck, Eskalationsverläufe zu unterbrechen und z. Bsp. Solidarisierungen Dritter gegen die Polizei zu verhindern, tatsächlich durch Tonaufnahmen messbar besser erfüllt wird als durch reine Bildaufzeichnungen. Wird erkennbar, dass Tonaufzeichnungen vorrangig Verwendung finden, um nach erfolgten Übergriffen mündlich erteilte polizeiliche Weisungen oder Beleidigungen der eingesetzten Beamten zu dokumentieren, haben sie sich als ungeeignet für den Zweck erwiesen, eine Gefahr für Leib, Leben oder Freiheit abzuwehren. Für Beweiszwecke eines

Bagatelldelikts wie Beleidigung ist eine Tonaufzeichnung des gesprochenen Wortes nicht als verhältnismäßig anzusehen.

In der bisherigen, räumlich auf den Einsatz in Fahrzeugen der Polizei beschränkten Regelung mussten die Bild- und Tonaufzeichnungen am Tage nach dem Anfertigen gelöscht oder vernichtet werden. Durch den Verweis auf die in Absatz 1 Satz 4 eingefügte Änderung, wird die Löschfrist auf zwei Wochen erweitert. Wie in der Begründung erwähnt, sollen die zu Zwecken der Eigensicherung gefertigten Aufzeichnungen als Nebeneffekt auch dann zur Verfügung stehen, wenn polizeiliches Handeln im Falle eines Vorwurfs pflichtwidrigen oder strafbaren Verhaltens durch Auswertung der Daten überprüft werden soll. Zur Wahrung effektiver Betroffenenrechte (Auskunft und Einsichtnahme in die Bild- und Tonaufzeichnung) ist eine längere Mindestspeicherdauer erforderlich. Wir halten diese Verlängerung auf bis zu zwei Wochen im Hinblick auf diesen Zweck für vertretbar. Sie stellt potenziell eine Verbesserung der Betroffenenrechte dar. Es ist jedoch durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass das Datenmaterial vor unbefugten, auch manipulativen Zugriffen geschützt ist.

Der Gesetzestext enthält darüber hinaus keine Regelung dazu, wie der Auswertungsvorgang durch die Polizei erfolgen soll. Aus Transparenzgründen sollte festgelegt werden, wer die Aufzeichnungen auswertet. Zugleich ist ein Auskunftsrecht für Betroffene vorzusehen.

9. § 32 BbgPolG-E: Datenerhebung durch Observation

Die Änderung des § 32 BbgPolg-E beabsichtigt ausweislich der Gesetzesbegründung eine angemessene Erweiterung der Dauer der kurzfristigen Observation. Bisher kann eine anordnungsfreie und damit kurzfristige Observation durchgeführt werden, wenn sie durchgehend nicht länger als 24 Stunden dauert oder sie nur an bis zu zwei Tagen erfolgt. Dabei bedingen sich die Alternativen gegenseitig, das heißt, es ist nicht möglich, an zwei Tagen durchgehend zu observieren; dies muss unterbrochen erfolgen. Das zulässige Höchstmaß einer kurzfristigen Observation beträgt somit bisher jeweils 23 Stunden und 59 Minuten an insgesamt zwei Tagen oder einmalig durchgehend 24 Stunden.

Durch die Gesetzesänderung soll die durchgehende, kurzfristige Observation auf 72 Stunden erhöht und die Anzahl der Tage auf vier erhöht werden. Hiergegen habe ich erhebliche Einwände, da die Verdopplung bzw. Verdreifachung der Observierungszeiten dazu führt, dass massiv in die datenschutzrechtlichen Belange der betroffenen Personen und ihrer Kontakt- oder Begleitpersonen eingegriffen wird. Leider wird auch hier in der Gesetzesbegründung nicht in ausreichendem Umfang dargelegt, warum die Erhöhung der Observierungszeiten erforderlich ist. Es gibt keinerlei Ausführungen dazu, dass die bisher bestehenden Zeiten sich als zu kurz erwiesen hätten, um eine vorbeugende Bekämpfung von Straftaten gewähr-

leisten zu können. Vielmehr wurde lediglich erläutert, dass Observationen ein probates Mittel seien, um im Rahmen der vorbeugenden Bekämpfung von Straftaten mögliche Tatvorbereitungshandlungen erkennen und entstehende Gefahren verhindern bzw. abwehren zu können. Durch die Erweiterung könnten Überwachungsmaßnahmen auch über das Wochenende und an Feiertagen eigenständig durchgeführt werden. Dies genügt den Anforderungen an eine Erforderlichkeit nicht.

Im Vergleich mit anderen Bundesländern würde Brandenburg zukünftig somit einen vergleichsweise langen Observierungszeitraum erlauben. Sachsen, Nordrhein-Westfalen und Bayern erlauben weiterhin nur die bisherigen durchgehenden 24 Stunden bzw. zwei Tage. Auch angesichts der Regelungen dieser Vergleichsländer erschließt sich die deutlich darüber hinausgehende brandenburgische Regelung nicht.

Begrüßenswert ist allerdings, dass die längerfristige Observation zukünftig von einem Gericht bzw. bei Gefahr im Verzug durch die Behördenleitung angeordnet werden soll. Durch die Einbindung des Gerichts als unabhängiger Stelle wird eine Überprüfung der Notwendigkeit eines Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Personen erreicht.

10. § 33 BbgPolG-E: Datenerhebung durch den verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes und zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen

Durch die Änderung des § 33 BbgPolG-E soll der verdeckte Einsatz technischer Mittel, soweit er länger als durchgehend 72 Stunden oder an mehr als vier Tagen erfolgen soll, durch ein Gericht, bei Gefahr im Verzug durch die Behördenleitung angeordnet werden können. Der kurzfristige Einsatz, der die obigen Zeiten nicht überschreitet, soll (weiterhin) von der Behördenleitung angeordnet werden. Ausweislich der Gesetzesbegründung soll durch die zeitliche Beschränkung des Richtervorbehalts ein Gleichklang mit § 32 Abs. 1 BbgPolG-E hergestellt werden, damit die kurzfristigen (anordnungsfreien) Observationen vom Einsatz technischer Mittel begleitet werden können.

Ich begrüße prinzipiell, dass der Einsatz technischer Mittel schon ab einer bestimmten Dauer vom Gericht angeordnet werden muss. Bisher war es der Behördenleitung möglich, solange die Maßnahme einen Monat nicht überschritt, die Einsatzzeit technischer Mittel (unter Verhältnismäßigkeitsaspekten) selbst zu bestimmen. Durch die Einbindung des Gerichts als unabhängiger Stelle wird eine unabhängige Überprüfung der Notwendigkeit eines Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Personen erreicht.

11. § 33d BbgPolG-E: Datenerhebung durch Eingriffe in informationstechnische Systeme

Die Regelung erlaubt die Überwachung und Aufzeichnung des Telekommunikationsverkehrs (TKÜ) und Datenerhebungen durch den verdeckten Einsatz „technischer Mittel" in informationstechnischen Systemen (z. Bsp. Computer oder Smartphones). In Absatz 1 und 2 werden die Ermittlungsmethoden der sog. "Quellen-TKÜ" und der "Online-Durchsuchung" geregelt. Erstere dient dazu, Kommunikationsinhalte trotz zunehmender Nutzung internetbasierter Telekommunikation und verbreiteter Nutzung kryptographischer Verfahren zu erheben und auszuleiten. Dazu ist es erforderlich, die Daten auf dem Telekommunikationsgerät des Nutzers, also an der „Quelle" abzugreifen. Die zweite Befugnis umfasst die Erhebung sonstiger, nicht zur laufenden Telekommunikation bestimmter, personenbezogener Daten aus einem informationstechnischen System. Beide Maßnahmen sind Grundrechtseingriffe von erheblichem Gewicht in die Vertraulichkeit individueller Kommunikation (Art. 10 GG), das informationelle Selbstbestimmungsrecht sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eines informationstechnischen Systems (Art. 2 Abs.1 i.v.m. Art. 1 Abs.1 GG) dar.

Die Schwere des Eingriffs beruht darauf, dass mit der Infiltration die entscheidende Hürde genommen ist, um diese Systeme insgesamt auszuspähen, d. h. weitere auf dem System abgelegte persönlichkeitsrelevante Informationen und die Nutzung von Diensten zu erfassen. Da ein Zugriff damit Einblick in wesentliche Teile der Lebensgestaltung eines Betroffenen erlaubt und die Bildung von Verhaltens und Kommunikationsprofilen ermöglicht, hat das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) der Durchführung derartiger Maßnahmen enge Grenzen gesetzt. Der Entwurfstext des § 33d lehnt sich erkennbar an die Vorgaben des Bundesverfassungsgerichts an. Ich habe jedoch erhebliche Zweifel, ob diese umgesetzt werden können.

11.1. Absatz 1 Quellen - Telekommunikationsüberwachung (Quellen-TKÜ):

Die Quellen-TKÜ soll unter den Voraussetzungen der Wohnraumüberwachung (§ 33a Abs. 1 BbgPolG) erlaubt werden, die auch für die bereits bestehende Befugnisnorm zur Telekommunikationsüberwachung gelten. Weitere Voraussetzung ist, dass sichergestellt wird, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird und der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere in unverschlüsselter Form zu ermöglichen. Durch die Quellen-TKÜ wird aber in weitreichenderer Weise als durch die einfache Telekommunikationsüberwachung in die Grundrechte und damit in datenschutzrechtliche Belange der betroffenen Person eingegriffen. Dies wird schon allein daraus ersichtlich, dass es das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 für notwendig erachtete, explizit ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das eine Ausprägung des allgemeinen Persönlichkeitsrechts darstellt,

zu entwickeln. Denn nur so konnten Schutzlücken, verursacht durch die neuartigen Ermittlungsmethoden, geschlossen werden. Durch dieses Grundrecht soll das Interesse des Nutzers geschützt werden, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben (BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 u. a., Rn. 204). Denn die Quellen-TKÜ unterscheidet sich von der „normalen" TKÜ dadurch, dass das informationstechnische System infiltriert wird und damit die Hürde bereits genommen wurde, um das System insgesamt auszuspähen (BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 u. a., Rn. 188).

Bei der bestehenden Überwachung der Telekommunikation werden die Inhalte erfasst, ohne auf das Gerät des Nutzers zu gelangen. Zwar soll auch bei der Quellen-TKÜ ausschließlich die laufende Telekommunikation überwacht werden. Es ist aber fraglich, ob mittels der bestehenden EDV-Maßnahmen überhaupt gesichert werden kann, dass der eingesetzte Staatstrojaner nicht doch auf die im System gespeicherten Daten zugreift und damit einen stärkeren Eingriff verkörpert, als eigentlich zulässig ist. Durch die Infiltration wird das Vertrauen des Nutzers in das System erschüttert und er passt sein Nutzerverhalten dementsprechend an.[3] Darin liegt der grundrechtliche Eingriff, der datenschutzrechtlich hoch brisant ist.

11.2. Absatz 2 Online-Durchsuchung

Der Begriff der Online-Durchsuchung ist missverständlich, da die Durchsuchung im juristischen Sprachgebrauch eine offene Maßnahme ist, an der der Betroffene teilnehmen kann. Bei der sog. Online-Durchsuchung wird dagegen heimlich ein Staatstrojaner auf das informationstechnische System der betroffenen Person aufgespielt, ohne dass diese davon weiß. Dies hat eher den Charakter eines Ausspähens.[4] Die Norm, die der Online-Durchsuchung mit ihrer Eingriffsintensität am nächsten kommt, ist die akustische Wohnraumüberwachung (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 210; BT-Drs. 18/12785, S. 54). Die Online-Durchsuchung erlaubt dennoch weit einschneidendere Maßnahmen: Dadurch, dass auf ein informationstechnisches System zugegriffen wird, wird der Polizei die Möglichkeit eröffnet, auf sämtliche gespeicherte Daten zuzugreifen. Dies betrifft beispielsweise auch die zurückliegende Kommunikation der betroffenen Person, ihre gespeicherten Bilder oder Nutzungsprofile in Internetportalen. Dadurch kann ein ziemlich genaues Bild von der Persönlichkeit der betroffenen Person, das eventuell über Jahre reichen kann, erstellt werden.[5] Dies bedeutet einen fast schon existenziellen datenschutzrechtlichen Eingriff.

Im Gegensatz zur Quellen-TKÜ ist die Online-Durchsuchung auch unter den unter Abschnitt 1a des Entwurfs des Brandenburgischen Polizeigesetzes geschilderten Voraussetzungen möglich, ohne dass es sich allerdings um eine terroristische Straftat handeln muss.

---

[3] Mansdörfer, „Sicherheit und Strafverfahren", GSZ 2018, S. 45 ff.
[4] Mansdörfer a.a.O.
[5] vgl. zum Vorstehenden: Mansdörfer a.a.O.

Auch hier wird die Eingriffsschwelle weit ins Vorfeld einer konkreten Gefahr vorverlagert. Ich beziehe mich insoweit auf die oben vorgebrachte Kritik, dass der Gesetzgeber die Vorgaben des Bundesverfassungsgerichts angemessen hätte ausfüllen müssen, um Normenklarheit herbeizuführen. Die Gesetzesbegründung, dass eine weitere Konkretisierung nicht erforderlich sei, um die notwendig flexible polizeiliche Reaktion auf entsprechende Anhaltspunkte zu ermöglichen, erachte ich daher weder als ausreichend noch als richtig.

Zweifel hinsichtlich der Umsetzbarkeit der strikten Anforderungen an Eingriffe in informationstechnische Systeme lassen sich auch aus Absatz 4 der Regelung ableiten. Die Vorgabe, dass durch die Infiltration vorgenommene Veränderungen wieder rückgängig gemacht werden müssen und die ausgeleitete Kommunikation oder kopierte Daten vor Veränderungen, unbefugter Löschung oder Kenntnisnahme zu schützen sind, werden unter den Vorbehalt gestellt, dass dies nach dem Stand der Technik möglich ist. Dabei handelt es sich jedoch nicht um verhandelbare Maßgaben. Wenn nicht sichergestellt ist, dass die Anforderungen an Maßnahmen gemäß Absatz 1 und 2 zu erfüllen sind, ist ein Eingriff aus meiner Sicht unverhältnismäßig und damit verfassungswidrig.

11.3. Kernbereich

Absatz 5 Satz 4 des Entwurfs legt eine Unterbrechung der Datenerhebung fest, wenn erkennbar wird, dass in den Kernbereich privater Lebensgestaltung oder in ein geschütztes Vertrauensverhältnis eingegriffen wird. Absatz 9 regelt das weitere Verfahren, insbesondere die Verwendung der Daten. Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz erneut bestätigt, dass die Durchführung von besonders eingriffsintensiven Überwachungsmaßnahmen besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung stellt. Der Schutz dieses Kernbereichs dürfe auch nicht durch Abwägungen mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden. Vorkehrungen sind nicht nur gegen das Miterfassen von Kernbereichsinformationen auf der Ebene der Datenerhebung zu treffen, sondern auch auf der Ebene der Auswertung und Verwertung, für den Fall, dass eine Erhebung kernbereichsrelevanter Informationen nicht vermieden werden konnte. (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, Rn.124 -129). Die Sichtung der erfassten höchstpersönlichen Daten muss nicht durch eine unabhängige Stelle erfolgen, aber es muss unverzüglich, vor einer Auswertung geprüft werden, ob es sich um Daten handelt, die gelöscht werden müssen.

Ich habe Zweifel, dass die Regelung in § 33d Abs. 9 BbgPolG-E diesen Anforderungen entspricht. Die Handlungsanweisung für die Ebene der Datenerhebung (Absatz 5 Satz 4) – diese zu unterbrechen – ist klar und entspricht den Vorgaben des Gerichts. Hinsichtlich der Verwendung erhobener Daten verweist der Entwurf jedoch auf § 33b Abs. 8-11 BbgPolG. Dabei handelt es sich um spezielle Vorschriften zur einfachen Telekommunikationsüberwachung. Absatz 10 dieser Norm erlaubt die weitere Verwendung der Daten zur Abwehr einer

gegenwärtigen Gefahr für bedeutende Rechtsgüter, vorausgesetzt es wird eine richterliche Entscheidung beim Amtsgericht darüber eingeholt. Zum einen widerspricht dies der Regel, jegliche Verwendung auszuschließen, zum anderen wird nicht unmittelbar deutlich, ob die Entscheidung auch bei Gefahr im Verzuge ausschließlich durch das Gericht getroffen wird.. Aufgrund der Eingriffstiefe der Befugnis empfehle ich dringend, die wesentliche Frage des Kernbereichsschutzes normenklar in § 33d selbst zu regeln.

11.4. Benachrichtigungen

Absatz 9 der Vorschrift verweist hinsichtlich der Unterrichtung der betroffenen Person auf die grundlegende Verpflichtung, bei verdeckten Maßnahmen den Betroffenen nachträglich über die Datenerhebung zu benachrichtigen. Diese bei eingriffsintensiven Maßnahmen wesentliche Schutzvorkehrung, ist für den Anwender gesetzestechnisch unübersichtlich geregelt. Die Entwurfsfassung des §§ 33d verweist in Absatz 9 auf die entsprechende Regelung des § 33b Abs. 8 -11 BbgPolG, der wiederum auf § 29 Abs. 7 und 8 sowie § 33a Abs. 6 BbgPolG verweist. Aus Gründen der Übersichtlichkeit und Verständlichkeit empfehle ich von Kettenverweisungen Abstand zu nehmen. Sofern die Benachrichtigungspflicht nicht einzeln in jeder Norm gefasst werden soll, könnte eine Zusammenfassung aller Benachrichtigungspflichten nach dem Muster des § 74 BKAG erfolgen.

11.5. Bedenken aus technisch-organisatorischer Sicht

Quellen-TKÜ und Online-Durchsuchung sind angesichts des hohen Grundrechtseingriffs auch aus technischer und organisatorischer Sicht u. a. aus folgenden Gründen als kritisch anzusehen.

- Die Software muss auf dem IT-System der betroffenen Person aufgebracht werden. Das heimliche Aufspielen von Software auf ein IT-System erfordert eine Software-Schwachstelle des betroffenen IT-Systems. Zur Infektion werden mindestens mittlere, im Regelfall sogar schwere bis kritische Schwachstellen benötigt.[6] Es ist nicht auszuschließen, dass auch Kriminelle diese Schwachstellen nutzen könnten.

  Bekannt gewordene Schwachstellen sollten daher schnellstmöglich an die jeweiligen Hersteller übermittelt werden, damit diese entsprechende Maßnahmen ergreifen können. Ein Sammeln und Ausnutzen von Schwachstellen durch öffentliche Stellen ist unter allen Umständen zu vermeiden.

---

[6] Chaos Computer Club: Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung, Sachverständigenauskunft zum Änderungsantrag der Fraktion CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18/11272) vom 31. Mai 2017.

- Es ist nicht auszuschließen, dass aufgrund der Komplexität der eingesetzten Software diese auch Fehler enthalten kann. Dadurch wäre die Integrität des infiltrierten IT-Systems gefährdet. Eine Offenlegung des Quellcodes, öffentliche Diskussion und eine Prüfung und Zertifizierung der Überwachungssoftware durch eine unabhängige Institution sind unabdingbar.

- Die auf dem IT-System gem. Abs. 1 und 2 erfassten bzw. erhobenen Daten könnten auch durch auf dem IT-System bereits installierte Schadsoftware weiter verarbeitet bzw. versendet werden. Durch den Einsatz von kryptographischen Verfahren ist eine missbräuchliche Nutzung der erhobenen Daten zu verhindern. Die Verschlüsselungsverfahren und die entsprechenden Schlüssellängen müssen sich nach dem jeweiligen Stand der Technik richten.

- Es ist unklar, wie sich die manipulativen Eingriffe in informationstechnische Systeme auf die Gerichtsfestigkeit der Beweise auswirken. Ein wesentlicher Grundsatz der Forensik ist, Manipulationen an informationstechnischen Geräten zu verhindern. Vor jedweder Analyse ist ein Image der Datenträger zu erstellen, damit die originalen Datenträger für Beweiszwecke erhalten bleiben.

- Der externe Zugang zur Überwachungssoftware erfordert die Öffnung der Firewall und mindestens eines Netzwerk-Ports. Diese Öffnung der Netzwerkschnittstelle könnte auch von Kriminellen missbräuchlich verwendet werden. Auch dieser Zugang zur Überwachungssoftware ist mithilfe kryptographischer Verfahren zu sichern.

Das für Inneres zuständige Mitglied der Landesregierung sollte ermächtigt werden, durch Rechtsverordnung über die grundlegenden technischen und organisatorischen Anforderungen für Maßnahmen nach Absatz 1 und 2 zu bestimmen. Die technischen Einzelheiten sollten in einer technischen Richtlinie detailliert beschrieben werden.

Für die Verarbeitung personenbezogener Daten, die durch einen besonders schwerwiegenden Eingriff in Persönlichkeitsrechte Betroffener gewonnen werden, ist auf die Möglichkeit der Ad-hoc-Freigabe (Nr.5 Dateienrichtlinie-Polizei, § 48 Abs. 5 BbgPolG) zu verzichten.

Ich würde mich freuen, wenn meine Bedenken im weiteren Gesetzgebungsverfahren berücksichtigt werden. Für Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen