

## Gesetzentwurf

### der Staatsregierung

#### zur Änderung des Bayerischen Verfassungsschutzgesetzes, des Ausführungsgesetzes Art. 10-Gesetz und des Parlamentarischen Kontrollgremium-Gesetzes

##### A) Problem

1. Die präventive Wohnraumüberwachung ist ein wichtiges und unverzichtbares Instrument zur Gefahrenabwehr. Dies gilt insbesondere in Zeiten wachsender Bedrohung durch den islamistischen Terrorismus und gewisser Erscheinungsformen der Organisierten Kriminalität. Herkömmliche Befugnisse reichen für eine effektive Bekämpfung von Terrorismus und Organisierter Kriminalität nicht aus. Das Bundesverfassungsgericht hat in seinem Urteil zur repressiven Wohnraumüberwachung vom 03.03.2004 (Az.: 1 BvR 2378/98, 1 BvR 1084/99) das Instrument der Wohnraumüberwachung und den damit verbundenen Eingriff in das Grundrecht des Art. 13 Abs. 1 GG für verfassungsgemäß erklärt. Das Urteil ist ausschließlich zur repressiven Wohnraumüberwachung und zu Art. 13 Abs. 3 GG sowie zu dessen Umsetzung in der Strafprozessordnung ergangen. Gleichwohl sind hier und in anderen Entscheidungen (1 BvR 668/04 vom 27.07.2005, 2 BvR 581/01 vom 12.04.2005, 1 BvF 3/92 vom 03.03.2004, 2 BvR 543/06 vom 11.05.2007) Grundsätze entwickelt worden, die auch beim präventiven Einsatz besonderer technischer Mittel durch den Verfassungsschutz im Schutzbereich des Art. 13 GG nach Art. 6a BayVSG zu beachten sind. Dies gilt insbesondere für den Schutz des Kernbereichs privater Lebensgestaltung, einen hinreichend bestimmten und eng begrenzten Straftatenkatalog, aber auch für die Geltung grundrechtssichernder Verfahrensregelungen wie Verwendungsverbote und Kennzeichnungspflichten bei erhobenen Daten und Benachrichtigungspflichten gegenüber Betroffenen.
2. Das Landesamt für Verfassungsschutz hat besondere Auskunftsbefugnisse gegenüber Kreditinstituten, Fluggesellschaften, Post- und Telekommunikationsdienstleistern sowie Telemedienanbietern und ist berechtigt, den IMSI-Catcher einzusetzen. Eine stärker an der Praxis orientierte Gestaltung und entsprechende Erweiterung dieser Befugnisse ist geboten, nachdem die entsprechenden Befugnisse auf Bundesebene durch das Terrorismusbekämpfungsergänzungsgesetz bereits praktikabler gestaltet worden sind.
3. Eine wirksame Nachrichtenbeschaffung, gerade im Bereich der Erforschung der Bestrebungen des internationalen Terrorismus, verlangt auch die Möglichkeit eines verdeckten Zugriffs auf informationstechnische Systeme mit dem Ziel der Datenerhebung aus Speichermedien. Dies ist ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (siehe Urteil des BVerfG vom 27.02.2008, 1 BvR 370/07). Eine Eingriffsbefugnis für Fälle, in denen wegen der drohenden Gefahren auf eine Nachrichtenbeschaffung auf diesem Weg im konkreten Einzelfall nicht verzichtet werden kann, fehlt bislang.

4. Nachrichtendienstliche Mittel sind bislang aufgrund einer Generalklausel zugelassen, eine nähere Bestimmung der zugelassenen Mittel durch das Landesamt für Verfassungsschutz vor ihrer Anwendung ist bislang nicht vorgesehen.
5. Der Einsatz verdeckter technischer Mittel zum Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb des Schutzbereichs des Art. 13 GG ist bislang trotz einer im Einzelfall denkbaren potentiell großen Eingriffsintensität nicht speziell gesetzlich geregelt.
6. Die Auskunft über Datenspeicherungen an Betroffene ist im Bayerischen Verfassungsschutzgesetz zwar verfassungskonform (vgl. Urteil des Bayerischen Verfassungsgerichtshofs vom 11.11.1997 (Vg. 22-VII-94)) und im Einklang mit dieser Rechtsprechung ins Ermessen des Landesamts für Verfassungsschutz gestellt. Ein grundsätzlicher Auskunftsanspruch verbessert allerdings den Schutz der Betroffenen.
7. Nach gefestigter Verwaltungspraxis übermittelt das Bayerische Staatsministerium des Innern anstelle des Landesamts für Verfassungsschutz insbesondere in Verfassungstreue-, Ausländer- und Einbürgerungsfällen belastende Erkenntnisse des Verfassungsschutzes an die zuständigen Stellen. Soweit solche Erkenntnisse des Verfassungsschutzes durch das Staatsministerium des Innern nach nochmaliger Prüfung der Relevanz übermittelt werden sollen, fehlt bislang eine ausdrückliche gesetzliche Übermittlungsbefugnis. Für die Zukunft ist somit die Befugnis des Staatsministeriums des Innern zu entsprechenden Datenübermittlungen gesetzlich zu regeln.
8. Das Landesamt für Verfassungsschutz unterrichtet die Öffentlichkeit über verfassungsfeindliche Bestrebungen und Aktivitäten. In der Rechtsprechung wird mittlerweile teilweise in Frage gestellt, ob, ohne ausdrückliche Regelung, über Anhaltspunkte für solche Bestrebungen berichtet werden darf. Die Öffentlichkeit muss nach dem Grundsatz der wehrhaften Demokratie über verfassungsfeindliche Bestrebungen jedoch möglichst frühzeitig informiert werden.

## **B) Lösung**

1. Die Regelungen über den Einsatz besonderer technischer Mittel im Schutzbereich des Art. 13 GG werden den verfassungsrechtlichen Erfordernissen angepasst. Der Schutz des Kernbereichs privater Lebensgestaltung wird durch umfassende Vorkehrungen sichergestellt. Höchstpersönliche Gespräche mit engsten Familienangehörigen, engsten Vertrauten sowie mit Berufsgeheimnisträgern in Privatwohnungen unterliegen ebenso wie höchstpersönliche Gespräche in Räumen, die von Berufsgeheimnisträgern ausschließlich zu deren Berufsausübung benutzt werden, einem umfassenden Erhebungsverbot, es sei denn, die Vertrauten oder Berufsgeheimnisträger sind selbst Adressat der Maßnahme. Wird erkennbar, dass ein Eingriff in den Kernbereich privater Lebensgestaltung erfolgt, besteht die Verpflichtung, die laufende Maßnahme zu unterbrechen und die Aufzeichnungen unverzüglich zu löschen. Eine Verwendung dieser Daten ist grundsätzlich verboten. Die Zweckbindung der Daten wird durch eine Kennzeichnungspflicht gewährleistet. Verfahrensrechtlich wird der Schutz des Kernbereichs dadurch verstärkt, dass jede Verwertbarkeit von Daten außerhalb des eng umgrenzten Bereichs des Verfassungsschutzes auch einer richterlichen Kontrolle unterliegt. Auch bei der Zurückstellung der verfassungsrechtlich gebotenen Benachrichtigung ist eine weitergehende verfahrensrechtliche Sicherung vorgesehen.

2. Voraussetzungen und Verfahren der in Umsetzung des Terrorismusbekämpfungsgesetzes geschaffenen Auskunftsbefugnisse des Landesamts für Verfassungsschutz gegenüber Kreditinstituten, Fluggesellschaften, Post- und Telekommunikationsdienstleistern sowie Telemedienanbietern werden entsprechend dem unterschiedlichen Eingriffsgehalt differenzierter und damit bei Wahrung datenschutzrechtlicher Belange praktikabler gestaltet. Es wird unterschieden zwischen
  - Bestands- und Verkehrsdaten in den sachlichen Anordnungsvoraussetzungen sowie
  - Verkehrsdaten innerhalb und außerhalb des Schutzbereichs des Art. 10 GG im Anordnungs- und sonstigen Verfahren.

Darüber hinaus wird der bei der Beobachtungsaufgabe nach Art. 3 Abs. 1 Satz 1 Nr. 1 BayVSG bislang auf den gewaltbezogenen Inlandsextremismus begrenzte Anwendungsbereich der Auskunftsbefugnisse des Landesamts für Verfassungsschutz auch auf volksverhetzende Bestrebungen erweitert. Auskünfte zu Bestandsdaten hingegen stehen dem Landesamt für Verfassungsschutz nunmehr im gesamten Aufgabenbereich des Art. 3 Abs. 1 Satz 1 Nr. 1 BayVSG ohne weitere Beschränkung zu.

Beim Einsatz des IMSI-Catchers werden die materiellen Anordnungsvoraussetzungen gesenkt. Sein Anwendungsbereich im Aufgabenbereich des Art. 3 Abs. 1 Satz 1 Nr. 1 BayVSG wird ebenfalls auf volksverhetzende Bestrebungen erweitert.

3. Es wird eine Befugnisnorm geschaffen, für Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Landesamt für Verfassungsschutz hat danach im Einzelfall die Möglichkeit, mit technischen Mitteln verdeckt auf informationstechnische Systeme zuzugreifen, um Daten zu erheben. Die Befugnis berücksichtigt die Vorgaben des Bundesverfassungsgerichts vom 27.02.2008 (1 BvR 370/07). Maßnahmen in diesem Bereich sind wegen ihrer Eingriffsintensität an hohe materiellrechtliche Voraussetzungen geknüpft, insbesondere an das Vorliegen tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut. Sie stehen grundsätzlich unter dem Vorbehalt richterlicher Anordnung. Der Kernbereich privater Lebensgestaltung wird durch entsprechende Regelungen geschützt. Es gelten grundsätzlich die gleichen Verfahrensregelungen wie bei der Wohnraumüberwachung.
4. In Art. 6 Abs. 1 BayVSG wird normiert, dass nachrichtendienstliche Mittel künftig vorab in einer Dienstvorschrift festgelegt werden, die vom Staatsministerium des Innern zu genehmigen ist und über die das Parlamentarische Kontrollgremium unterrichtet wird. Für das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes mit verdeckten technischen Mitteln außerhalb des Schutzbereichs von Artikel 10 und 13 GG wird in Art. 6d BayVSG eine spezielle gesetzliche Regelung geschaffen. Benachrichtigungspflichten gegenüber Betroffenen werden hierfür ebenso vorgesehen wie Verwendungs- und Lösungsregelungen zum Schutz des Kernbereichs privater Lebensgestaltung. Die Auskunftsbefugnis in Art. 11 BayVSG wird umgestaltet und den Betroffenen insbesondere ein grundsätzlicher Auskunftsanspruch eingeräumt.
5. In Art. 14 Abs. 6 BayVSG wird nunmehr auch dem Staatsministerium des Innern ausdrücklich die Befugnis zur Übermittlung personenbezogener Daten nach den Abs. 1 bis 4 eingeräumt.

6. In Art. 15 BayVSG wird klarstellend geregelt, dass das Landesamt für Verfassungsschutz die Öffentlichkeit entsprechend der bisherigen Praxis bereits über tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen unterrichtet.

### **C) Alternativen**

Keine

### **D) Kosten**

#### **1. Kosten für den Staat**

Da die präventive Wohnraumüberwachung schon bislang im Bayerischen Verfassungsschutzgesetz normiert war, sind keine Kostensteigerungen zu erwarten. Zwar dürfte einerseits – bedingt durch die Komplexität der Regelungen – der Verwaltungsaufwand und damit die Kosten für die einzelne Maßnahme steigen, jedoch ist andererseits – aufgrund des engen Anwendungsbereichs – mit einem Rückgang der ohnehin geringen Fallzahlen zu rechnen. Bisher wurden nach der geltenden Regelung in Art. 6a BayVSG bis zur Entscheidung des Bundesverfassungsgerichts im Jahr 2004 ein bis drei Maßnahmen jährlich durchgeführt.

Im Bereich der Auskunftersuchen nach Art. 6c BayVSG sind Anordnungsvoraussetzungen herabgesetzt und Verfahren vereinfacht worden. Dennoch ist davon auszugehen, dass sich die Auskunftszahlen innerhalb der bisherigen Größenordnung halten werden (im Durchschnitt der letzten Jahre (2003 bis 2006) weniger als 20 Ersuchen pro Jahr), so dass keine wesentlichen zusätzlichen Kosten entstehen. Die Kosteneinsparungen durch Verfahrensvereinfachungen sind nicht näher bezifferbar.

Soweit durch die Befugnis nach Art. 6e BayVSG die Möglichkeit der verdeckten Datenerhebung aus informationstechnischen Systemen eröffnet wird, entstehen dadurch zusätzliche Kosten, deren Umfang im Einzelnen noch nicht abschätzbar ist. Nachdem solche Maßnahmen jedoch auf wenige Einzelfälle im Jahr beschränkt sein werden, ist nicht damit zu rechnen, dass eine Größenordnung erreicht wird, die den Haushalt des Landesamts für Verfassungsschutz maßgeblich beeinflusst.

Sonstige Änderungen und Ergänzungen führen zu keinen zusätzlichen Kosten, soweit sie lediglich eine bereits bisher geltende Verwaltungspraxis im Gesetz verankern oder redaktioneller Art sind. Die neu geschaffenen Schutzvorkehrungen und Rechte beim Einsatz verdeckter Mittel zum Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes können – abhängig von der künftigen Fallzahl solcher Maßnahmen – zwar zu einer gewissen Erhöhung des Verwaltungsaufwands führen, der aber mit den vorhandenen Ressourcen abzudecken ist.

Die Normierung der Kostenfreiheit von Auskünften an Betroffene führt zu keinen Einnahmeausfällen, da bereits bisher in der Praxis keine Kosten erhoben werden.

## **2. Kosten für die Kommunen**

Gemeinden sind von diesem Gesetz nicht betroffen.

## **3. Kosten für Wirtschaft und Bürger**

Die schon bisher bestehenden Informationspflichten, nach denen Luftfahrtunternehmen, Kreditinstitute, Postdienstleistungsunternehmen, Telekommunikationsunternehmen und Telemediendienstleister, unentgeltlich Auskunft zu erteilen haben, werden geändert (Art. 6c und 6f BayVSG). Die Änderung beinhaltet ein erleichtertes Anordnungsverfahren und eine teilweise Absenkung der materiellen Anordnungsvoraussetzungen. Es ist jedoch davon auszugehen, dass sich die Auskunftersuchen wie bisher auf wenige Einzelfälle beschränken. Im Jahr 2006 gab es ausschließlich Auskunftersuchen gegenüber sechs Kreditinstituten in fünf Fällen. Im Jahr 2005 gab es Auskunftersuchen gegenüber zwei Kreditinstituten in zwei Fällen und gegenüber einem Telekommunikationsunternehmen in einem Fall und im Jahr 2004 waren es Auskunftersuchen gegenüber acht Kreditinstituten in fünf Fällen, gegenüber zwei Fluggesellschaften in zwei Fällen und gegenüber fünf Telekommunikationsunternehmen in drei Fällen (vgl. LT-Drs. 15/8206, 15/4573 und 15/3402). Die auch künftig hierfür zu erwartenden Bürokratiekosten sind in Anbetracht der äußerst geringen Fallzahlen marginal.



## Gesetzentwurf

### zur Änderung des Bayerischen Verfassungsschutzgesetzes, des Ausführungsgesetzes Art. 10-Gesetz und des Parlamentarischen Kontrollgremium-Gesetzes

#### § 1

#### Änderung des Bayerischen Verfassungsschutzgesetzes

Das Bayerische Verfassungsschutzgesetz (BayVSG) in der Fassung der Bekanntmachung vom 10. April 1997 (GVBl S. 70, BayRS 12-1-I), zuletzt geändert durch § 1 des Gesetzes vom 24. Dezember 2002 (GVBl S. 969), wird wie folgt geändert:

1. Art. 6 wird wie folgt geändert:
  - a) Abs. 1 wird wie folgt geändert:
    - aa) In Satz 1 wird der Punkt durch einen Strichpunkt ersetzt und folgender Halbsatz angefügt:  
„besondere gesetzliche Regelungen bleiben unberührt“
    - bb) Es werden folgender neuer Satz 4 und folgender Satz 5 eingefügt:  
„<sup>4</sup>Die nachrichtendienstlichen Mittel sind in einer Dienstvorschrift zu benennen, in der auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen zu regeln ist. <sup>5</sup>Die Dienstvorschrift bedarf der Zustimmung des Staatsministeriums des Innern, das das Parlamentarische Kontrollgremium unterrichtet.“
    - cc) Der bisherige Satz 4 wird Satz 6.
  - b) Abs. 4 wird aufgehoben.
1. Art. 6a und 6b erhalten folgende Fassung:

„Art. 6a  
Einsatz technischer Mittel im  
Schutzbereich des Art. 13 Grundgesetz

(1) Das Landesamt für Verfassungsschutz darf technische Mittel im Schutzbereich des Art. 13 des Grundgesetzes als nachrichtendienstliche Mittel im Sinn des Art. 6 Abs. 1 unter besonderer Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach Art. 6 Abs. 3 nur unter den nachfolgenden Voraussetzungen einsetzen.

(2) <sup>1</sup>Maßnahmen nach Abs. 1 sind nur zulässig, sofern tatsächliche Anhaltspunkte für den Verdacht vorliegen, dass jemand Bestrebungen oder Tätigkeiten der dort

genannten Art durch die Planung oder Begehung von Straftaten verfolgt, die im Einzelfall geeignet sind, den Bestand oder die Sicherheit des Bundes oder eines Landes oder in erheblichem Maße Leib, Leben oder Freiheit von Personen zu gefährden. <sup>2</sup>Solche Straftaten sind:

1. Straftaten des Friedensverrats, Hochverrats und Landesverrats (§§ 80, 81, 82, 94 Strafgesetzbuch - StGB),
  2. Bildung und Unterstützung einer kriminellen oder terroristischen Vereinigung (§ 129 Abs. 1 in Verbindung mit Abs. 4, §§ 129a, 129b StGB),
  3. Straftaten gegen das Leben (§§ 211, 212 StGB, § 6 Völkerstrafgesetzbuch),
  4. Straftaten gegen die persönliche Freiheit (§§ 232, 233, 233a Abs. 2, §§ 234, 234a Abs. 1, §§ 239a, 239b StGB),
  5. Gemeingefährliche Straftaten in den Fällen der §§ 306a, 306b, 307 Abs. 1 und Abs. 2, § 308 Abs. 1, § 309 Abs. 1, § 310 Abs. 1, § 313 Abs. 1, § 314 Abs. 1, § 315 Abs. 3, § 315b Abs. 3, § 316c StGB und
  6. Straftaten nach dem Waffengesetz (WaffG) und dem Gesetz über die Kontrolle von Kriegswaffen (§ 51 Abs. 1 in Verbindung mit Abs. 2, § 52 Abs. 1 Nr. 1 in Verbindung mit Abs. 5 WaffG; § 19 Abs. 2, § 20 Abs. 1, jeweils auch in Verbindung mit § 21 des Gesetzes über die Kontrolle von Kriegswaffen; § 22a Abs. 1 in Verbindung mit Abs. 2 des Gesetzes über die Kontrolle von Kriegswaffen).
- (3) <sup>1</sup>Maßnahmen nach Abs. 1 sind nur zulässig, wenn und soweit
1. die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und
  2. für den Fall, dass zu privaten Wohnzwecken genutzte Räumlichkeiten betroffen sind, in denen sich die Person, gegen die sich die Maßnahme richtet, allein oder ausschließlich mit engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsheimlichkeitsgeheimnisträgern nach §§ 53, 53a der Strafprozessordnung (StPO) in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl I S. 1074, 1319) in der jeweils geltenden Fassung aufhält,
    - a) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gespräche geführt werden, die einen unmittelbaren Bezug zu den im

Abs. 2 genannten Bestrebungen oder Tätigkeiten haben, ohne dass ein Gesprächsteilnehmer über ihren Inhalt das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigern könnte, oder

b) die Maßnahme sich auch gegen die Familienangehörigen, Vertrauten oder Berufsgeheimnisträger richtet, und

3. für den Fall, dass sich die Maßnahme gegen einen Berufsgeheimnisträger nach §§ 53, 53a StPO selbst richtet und die zu seiner Berufsausübung bestimmten Räumlichkeiten betroffen sind, die Voraussetzungen der Nr. 2 Buchst. a vorliegen.

<sup>2</sup>In den Fällen des Satzes 1 Nrn. 2 und 3 ist eine nur automatische Aufzeichnung zulässig, wenn bei Anordnung der Maßnahme abzusehen ist, dass keine Gespräche geführt werden, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind; wird bei einer Maßnahme nach Abs. 1 erkennbar, dass solche Gespräche geführt werden, ist die Datenerhebung unverzüglich und so lange erforderlich zu unterbrechen.

(4) <sup>1</sup>Maßnahmen nach Abs. 1 dürfen im Fall des Abs. 3 Satz 1 Nr. 2 nur in Wohnungen des in der Anordnung bezeichneten Adressaten durchgeführt werden. <sup>2</sup>In Wohnungen anderer Personen sind die Maßnahmen zulässig, wenn es nicht Wohnungen von Berufsgeheimnisträgern nach §§ 53, 53a StPO sind und auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der Adressat sich dort aufhält und
2. die Maßnahme in Wohnungen des Adressaten allein zur Erforschung des Sachverhalts nicht möglich oder nicht ausreichend ist.

<sup>3</sup>Die Erhebung personenbezogener Daten über andere als die in Satz 1 genannten Personen ist zulässig, soweit sie unvermeidliche Folge einer Maßnahme nach Abs. 1 ist.

Art. 6b  
Verfahrensregelungen für  
Maßnahmen nach Art. 6a

(1) <sup>1</sup>Der Einsatz technischer Mittel nach Art. 6a bedarf einer richterlichen Anordnung auf Antrag des Präsidenten des Landesamts für Verfassungsschutz oder dessen Stellvertreters. <sup>2</sup>Bei Gefahr im Verzug kann der Präsident des Landesamts für Verfassungsschutz oder dessen Vertreter die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen. <sup>3</sup>In der schriftlichen Anordnung sind Adressat, Art, Umfang und Dauer der Maßnahme zu bestimmen und die wesentlichen Gründe zu benennen. <sup>4</sup>Die Anordnung ist auf längstens einen Monat zu befristen; Verlängerungen um jeweils nicht mehr als einen Monat sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung

fortbestehen. <sup>5</sup>Liegen die Voraussetzungen nicht mehr vor oder ist der verdeckte Einsatz technischer Mittel nicht mehr erforderlich, so ist die Maßnahme ungeachtet des in der Anordnung genannten Zeitraums unverzüglich zu beenden. <sup>6</sup>Die Beendigung ist dem Richter mitzuteilen. <sup>7</sup>Ein Bediensteter des Landesamts für Verfassungsschutz mit Befähigung zum Richteramt beaufsichtigt den Vollzug der Anordnung und eventuelle Datenübermittlungen.

(2) <sup>1</sup>Die durch Maßnahmen nach Art. 6a erhobenen Daten sind als solche zu kennzeichnen. <sup>2</sup>Nach einer Übermittlung hat der Empfänger die Kennzeichnung aufrecht zu erhalten; darauf ist dieser hinzuweisen. <sup>3</sup>Daten aus Maßnahmen nach Art. 6a dürfen nur verwendet werden

1. zur Abwehr und Aufklärung der in Art. 6a Abs. 2 genannten Gefahren,
2. zur Verfolgung von Straftaten, wenn die Voraussetzungen der Strafprozessordnung für die Datenerhebung bei der Erhebung vorgelegen haben und bei der Übermittlung noch vorliegen,
3. zur Abwehr dringender Gefahren für Leib, Leben oder Freiheit von Menschen.

<sup>4</sup>Das Landesamt für Verfassungsschutz prüft unverzüglich und dann in Abständen von sechs Monaten, ob die durch Maßnahmen nach Art. 6a erhobenen personenbezogenen Daten allein oder zusammen mit bereits vorliegenden Daten für die Zwecke des Satzes 3 erforderlich sind. <sup>5</sup>Daten, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder
3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art 6a Abs. 2 genannten Bestrebungen oder Tätigkeiten haben,

dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. <sup>6</sup>Über eine Verwendung der Daten nach Satz 5 oder eine Übermittlung von Daten aus einer Maßnahme nach Art. 6a an Stellen außerhalb des Verbunds der Verfassungsschutzbehörden entscheidet der Richter. <sup>7</sup>Bei Gefahr im Verzug kann die Entscheidung auch der Präsident des Landesamts für Verfassungsschutz oder dessen Vertreter treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen.

(3)<sup>1</sup>Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen. <sup>2</sup>Die durch eine Maßnahme nach Art. 6a Abs. 1 erlangten personenbezogenen Daten, deren Verwendung zu den in Abs. 2 Satz 3 genannten Zwecken nicht erforderlich ist oder für die ein Verwendungsverbot besteht, sind unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen; soweit die Daten für eine Mitteilung an den Betroffenen oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme von Bedeutung sein können, sind sie zu sperren. <sup>3</sup>Die gesperrten Daten dürfen nur zu den in Satz 2 Halbsatz 2 genannten Zwecken verwendet werden. <sup>4</sup>Im Fall der Mitteilung an den Betroffenen sind die Daten erst zu löschen, wenn der Betroffene nach Ablauf eines Monats nach seiner Benachrichtigung keine Klage erhebt; auf diese Frist ist in der Mitteilung hinzuweisen. <sup>5</sup>Im Fall einer gerichtlichen Überprüfung sind die Daten nach deren Abschluss zu löschen. <sup>6</sup>Die Löschung von Daten ist zu protokollieren.

(4) <sup>1</sup>Das Landesamt für Verfassungsschutz teilt den in der Anordnung bezeichneten Personen sowie denjenigen, deren personenbezogene Daten erhoben und zu den Zwecken des Abs. 2 Satz 3 verwendet wurden, Maßnahmen nach Art. 6a Abs. 1 nach ihrer Einstellung, frühestens jedoch dann mit, wenn eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. <sup>2</sup>Erfolgt die Mitteilung nicht binnen sechs Monaten nach Einstellung der Maßnahmen, bedarf ihre weitere Zurückstellung der richterlichen Zustimmung. <sup>3</sup>Dem Gericht sind die Gründe mitzuteilen, die einer Mitteilung an den Betroffenen entgegenstehen. <sup>4</sup>Die richterliche Entscheidung ist jeweils nach einem Jahr erneut einzuholen, wenn das Gericht keine andere Frist bestimmt. <sup>5</sup>Eine Mitteilung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn

1. überwiegende Interessen eines Betroffenen entgegenstehen,
2. die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann oder
3. die Voraussetzungen für eine Mitteilung auch nach fünf Jahren nach Beendigung der Maßnahme nicht eingetreten sind, sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden und die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch beim Empfänger der Daten vorliegen.

(5) <sup>1</sup>Der verdeckte Einsatz technischer Mittel im Schutzbereich des Art. 13 des Grundgesetzes ausschließlich zum Schutz der für den Verfassungsschutz in diesem Bereich tätigen Personen bedarf der Anordnung des Präsidenten des Landesamts für Verfassungsschutz oder eines von ihm bestellten Beauftragten. <sup>2</sup>Eine anderweitige Verwendung der hierbei erlangten Erkenntnisse ist nur zulässig, wenn zuvor der Richter

festgestellt hat, dass die Maßnahme rechtmäßig ist und die Voraussetzungen des Art. 6a Abs. 2 vorliegen; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. <sup>3</sup>Soweit Erkenntnisse verwendet werden, gelten für die Datenverarbeitung, die Löschung der Daten und die Mitteilung an den Betroffenen Abs. 2 bis 4 entsprechend. <sup>4</sup>Im Übrigen sind die Daten unverzüglich zu löschen.

(6) <sup>1</sup>Zuständiges Gericht zur Entscheidung nach den Abs. 1, 2, 4 und 5 ist das Amtsgericht am Sitz des Landesamts für Verfassungsschutz. <sup>2</sup>Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit (BGBl III 315-1), zuletzt geändert durch Art. 10 des Gesetzes vom 12. Dezember 2007 (BGBl I S. 2840), entsprechend.

(7) <sup>1</sup>Die Staatsregierung unterrichtet den Landtag jährlich über die gemäß Art. 6a und, soweit richterlich überprüfungsbedürftig, nach Abs. 5 angeordneten Maßnahmen. <sup>2</sup>Das Parlamentarische Kontrollgremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus.“

2. Es werden folgende Art. 6c bis 6h eingefügt:

„Art. 6c  
Besondere Auskunftsersuchen und  
Einsatz technischer Mittel zur Ortung  
von Mobilfunkendgeräten

(1) <sup>1</sup>Das Landesamt für Verfassungsschutz darf im Einzelfall bei denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder Telemedien anbieten oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien gespeichert worden sind, soweit dies zur Erfüllung der Aufgaben nach Art. 3 Abs. 1 Satz 1 erforderlich ist. <sup>2</sup>Die Verpflichteten haben die Auskunft unentgeltlich zu erteilen.

(2) <sup>1</sup>Das Landesamt für Verfassungsschutz darf im Einzelfall auch im Rahmen des § 113a des Telekommunikationsgesetzes (TKG) vom 22.06.2004 (BGBl I S. 1190) in der jeweils geltenden Fassung Auskunft einholen bei

1. Luftfahrtunternehmen zu Namen und Anschriften von Kunden sowie zu Inanspruchnahme und Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg,
2. Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhaber und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und über Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge,
3. denjenigen, die geschäftsmäßig Postdienstleistungen erbringen und daran mitwirken, zu den Umständen des Postverkehrs,

4. denjenigen, die geschäftsmäßig Telekommunikationsdiensten erbringen oder daran mitwirken, zu Verkehrsdaten nach § 96 Abs. 1 Nrn. 1 bis 4 TKG und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten und
5. denjenigen, die geschäftsmäßig Telemedien anbieten oder daran mitwirken, über
  - a) Merkmale zur Identifikation des Nutzers von Telemedien,
  - b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und
  - c) Angaben über die vom Nutzer in Anspruch genommenen Telemedien,

soweit dies zur Erfüllung der Aufgaben nach Art. 3 Abs. 1 Satz 1 erforderlich ist und tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für die in Art. 3 Abs. 1 genannten Schutzgüter vorliegen.<sup>2</sup> Im Fall des Art. 3 Abs. 1 Satz 1 Nr. 1 gilt dies nur für Bestrebungen, die bezwecken oder auf Grund ihrer Wirkungsweise geeignet sind,

1. zu Hass- oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumdungen anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder
2. Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, auch durch Unterstützen von Vereinigungen, die Anschläge gegen Personen oder Sachen veranlassen, befürworten oder androhen.

<sup>3</sup>Die Verpflichteten haben die Auskunft unentgeltlich zu erteilen.

(3) Auskünfte nach Abs. 2 dürfen nur über Personen eingeholt werden, bei denen

1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegenden Gefahren nach Abs. 2 fördern, oder
2. auf Grund bestimmter Tatsachen anzunehmen ist
  - a) bei Auskünften nach Abs. 2 Satz 1 Nrn. 1, 2 und 5, dass sie die Leistung für eine Person nach Nr. 1 in Anspruch nehmen, oder
  - b) bei Auskünften nach Abs. 2 Satz 1 Nr. 3 und 4, dass sie für eine Person nach Nr. 1 bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben oder im Fall des Abs. 2 Satz 1 Nr. 4, dass eine Person nach Nr. 1 ihre Kommunikationseinrichtung benutzt.

(4)<sup>1</sup>Das Landesamt für Verfassungsschutz darf im Einzelfall unter den Voraussetzungen des Abs. 2 auch

technische Mittel zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts oder zur Ermittlung der Geräte- und Kartennummern einsetzen.<sup>2</sup> Die Maßnahme ist nur zulässig, wenn ohne die Ermittlung die Erreichung des Zwecks der Überwachungsmaßnahme aussichtslos oder wesentlich erschwert wäre.<sup>3</sup> Sie darf sich nur gegen die in Abs. 3 Nrn. 1 und 2 Buchst. b bezeichneten Personen richten.<sup>4</sup> Personenbezogene Daten eines Dritten dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Satz 1 unvermeidbar ist.<sup>5</sup> Sie unterliegen einem absoluten Verwendungsverbot und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

#### Art. 6d

#### Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes

Das Landesamt für Verfassungsschutz darf außerhalb von Wohnungen und außerhalb des Anwendungsbereichs des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) vom 26. Juni 2001 (BGBl I S. 1254,2298) in der jeweils geltenden Fassung das nichtöffentlich gesprochene Wort unter besonderer Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach Art. 6 Abs. 3 mit dem verdeckten Einsatz technischer Mittel abhören und aufzeichnen.

#### Art. 6e

#### Verdeckte Online-Datenerhebung

(1)<sup>1</sup>Das Landesamt für Verfassungsschutz kann bei Vorliegen tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut unter den Voraussetzungen des Art. 6a Abs. 2 im Einzelfall mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben.<sup>2</sup> Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.<sup>3</sup> Sie darf sich nur gegen Verdächtige und ihre Nachrichtenmittler richten.<sup>4</sup> Gegen Nachrichtenmittler darf sich die Maßnahme nur insoweit richten, als sie kein Recht zur Verweigerung des Zeugnisses nach den §§ 53, 53a StPO haben.<sup>5</sup> Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, ist die Maßnahme insoweit unzulässig, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst oder ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich.<sup>6</sup> Soweit informationstechnisch und ermittlungstechnisch möglich, sind alle Maßnahmen zu ergreifen, mit denen die Erhebung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, vermieden werden kann.<sup>7</sup> Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die weitere Datenerhebung insoweit unzulässig.

(2) <sup>1</sup>Zur Vorbereitung einer Maßnahme nach Abs. 1 dürfen auch technische Mittel eingesetzt werden, um spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln. <sup>2</sup>Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, soweit dies aus technischen Gründen unvermeidbar ist. <sup>3</sup>Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen.

#### Art. 6f Verfahrensvorschriften

(1) <sup>1</sup>Maßnahmen nach Art. 6c Abs. 4 sowie Auskünfte nach Art. 6c Abs. 2 bedürfen eines Antrags, der durch den Präsidenten des Landesamts für Verfassungsschutz oder seinen Vertreter schriftlich zu stellen und zu begründen ist. <sup>2</sup>Über den Antrag entscheidet das Staatsministerium des Innern.

(2) <sup>1</sup>Die Anordnung einer Maßnahme nach Art. 6c Abs. 4 sowie eines Auskunftersuchens nach Art. 6c Abs. 2 über künftig anfallende Daten ist auf höchstens drei Monate zu befristen. <sup>2</sup>Eine Verlängerung um jeweils nicht mehr als drei Monate ist auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. <sup>3</sup>Anordnungen über Auskunftersuchen nach Art. 6c Abs. 2 sind dem Verpflichteten insoweit schriftlich mitzuteilen, als dies erforderlich ist, um ihm die Erfüllung seiner Verpflichtung zu ermöglichen. <sup>4</sup>Das Auskunftersuchen und die übermittelten Daten darf der Verpflichtete dem Betroffenen oder Dritten nicht mitteilen.

(3) <sup>1</sup>Im Fall der Anordnung eines Auskunftersuchens nach Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5 sowie bei Maßnahmen nach Art. 6c Abs. 4 unterrichtet das Staatsministerium des Innern monatlich die nach Art. 2 des Ausführungsgesetzes Art. 10-Gesetz (AGG 10) gebildete Kommission über die Anordnungen vor deren Vollzug. <sup>2</sup>Bei Gefahr im Verzug kann es den Vollzug der Anordnung auch bereits vor der Unterrichtung der Kommission anordnen. <sup>3</sup>Die Kommission prüft von Amts wegen oder auf Grund von Beschwerden, ob die Anordnung zulässig und notwendig ist. <sup>4</sup>§ 15 Abs. 5 G 10 ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der nach Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5 und Abs. 4 erlangten personenbezogenen Daten erstreckt. <sup>5</sup>Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt hat, hat das Staatsministerium des Innern unverzüglich aufzuheben. <sup>6</sup>Die Daten unterliegen in diesem Fall einem absoluten Verwendungsverbot und sind unverzüglich zu löschen. <sup>7</sup>Für die Verarbeitung der erhobenen Daten ist § 4 G 10 entsprechend anzuwenden. <sup>8</sup>Für die Mitteilung an den Betroffenen finden § 12 Abs. 1 und 3 G 10 entsprechende Anwendung.

(4) <sup>1</sup>Die Erhebung und Verwendung von Daten nach Art. 6d bedarf der Genehmigung des Präsidenten des Landesamts für Verfassungsschutz oder seines Stellvertreters. <sup>2</sup>Soweit bei Maßnahmen nach Art. 6d Daten er-

hoben wurden, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder
3. sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 6c Abs. 2 genannten Bestrebungen oder Tätigkeiten haben,

dürfen sie nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. <sup>3</sup>Über eine Verwendung der Daten im Sinn des Satzes 2 Halbsatz 2 entscheidet die nach Art. 2 AGG 10 gebildete Kommission. <sup>4</sup>Bei Gefahr im Verzug kann die Entscheidung auch der Präsident des Landesamts für Verfassungsschutz oder dessen Vertreter treffen; in diesem Fall ist eine Entscheidung der Kommission unverzüglich nachzuholen. <sup>5</sup>Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen. <sup>6</sup>Sofern bei Maßnahmen nach Art. 6d Daten gemäß Satz 2 verwendet werden, sind sie zu kennzeichnen und die Maßnahmen dem Betroffenen in entsprechender Anwendung des § 12 Abs. 1 und 3 G 10 mitzuteilen.

(5) <sup>1</sup>Bei Maßnahmen nach Art. 6e gelten Art. 6b Abs. 1 bis 4 und 6 entsprechend. <sup>2</sup>Die schriftliche Anordnung der Maßnahme muss, soweit möglich Namen und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, sowie die Bezeichnung des informationstechnischen Systems, auf das zugegriffen werden soll, enthalten und ist bei der erstmaligen Anordnung abweichend von Art. 6b Abs. 1 Satz 4 auf höchstens drei Monate zu befristen. <sup>3</sup>Bestehen bei der Durchsicht der Daten Anhaltspunkte dafür, dass Daten

1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind oder
2. Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder
3. einem Vertrauensverhältnis mit anderen Berufsheimnisträgern zuzuordnen sind

sind diese unverzüglich zu löschen oder dem zuständigen Richter zur Entscheidung über die weitere Verwendung vorzulegen. <sup>4</sup>Art. 6b Abs. 2 Satz 7 und Art. 6b Abs. 6 gelten im Fall des Satzes 4 entsprechend.

Art. 6g  
Notwendige Begleitmaßnahmen

<sup>1</sup>Zur Durchführung von Maßnahmen nach Art. 6a und 6e Abs. 1 und 2 kann das Landesamt für Verfassungsschutz verdeckt Sachen durchsuchen sowie die Wohnung des Betroffenen ohne Einwilligung betreten und durchsuchen. <sup>2</sup>Für die Anordnung dieser Begleitmaßnahmen und die Unterrichtung der Betroffenen finden die für die Maßnahmen nach Art. 6a und 6e Abs. 1 und 2 jeweils geltenden Vorschriften entsprechende Anwendung. <sup>3</sup>Zur Durchführung von Maßnahmen nach dem Artikel 10-Gesetz, kann das Landesamt für Verfassungsschutz verdeckt Sachen durchsuchen sowie bei Vorliegen einer dringenden Gefahr für die öffentliche Sicherheit und Ordnung die Wohnung des Betroffenen ohne Einwilligung betreten und durchsuchen. <sup>4</sup>Für die Anordnung dieser Begleitmaßnahme und die Unterrichtung der Betroffenen finden die für Maßnahmen nach Art. 6e geltenden Vorschriften entsprechende Anwendung.

Art. 6h  
Information des  
Parlamentarischen Kontrollgremiums

(1) <sup>1</sup>Das Staatsministerium des Innern unterrichtet im Abstand von höchstens sechs Monaten das Parlamentarische Kontrollgremium nach dem Parlamentarischen Kontrollgremium-Gesetz über die Durchführung von Auskunftersuchen und Maßnahmen nach Art. 6c Abs. 2 und Abs. 4 sowie in jährlichem Abstand über die Datenerhebung nach Art. 6e und, sofern diese Daten länger als sechs Monate gespeichert wurden, nach Art. 6d; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen nach Art. 6c Abs. 2 zu geben. <sup>2</sup>Das Gremium erstattet dem Landtag jährlich einen Bericht über die Durchführung sowie Art, Umfang und Anordnungsgründe der Auskunftersuchen und Maßnahmen nach Art. 6c Abs. 2, 4 und Art. 6e. <sup>3</sup>Die Grundsätze des Art. 2 Abs. 1 PKGG sind zu beachten.

(2) Das Staatsministerium des Innern erstattet dem Parlamentarischen Kontrollgremium des Bundes jährlich einen Bericht nach § 8a Abs. 8 des Bundesverfassungsschutzgesetzes über die Durchführung des Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen nach Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5 zu geben.“

3. Art. 9 Abs. 1 wird wie folgt geändert:

a) Es wird folgender neuer Satz 3 eingefügt:

„<sup>3</sup>Werden in der automatisierten Datei personenbezogene Daten verarbeitet, die der Kontrolle der nach Art. 2 AGG 10 gebildeten Kommission unterliegen, ist die Errichtungsanordnung auch der Kommission mitzuteilen.“

b) Der bisherige Satz 3 wird Satz 4.

4. Art. 11 Abs. 1 erhält folgende Fassung:

„(1) <sup>1</sup>Das Landesamt für Verfassungsschutz erteilt dem Betroffenen auf Antrag kostenfrei Auskunft über die zu seiner Person in Dateien oder Akten gespeicherten Daten. <sup>2</sup>Die Auskunftsverpflichtung besteht nur, soweit der Betroffene ein besonderes Interesse an einer Auskunft darlegt. <sup>3</sup>Sie erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen. <sup>4</sup>Das Landesamt für Verfassungsschutz bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.“

5. Art. 14 wird wie folgt geändert:

a) In Abs. 1 Satz 4 wird das Wort „Übermittlung“ durch das Wort „Weitergabe“ ersetzt.

b) Es wird folgender Abs. 6 angefügt:

„(6) Zur Übermittlung personenbezogener Daten nach Abs. 1 bis 4 ist unter den dort genannten Voraussetzungen auch das Staatsministerium des Innern befugt.“

6. In Art. 15 Satz 1 werden nach den Worten „die Öffentlichkeit über“ die Worte „tatsächliche Anhaltspunkte für“ eingefügt.

## § 2

### Änderung des Ausführungsgesetzes Art. 10-Gesetz

Art. 4 des Gesetzes über die Aufgaben der G 10-Kommission im Bayerischen Landtag und zur Ausführung des Art. 10-Gesetzes – G 10 (Ausführungsgesetz Art. 10-Gesetz – AGG 10) vom 11. Dezember 1984 (GVBl S. 522, BayRS 12-2-I), zuletzt geändert durch § 2 des Gesetzes vom 24. Dezember 2002 (GVBl S. 969), erhält folgende Fassung:

„Art. 4

Bei Wahrnehmung der in Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5, Abs. 4 und Art. 6d des Bayerischen Verfassungsschutzgesetzes (BayVSG) geregelten Befugnisse durch das Landesamt für Verfassungsschutz hat die Kommission die in Art. 6f Abs. 3 und 4 BayVSG bezeichneten Aufgaben bzw. Mitwirkungsrechte.“

## § 3

### Änderung des Parlamentarischen Kontrollgremium-Gesetzes

Das Gesetz zur parlamentarischen Kontrolle der Staatsregierung hinsichtlich der Maßnahmen nach Art. 13 Abs. 3 bis 5 des Grundgesetzes sowie der Tätigkeit des Landesamts für Verfassungsschutz (Parlamentarisches Kontrollgremium-Gesetz – PKGG) vom 10. Februar 2000 (GVBl S. 40, BayRS 12-4-I), zuletzt geändert durch § 2 des Gesetzes vom 24. Dezember 2005 (GVBl S. 641), wird wie folgt geändert:

1. In Art. 1 Abs. 1 Satz 1 werden die Worte „Art. 6a Abs. 8“ durch die Worte „Art. 6b Abs. 7“ ersetzt und die Worte „in der Fassung der Bekanntmachung vom 10. April 1997 (GVBl S. 70, BayRS 12-1-I), zuletzt geändert durch Art. 4 Abs. 1 des Gesetzes vom 10. Februar 2000 (GVBl S. 40)“ gestrichen.
2. Art. 3 wird wie folgt geändert:
  - a) In Abs. 2 Satz 1 werden die Worte „Art. 6a Abs. 8“ durch die Worte „Art. 6b Abs. 7“ ersetzt.
  - b) In Abs. 4 Satz 1 werden nach den Worten „des Art. 10-Gesetzes – G 10“ ein Komma und die Worte „nach Maßgabe des Art. 6 Abs. 1 BayVSG“ eingefügt und werden die Worte „Art. 6b Abs. 3 und 4“ durch die Worte „Art. 6h“ ersetzt.

#### § 4

##### Einschränkung von Grundrechten

Auf Grund dieses Gesetzes können das Brief-, Post- und Fernmeldegeheimnis (Art. 10 des Grundgesetzes und Art. 112 der Verfassung) sowie das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 des Grundgesetzes und Art. 106 Abs. 3 der Verfassung) eingeschränkt werden.

#### § 5

##### Inkrafttreten

Dieses Gesetz tritt am ..... in Kraft.

##### Begründung:

###### A) Allgemeines

1. Die präventive Wohnraumüberwachung ist ein unverzichtbares Instrument zur Gefahrenabwehr. Sie erlaubt es, auch dann Informationen zu gewinnen, wenn Täter nach außen abgedeckt handeln. Das ist vor allem wichtig bei der Bekämpfung von Terrorismus und Organisierter Kriminalität. Terroristen und Organisierte Kriminelle agieren in hohem Maß konspirativ und nach außen abgeschottet. Herkömmliche Befugnisse reichen daher häufig nicht aus, um in die Strukturen und den inneren Kreis solcher krimineller Organisationen einzudringen. Dies ist jedoch unerlässlich, um die Absichten der Täter rechtzeitig erkennen und die Begehung weiterer Straftaten verhindern zu können. Das Bundesverfassungsgericht hat in seinem Urteil vom 03.03.2004 zur repressiven Wohnraumüberwachung (Az.: 1 BvR 2378/98, 1 BvR 1084/99) das Instrument der Wohnraumüberwachung und den damit verbundenen Eingriff in das Grundrecht aus Art. 13 Abs. 1 GG im Grundsatz für verfassungsmäßig erklärt. Die Entscheidung ist ausschließlich zu Art. 13 Abs. 3 GG sowie dessen Umsetzung in der Strafprozessordnung (§§ 100c ff. StPO) ergangen. Verfahrensgegenstand war damit die repressive Wohnraumüberwachung und nicht der Bereich der Gefahrenabwehr. Das Bundesverfassungsgericht entwickelte jedoch in dieser und

weiteren Entscheidungen (1 BvR 668/04 vom 27.07.2005, 2 BvR 581/01 vom 12.04.2005, 1 BvF 3/92 vom 03.03.2004) Grundsätze für Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung und den Schutz des Kernbereichs privater Lebensgestaltung, die auch für den präventiven Einsatz besonderer technischer Mittel im Schutzbereich des Art. 13 GG nach Art. 6a BayVSG zu beachten sind und eine Neufassung der Befugnisnorm erforderlich machen.

Dabei ist allerdings zu berücksichtigen, dass der Prävention von schwerwiegenden Straftaten im Vergleich zur Strafverfolgung bei einer Abwägung der geschützten Rechtsgüter grundsätzlich ein höheres verfassungsrechtliches Gewicht zukommt. In der Prävention geht es um die Verhinderung von Rechtsgutbeeinträchtigungen. Während im Bereich der Strafverfolgung die Straftat bereits begangen und das Rechtsgut bereits beeinträchtigt worden ist, ist im Bereich der Prävention die Straftat noch zu verhindern, im Extremfall das Leben noch zu retten. Auch die Betrachtung des unterschiedlichen Wortlauts der verfassungsrechtlichen Regelungen in Art. 13 Abs. 3 und Abs. 4 GG legt einen unterschiedlichen Maßstab der Maßnahmen nahe. Während Art. 13 Abs. 3 GG für die repressive Wohnraumüberwachung den Verdacht besonders schwerer durch Gesetz einzeln bestimmter Straftaten verlangt, reicht für die präventive Wohnraumüberwachung nach Art. 13 Abs. 4 GG eine – wenn auch dringende – Gefahr für die öffentliche Sicherheit aus.

Der Menschenwürdegehalt des Art. 13 Abs. 1 GG gebietet jedoch einen möglichst umfassenden Schutz des Kernbereichs privater Lebensgestaltung im Bereich der präventiven Befugnisse zur Wohnraumüberwachung. Dieser Schutz wird auf Berufsgeheimnisträger nach §§ 53, 53a StPO ausgedehnt. Um die Zweckbindung der Daten zu gewährleisten, ist eine Kennzeichnungspflicht sowie eine zusätzliche verfahrensrechtliche Sicherung für eine Nutzung solcher Daten außerhalb des eng umgrenzten Bereichs des Verfassungsschutzes vorgesehen. Auch die Zurückstellung der verfassungsrechtlich gebotenen Benachrichtigung der Betroffenen bedarf einer verstärkten verfahrensrechtlichen Sicherung.

2. Als Reaktion auf die Anschläge des 11. September 2001 in den Vereinigten Staaten und die darin zu Tage getretene neue Dimension der terroristischen Bedrohung hat der Bundesgesetzgeber die Befugnisse des Bundesamts für Verfassungsschutz und – im Rahmen der Reichweite seiner Gesetzgebungskompetenz – auch der Verfassungsschutzbehörden der Länder durch das Terrorismusbekämpfungsgesetz (Gesetz vom 9. Januar 2002 (BGBl I S. 361)) um Auskunftsbefugnisse gegenüber Kreditinstituten, Fluggesellschaften, Post-, Telekommunikations- und Teledienstleistern ergänzt. Dem Bundesamt für Verfassungsschutz wurde ferner die Befugnis zum Einsatz des IMSI-Catchers eingeräumt. Durch das Gesetz zur Änderung des Bayerischen Verfassungsschutzgesetzes, des Gesetzes zur Ausführung des Gesetzes zu Art. 10 GG, des Bayerischen Sicherheitsüberprüfungsgesetzes und des Parlamentarischen Kontrollgremium-Gesetzes vom 24. Dezember 2002 (GVBl S. 969) hat der Landesgesetzgeber von der durch das Terrorismusbekämpfungsgesetz im Bundesverfassungsschutzgesetz geschaffenen Ermächtigung Gebrauch gemacht und die dort geregelten Auskunftsbefugnisse auch dem Landesamt für Verfassungsschutz übertragen. In Erweiterung der bundesrechtlichen Regelung erhielt das Landesamt für Verfassungsschutz die neuen Auskunftsbefugnisse auch zur Beobachtung des gewaltbereiten Inlandsterrorismus und der Organisierten Kriminalität. Des Weiteren wurde die landesrechtliche Grundlage für den Einsatz des IMSI-Catchers durch das

Landesamt für Verfassungsschutz geschaffen. Im Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl I S. 2) hat der Bundesgesetzgeber die Konsequenzen aus der Evaluierung der durch das Terrorismusbekämpfungsgesetz zunächst nur befristet geschaffenen Befugnisse gezogen und diese praktikabler gestaltet. Ferner wurde ihr Anwendungsbereich, wenn auch begrenzt, erweitert.

Auch die dem Landesamt für Verfassungsschutz in Umsetzung des Terrorismusbekämpfungsgesetzes eingeräumten Auskunftsbefugnisse, die ein wichtiges Element im Kampf gegen den internationalen Terrorismus darstellen, können nunmehr wie schon bei der bundesrechtlichen Regelung effektiver gestaltet und in ihrem Anwendungsbereich noch erweitert werden. Dies gilt insbesondere für die Auskunftsbeugnisse gegenüber Kreditinstituten und Fluggesellschaften, bei denen sich das aufgrund der bisherigen bundesrechtlichen Vorgaben systemwidrig anzuwendende Anordnungs- und Kontrollverfahren entsprechend dem G 10 in der Praxis als hinderlich erwiesen hat. Eine effektivere Gestaltung der Auskunftsbeugnisse des Landesamts für Verfassungsschutz ist im Hinblick auf die verfassungsrechtliche Zusammenarbeitspflicht der Verfassungsschutzbehörden auch geboten.

3. Bei der Ausgestaltung der infolge des Terrorismusbekämpfungsgesetzes originär auf Landesebene geschaffenen Befugnis zum Einsatz des IMSI-Catchers wird entsprechend der bundesrechtlichen Regelung dessen im Vergleich zu G 10-Maßnahmen geringeres Eingriffsgewicht berücksichtigt. Der Einsatz des IMSI-Catchers dient nur der Vorbereitung von G 10-Maßnahmen, nicht der Überwachung von Kommunikationseinhalten. Die für den Einsatz des IMSI-Catcher durch das Landesamt für Verfassungsschutz bislang geltende Einsatzschwelle des G 10 ist somit unangemessen und wird gesenkt. Des Weiteren wird der Anwendungsbereich des IMSI-Catchers entsprechend der bundesrechtlichen Regelung auf volksverhetzende Bestrebungen im Sinne von Art. 3 Abs. 1 Satz 1 Nr. 1 BayVSG erstreckt.
4. Informationen aus der islamistisch-terroristischen Szene über personelle Verbindungen, Netzwerke, die Verbreitung von Bombenbauanleitungen, Absprachen und Treffpunkte zur Vorbereitung von Anschlägen, Anschlagplanungen und potenzielle Anschlagziele sind nur durch eine Nutzung aller in Betracht kommenden technischen Potentiale zu erlangen. Eine wirksame Nachrichtenbeschaffung bei Vorliegen tatsächlicher Anhaltspunkte zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut verlangt dabei auch die Möglichkeit einer Datenerhebung durch Zugriff auf Speichermedien informationstechnischer Systeme. Es liegt bei einer solchen Maßnahme ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vor. Eine entsprechende Regelung für Fälle, in denen auf einen solchen Grundrechtseingriff im konkreten Einzelfall nicht verzichtet werden kann, fehlt bislang.

Dementsprechend wird ausdrücklich geregelt, dass das Landesamt für Verfassungsschutz bei Vorliegen tatsächlicher Anhaltspunkte zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut im Einzelfall auch die Befugnis hat, mit technischen Mitteln verdeckt auf informationstechnische Systeme zuzugreifen, um Daten zu erheben. Diese Befugnis ist eng begrenzt auf konkrete Einzelfälle, in denen die materiellen Anordnungsvoraussetzungen für eine Wohnraumüberwachung einschließlich des hier geltenden Straftatenkatalogs vorliegen würden. Maßnahmen in diesem Bereich sind wegen ihrer Eingriffsintensität in Umsetzung des Urteils des

Bundesverfassungsgerichts vom 27.02.2008 (1 BvR 370/07) an hohe materiellrechtliche Voraussetzungen geknüpft. Sie stehen grundsätzlich unter dem Vorbehalt richterlicher Anordnung. Der Kernbereich privater Lebensgestaltung wird durch entsprechende Regelungen geschützt. Es gelten grundsätzlich die gleichen Verfahrensregelungen wie bei der Wohnraumüberwachung.

5. Die sonstigen Änderungen bzw. Ergänzungen des Gesetzes folgen teils aus weiteren gerichtlichen Entscheidungen (BayVG, Urteil vom 09.04.2003 - 24 B 02.646 – und BVerwG, Urteil vom 09.03.2005 - 6 C 3.04 - zur Übermittlung personenbezogener Daten sowie Urteil des Oberverwaltungsgerichts Berlin-Brandenburg vom 06.04.2006 (3 B 3.99) zu den Voraussetzungen einer Berichterstattung im Rahmen des Verfassungsschutzberichts) und zielen insoweit darauf ab, eine bereits bisher geltende entsprechende Verwaltungspraxis aufzugreifen. Teils dienen sie dazu, die Rechte und den Schutz der Betroffenen zu verbessern. Hier sind zu nennen eine ausdrückliche Regelung für den Einsatz verdeckter technischer Mittel zum Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes mit besonderen Verfahrensregelungen und Berücksichtigung des Kernbereichs privater Lebensgestaltung, aber auch die Einführung eines grundsätzlichen Auskunftsanspruchs.

#### **B) Zwingende Notwendigkeit einer normativen Regelung**

Der Gesetzentwurf ist erforderlich, um bereits bestehende Befugnisse an die verfassungsrechtlichen Vorgaben anzupassen bzw. die Grenzen bestehender Befugnisse klarzustellen. Des Weiteren werden bestehende Befugnisse, die dazu beitragen, terroristische Strukturen besser aufzuklären und den Terrorismus zum Schutz der Bevölkerung bereits im Vorfeld abzuwehren, wie auf Bundesebene bereits geschehen, praktikabler gestaltet und in ihrem Anwendungsbereich noch erweitert. Auch die übrigen im Bayerischen Verfassungsschutzgesetz geregelten Befugnisse beinhalten Eingriffe in die Grundrechte der hiervon betroffenen Personen; dies setzt eine entsprechende gesetzliche Ermächtigung voraus. Die Schaffung zusätzlicher bzw. die Anpassung bereits bestehender Eingriffsbefugnisse kann daher aus verfassungsrechtlichen Gründen nur durch eine Ergänzung bzw. Änderung des Bayerischen Verfassungsschutzgesetzes erfolgen.

#### **Begründung der einzelnen Vorschriften**

##### **Zu § 1**

##### **Änderung des Bayerischen Verfassungsschutzgesetzes**

##### **Zu § 1 Nr. 1 Buchstabe a (Art. 6 Abs. 1 Sätze 4 bis 6 BayVSG)**

Der neue Halbsatz in Satz 1 dient der Klarstellung der schon bislang geltenden Rechtslage: Die Anwendung nachrichtendienstlicher Mittel zur Erfüllung der Aufgaben des Landesamts kommt nur in Betracht auf der Rechtsgrundlage des Art. 6 Abs. 1, soweit nicht andere speziellere gesetzliche Regelungen vorgehen. Insbesondere im Bereich des Artikel 10-Gesetzes bestehen weitergehende und strengere Voraussetzungen. Speziellere und damit vorrangig zu beachtende Anforderungen werden zudem im Rahmen der Art. 6a bis Art. 6g für die Wohnraumüberwachung und für besondere Formen der Datenerhebung aufgestellt.

Die neuen Sätze 4 und 5 zielen darauf ab, den aufgrund der Generalklausel in Satz 1 allgemein und grundsätzlich zugelassenen Einsatz nachrichtendienstlicher Mittel näher zu konkretisieren. Dabei wird gleichzeitig dem Umstand Rechnung getragen, dass eine

detaillierte öffentliche Aufzählung aller in Betracht kommender Mittel, die darauf abzielen, eine verdeckte Datenerhebung zu vermeiden, für die Arbeit des Verfassungsschutzes nachteilig wäre. Entsprechend der Regelung in § 8 Abs. 2 BVerfSchG wird daher festgelegt, dass in einer Dienstvorschrift die nachrichtendienstlichen Mittel vorab benannt werden, der Genehmigung des Staatsministeriums des Innern bedürfen und das Parlamentarische Kontrollgremium hierüber zu unterrichten ist. Eine Konkretisierung der nachrichtendienstlichen Mittel entspricht auch einer Forderung des Landesbeauftragten für den Datenschutz.

Zu § 1 Nr. 1 Buchstabe b (Streichung des bisherigen Art. 6 Abs. 4 BayVSG)

In Abs. 1 Satz 4 wird auf vorrangig zu beachtende speziellere Regelungen, wie das Artikel 10-Gesetz, hingewiesen. Eines erneuten Hinweises auf das Artikel 10-Gesetz bedarf es nicht mehr.

### Zu § 1 Nr. 2 (Art. 6a und 6b BayVSG)

Der bisherige Art. 6a wird an die Vorgaben des Urteils des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung vom 3. März 2004 (Az.: 1 BvR 2378/98, 1 BvR 1084/99) angepasst. Aus Gründen der Übersichtlichkeit wird die Vorschrift dabei neu gefasst und ein neuer Art. 6 b angefügt. Das Bundesverfassungsgericht hat in seiner Entscheidung die wirksame Aufklärung schwerer Straftaten und den Schutz der Bevölkerung vor der Begehung derartiger Straftaten erneut als wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 200). Die Bekämpfung des (internationalen) Terrorismus und der Organisierten Kriminalität spielen dabei eine besondere Rolle. Ziel ist, in die Strukturen und in den Innenbereich der kriminellen Organisationen einzudringen und dadurch die Begehung schwerer Straftaten zu verhindern.

#### Zu Art. 6a Abs. 1

Abweichend vom bisherigen Art. 6a Abs. 1, der alle Anordnungsvoraussetzungen für Wohnraumüberwachungen regelte, beschränkt sich Art. 6a Abs. 1 jetzt auf die Aussage, dass auch Wohnraumüberwachungen grundsätzlich zulässige nachrichtendienstliche Mittel im Sinn des Art. 6 sind. Hinsichtlich weiterer Anordnungsvoraussetzungen wird auf die folgenden Absätze verwiesen.

#### Zu Art. 6a Abs. 2

Art. 6a Abs. 2 erläutert die dringende Gefahr im Sinn von Art. 13 Abs. 4 GG. Sie ist zu bejahen, wenn Hinweise auf bevorstehende Straftaten vorliegen und durch ihre Verhütung hinreichend gewichtige Rechtsgüter geschützt werden. Die bisherige Differenzierung der Anordnungsvoraussetzungen in Art. 6a Abs. 1 Satz 1 nach der Beobachtungsaufgabe wird aufgegeben. Entscheidend ist, dass tatsächliche Anhaltspunkte für die Gefährdung von Leib, Leben und Freiheit von Personen in erheblichem Ausmaß bestehen. Da kann es nicht darauf ankommen, welche der in Art. 3 Abs. 1 genannten Bestrebungen oder Tätigkeiten verfolgt wurden.

Der Katalog der bisher in Art. 6a Abs. 1 Satz 1 Nr. 1 bis 3 aufgeführten Straftaten wird reduziert bzw. angepasst. Dies gilt insbesondere für bisher in der Nummer 3 genannte Straftaten. Das Bundesverfassungsgericht hat die Eignung und Erforderlichkeit von Wohnraumüberwachungen zur Aufklärung von OK-Strukturen und damit zur Verhinderung weiterer Straftaten zwar bestätigt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 212 f. und 217). Aufgrund der verfassungsrecht-

lichen Vorgaben war der Straftatenkatalog im Verhältnis zur bisherigen Rechtslage jedoch einzuschränken, auch wenn sich die Entscheidung des Bundesverfassungsgerichts unmittelbar nur auf den Straftatenkatalog des § 100c Abs. 1 Nr. 3 StPO a. F. bezog.

In Art. 6a Abs. 2 Satz 1 werden die Anforderungen an die Straftaten nunmehr zunächst abstrakt umschrieben; entsprechend den grundgesetzlichen Vorgaben muss es sich um Straftaten handeln, deren Ziel oder wahrscheinliche Folge eine erhebliche Gefährdung der Rechtsgüter Bestand oder Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit ist. In Satz 2 werden solche in Betracht kommenden Straftaten dann aufgezählt. Die Auswahl der Straftatbestände orientiert sich hier entsprechend Art. 13 Abs. 4 GG am Ausmaß der damit verbundenen Gefahren. In Anlehnung an die vom Bundesverfassungsgericht für repressive Wohnraumüberwachungen festgelegten Anforderungen an den Straftatenkatalog im Bereich von Art. 13 Abs. 3 GG wurde als Orientierungsrahmen eine Höchststrafe von mehr als fünf Jahren Freiheitsstrafe zugrundegelegt. Eine strikte Übernahme der vom Bundesverfassungsgericht festgelegten Mindesthöchststrafe war jedoch nicht geboten. Im Bereich der Prävention geht es nicht darum, Unrecht zu ahnden, sondern Schaden von Rechtsgütern abzuwenden. Dementsprechend muss etwa auch die Vorbereitung von Explosionsverbrechen (vgl. § 310 StGB) mit Mitteln der Wohnraumüberwachung bekämpft werden können. Vergleichbares gilt für die Herbeiführung einer Explosion durch Kernenergie (§ 307 Abs. 1, StGB) und die Bildung krimineller Vereinigungen in besonders schweren Fällen (§ 129 Abs. 1 StGB in Verbindung mit Abs. 4).

Im Straftatenkatalog nicht mehr enthalten sind im Wesentlichen Delikte aus dem Bereich Hochverrat, Gefährdung des demokratischen Rechtsstaates sowie Landesverrat und Gefährdung der äußeren Sicherheit, soweit die gesetzliche Höchststrafe nicht über fünf Jahren lag. Gleiches gilt für Straftaten aus den Bereichen Geldwäsche, Betrug und Untreue, Urkundenfälschung, Vorteilsnahme/-gewährung und Bestechlichkeit/Bestechung sowie Volksverhetzung.

Wie nach bisheriger Rechtslage (Art. 6a Abs. 1 Satz 1) besteht das Erfordernis tatsächlicher Anhaltspunkte für entsprechende Bestrebungen oder Tätigkeiten. Bloße Vermutungen reichen nicht aus. Das Landesamt für Verfassungsschutz und die Gerichte haben im Einzelfall abzuwägen, wie konkret die tatsächlichen Anhaltspunkte sind, um den Eingriff zu rechtfertigen. In die Abwägung sind die Intensität des Grundrechtseingriffs (insbesondere die Schutzwürdigkeit der Wohnung und der dort zu erwartenden Situationen) und die Bedeutung der durch die Strafnorm im jeweiligen Fall geschützten Rechtsgüter einzubeziehen.

#### Zu Art. 6a Abs. 3 Satz 1

Art. 6a Abs. 3 Satz 1 enthält weitere gesetzliche Einschränkungen und verfahrensrechtliche Sicherungen. Sie dienen dazu, die Einhaltung der verfassungsrechtlichen Grenzen für die Wohnraumüberwachung zu gewährleisten. Durch die Formulierung „wenn und soweit“ wird klargestellt, dass die Voraussetzungen bei Anordnung der Überwachungsmaßnahme nicht umfassend prognostiziert werden müssen, da insbesondere eine nach Nummer 2 erforderliche Prognose, wer sich wann in den Räumlichkeiten aufhalten wird, in der Regel nicht möglich ist. Es handelt sich insofern um Anforderungen, die während der Durchführung zu beachten sind und nur soweit vorhersehbar bereits bei Maßnahmenanordnung beachtet werden müssen.

In Art. 6a Abs. 3 Satz 1 Nr. 1 wurde der bisher in Art. 6 Abs. 1 Satz 1 geregelte Grundsatz der Subsidiarität von Wohnraumüberwachungen unverändert übernommen. Besondere technische Mittel dürfen wegen der Schwere des Eingriffs im Schutzbereich des

Art. 13 GG nur eingesetzt werden, wenn andere Maßnahmen versagen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 224).

Die Regelungen in den Nummern 2 und 3 gewährleisten den vom Bundesverfassungsgericht (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 119 ff., 169 ff.) geforderten Schutz des Kernbereichs privater Lebensgestaltung bei Wohnraumüberwachungen. Art. 6a Abs. 3 Satz 1 Nr. 2 untersagt den Einsatz besonderer technischer Mittel in privaten Wohnräumen, wenn zu erwarten ist, dass sich der Adressat dort allein oder ausschließlich mit Personen seines engsten Vertrauens aufhält und keine konkreten Anhaltspunkte für einen unmittelbaren Bezug zwischen den Gesprächen und den aufzuklärenden Bestrebungen oder Tätigkeiten gegeben sind (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 138). Das Landesamt für Verfassungsschutz hat durch geeignete Vorermittlungen (ggf. Observationen) Sorge zu tragen, dass in den konkreten Überwachungszeiträumen keine unzulässigen Eingriffe stattfinden. Dazu gehören zum Beispiel parallele Ermittlungsmaßnahmen oder die Feststellung, wer sich zu welcher Zeit in den betroffenen Räumlichkeiten aufhält. Wer zum Kreis der engsten Vertrauten gehört, ist im Einzelfall zu entscheiden. Erforderlich ist ein besonderes, den Kernbereich privater Lebensgestaltung betreffendes Vertrauensverhältnis. Der Personenkreis, der zum Kernbereich privater Lebensgestaltung zu rechnen ist, stimmt nach Darlegung des Bundesverfassungsgerichts nicht mit dem Kreis der nach §§ 52, 53 und 53a StPO Zeugnisverweigerungsberechtigten überein (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 147). Er ist einerseits enger, da nicht jedes Zeugnisverweigerungsrecht dem Kernbereichsschutz dient, andererseits weiter, da auch enge persönliche Freundschaften erfasst werden.

Die Regelung in Abs. 3 Satz 1 Nr. 2 schützt nicht nur Gespräche mit Familienangehörigen und engsten Vertrauten, sondern auch mit Berufsgeheimnisträgern nach § 53 StPO sowie deren Hilfspersonen nach § 53a StPO. Diese Gespräche sind aufgrund der besonderen Funktion der Berufsgeheimnisträger und der Bedeutung der Vertrauensverhältnisse ebenfalls schutzwürdig und werden daher vom Abhörverbot umfasst. Damit ist ein umfassender Schutz vertrauenswürdiger Gespräche gewährleistet. Die Schutzwirkungen greifen allerdings nicht, wenn Gespräche nach ihrem Inhalt die Verfolgung der im Abs. 2 genannten Bestrebungen oder Tätigkeiten zum Gegenstand haben (Satz 1 Nr. 2 Buchst. a (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 137)) oder wenn sich die Maßnahme auch gegen den Gesprächspartner selbst richtet, weil er verdächtig ist, entsprechende Bestrebungen oder Tätigkeiten zu verfolgen (Satz 1 Nr. 2 Buchst. b). Zu diesen Fallgruppen zählt z. B. die Planung von Selbstmordattentaten durch engste Familienangehörige.

Eine Ausnahme von dem Grundsatz, dass Gespräche mit unmittelbarem Bezug zu Bestrebungen im Sinn des Abs. 2 nicht schutzbedürftig sind, wird lediglich bei Berufsgeheimnisträgern gemacht, deren Beziehung zu dem Adressaten aufgrund ihrer besonderen beruflichen Funktion besonders schutzwürdig ist (Satz 1 Nr. 2 Buchst. a). Dies ist der Fall, wenn ein gesprächstypischer Bezug zu ihrer Tätigkeit als Berufsgeheimnisträger besteht. Das Zeugnisverweigerungsrecht nach § 53 StPO ist bei diesen Personen zugleich Ausdruck einer verfassungsrechtlichen Position, die einem Eingriff in das Vertrauensverhältnis bei Gesprächen in einer besonders geschützten Umgebung entgegensteht. Neben Geistlichen und Anwälten, denen sich der Adressat etwa im Zusammenhang mit bereits begangenen Straftaten anvertrauen kann, sind zu dieser Gruppe die Ärzte, Psychotherapeuten und Suchtberater zu rechnen. Der besondere Schutz greift aber nur, soweit das Zeugnisverweigerungsrecht reicht. Diese Schutzwirkungen enden aller-

dings, wenn ein Berufsgeheimnisträger selbst an der Verursachung der Gefahr beteiligt ist.

Der Schutz wird in Satz 1 Nr. 3 auf Räumlichkeiten von Berufsgeheimnisträgern ausgedehnt, die zu deren Berufsausübung bestimmt sind. Zwar bedürfen Betriebs- und Geschäftsräume grundsätzlich eines geringeren Schutzes, da sie typischerweise durch einen Sozialbezug geprägt sind; dies gilt aber nicht, wenn sie der Ausübung von Berufen dienen, die ein besonderes Vertrauensverhältnis voraussetzen, das den Bereich des Höchstpersönlichen betrifft (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 142 f.). Wenn allerdings der Berufsgeheimnisträger selbst verdächtig ist, die zu beobachtenden Bestrebungen oder Tätigkeiten zu verfolgen und Hinweise dafür bestehen, dass der Berufsgeheimnisträger mit Dritten Gespräche führt, die nach ihrem Inhalt einen unmittelbaren Bezug zu den im Abs. 2 genannten Bestrebungen oder Tätigkeiten haben, besteht keine Schutzwürdigkeit des Vertrauensverhältnisses. Es gelten dann die Voraussetzungen der Nr. 2a, so dass Gespräche, die mit unbeteiligten Dritten geführt werden und die Bestrebungen oder Tätigkeiten nicht betreffen, ausgenommen sind.

Zu Art. 6a Abs. 3 Satz 2

Art. 6a Abs. 3 Satz 2 trifft Regelungen über die Art und Weise der Durchführung und die Unterbrechungspflicht. Wie vom Bundesverfassungsgericht in seiner Entscheidung vom 03.03.2004 (Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 151 f.) für die repressive Wohnraumüberwachung klargestellt, kann es der Grundrechtsschutz bei dem Abhören von Gesprächen in einer Privatwohnung erforderlich machen, bei einer Maßnahme mitzuhören, um sie jederzeit unterbrechen zu können. Dieser Grundsatz ist auf die präventive Überwachung übertragbar. In diesen Fällen sollte zunächst die Gesprächssituation ermittelt werden. Eine ausschließlich automatisierte Aufzeichnung ist daher lediglich dann zulässig, wenn keine äußeren Anzeichen für eine mögliche Kernbereichsverletzung vorliegen.

Im zweiten Halbsatz wird zur Umsetzung der Vorgaben des Bundesverfassungsgerichts die Unterbrechung der Maßnahme angeordnet, wenn bei einer Wohnraumüberwachung erkennbar wird, dass es zu einem Kernbereichseingriff kommt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 152). Die Dauer der Unterbrechung und die Zulässigkeit des erneuten Abhörens richten sich nach den Umständen des jeweiligen Einzelfalles. Nach einer Unterbrechung ist ein Abhören wieder zulässig, wenn anzunehmen ist, dass nicht mehr in den Kernbereich privater Lebensgestaltung eingegriffen wird. Aus Gründen des Grundrechtsschutzes kann ein „Hineinhören“ in eine laufende Unterhaltung ohne Aufzeichnung angebracht sein. Stellt sich dabei heraus, dass entgegen der ursprünglichen Prognose immer noch Gespräche geführt werden, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, ist eine neuerliche Unterbrechung erforderlich.

Zu Art. 6a Abs. 4

Art. 6a Abs. 4 regelt, in welchen Wohnungen die Maßnahme durchgeführt werden darf. Dabei wird der Schutz von Wohnungen von Berufsgeheimnisträgern und Unbeteiligten im Vergleich zur bisherigen Rechtslage (Art. 6a Abs. 1 Satz 2), die sich am Artikel 10-Gesetz anlehnt, verbessert. Grundsätzlich darf nach Abs. 4 Satz 1 nur die Wohnung desjenigen überwacht werden, gegen den sich die Maßnahme richtet (Adressat). In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn anzunehmen ist, dass sich der Adressat dort aufhält (Satz 2 Nr. 1), und wenn – als Ausprägung des Subsidiaritätsgrundsatzes – Maßnahmen in seiner Wohnung nicht zur Erforschung der Bestrebungen im Sinn des Abs. 2 ausreichen bzw. nicht möglich sind (Satz 2 Nr. 2). Die

Wohnungen von Berufsheimnisträgern werden in Satz 2 ausdrücklich ausgenommen, so dass in deren Räumen eine Überwachung nur dann zulässig ist, wenn sie selbst verdächtig sind und deshalb Adressat der Maßnahme sind oder wenn sie mit der Maßnahme einverstanden sind, etwa weil sie ihrem eigenen Schutz dient.

Satz 3 stellt klar, dass auch Dritte von der Maßnahme betroffen sein können, die nicht Adressat sind. Neben den Gesprächspartnern sind dies z. B. Handwerker, Postboten oder zufällige Besucher. Zu ihrem Schutz dürfen Daten über sie nur erhoben werden, wenn dies unvermeidbar ist.

#### Zu Art. 6b Abs. 1

Die Sätze 1 und 2 übernehmen, den Vorgaben des Art. 13 Abs. 4 GG entsprechend, das bisher in Art. 6a Abs. 2 Satz 1 und Satz 2 geregelte Erfordernis einer richterlichen Anordnung und die Eilkompetenz des Präsidenten des Landesamts für Verfassungsschutz bzw. dessen Stellvertreters; die gerichtliche Bestätigung ist entsprechend den grundgesetzlichen Vorgaben (Art. 13 Abs. 4 Satz 2 GG) unverzüglich nachzuholen. Das Schriftlichkeitsgebot sowie die nach Satz 3 nunmehr bestehenden inhaltlichen Anforderungen an die Anordnung und deren Begründung dienen der Einhaltung der verfassungsrechtlichen Erfordernisse. Die Angaben zur Art der Maßnahme umfassen dabei insbesondere die Frage der automatisierten Aufzeichnung. Das Bundesverfassungsgericht hat die Aufgaben und Pflichten des anordnenden Gerichts bei dessen Prüfung festgelegt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 275). Der Einhaltung verfassungsrechtlicher Erfordernisse dient auch die von bisher drei auf einen Monat verkürzte Höchstdauer der Anordnung, wobei eine Verlängerung - wiederum begrenzt auf jeweils einen Monat - weiterhin möglich bleibt (Satz 4). Die Begrenzung auf einen Monat gewährleistet die regelmäßige gerichtliche Überprüfung und damit eine der Tiefe des Grundrechtseingriffs angemessene Überwachung durch eine weisungsunabhängige Instanz (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 281). Satz 5, der dem bisherigen Art. 6a Abs. 2 Satz 4 entspricht, ist Ausprägung und Präzisierung des Verhältnismäßigkeitsgrundsatzes, der in jedem Fall zu wahren ist. Die nach Satz 6 neu vorgesehene Mitteilung der Beendigung der Maßnahme an den Richter dient seiner Befugnis, die Maßnahme insgesamt zu kontrollieren. Die Regelung in Satz 7 entspricht dem bisherigen Art. 6a Abs. 3 Satz 1.

#### Zu Art. 6b Abs. 2 Sätze 1 bis 3

In Art. 6a Abs. 2 Sätze 1 bis 3 werden die Daten entsprechend dem bisherigen Art. 6a Abs. 3 Satz 2 einer Zweckbindung unterworfen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 328 ff.). Die Zweckbindung lässt sich nur gewährleisten, wenn die Herkunft der Daten auch nach der Informationserhebung erkennbar bleibt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 347). In den Sätzen 1 und 2 wird daher eine Kennzeichnungspflicht des Landesamts für Verfassungsschutz sowie der datenempfangenden Stelle gesetzlich eingeführt.

Art. 6b Abs. 2 Satz 3 gewährleistet die Zweckbindung auch z.B. bei der Speicherung sowie der Übermittlung der Daten an andere öffentliche Stellen. Die Übermittlung zu Präventionszwecken sowie zu Strafverfolgungszwecken wird aufgrund der verfassungsrechtlichen Vorgaben eingeschränkt. Die Übermittlung der Daten an andere öffentliche Stellen stellt aufgrund der damit verbundenen Zweckänderung grundsätzlich einen eigenständigen Grundrechtseingriff dar (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 333). Für die Zulässigkeit müssen u.a. der ursprüngliche Verwendungszweck und der veränderte Verwendungszweck miteinander vereinbar sein. Unvereinbarkeit

liegt vor, wenn die Daten für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 338). Entsprechend dieser Vorgaben wird die Übermittlungsbefugnis in Satz 3 Nr. 3 zu Strafverfolgungszwecken von den Voraussetzungen der Strafprozessordnung für die Datenerhebung zu strafprozessualen Zwecken abhängig gemacht. Auch wenn § 100 d Abs. 5 StPO bislang eine strafprozessuale Verwendung der durch den Verfassungsschutz erhobenen Daten nicht vorsieht, wird im Hinblick auf insoweit bestehenden Änderungsbedarf schon jetzt geregelt, dass Vorschriften des bayerischen Landesrechts einer solchen Verwendung nicht entgegenstehen. Die Übermittlungsbefugnis zu Präventionszwecken ist auf die Abwehr dringender Gefahren beschränkt, nämlich auf die Verhütung von Straftaten des Straftatenkatalogs nach Art. 6a Abs. 2, soweit sie die Rechtsgüter Leib, Leben oder Freiheit in erheblichem Maß gefährden sowie die Abwehr anderer dringender Gefahren für Leib, Leben oder Freiheit von Menschen. Auch für die Weiterverwendung von Daten aus Wohnraumüberwachungsmaßnahmen gilt, wenn auch im Einzelfall in abgeschwächter Form, der Subsidiaritätsgrundsatz, nach dem Daten vorrangig anderweitig zu beschaffen sind und nur in unvermeidlichen Fällen auf die Daten der Wohnraumüberwachung zurückgegriffen werden darf. Die Verpflichtung, die Zweckänderung zu dokumentieren, ergibt sich bereits aus Art. 14 Abs. 1 Satz 1 Halbsatz 2 und bedurfte somit keiner wiederholenden Regelung. Daten, die von vornherein nicht verwendet werden dürfen, etwa weil die Voraussetzungen für ihre Erhebung nicht vorlagen oder sie dem Kernbereich privater Lebensgestaltung zuzurechnen sind, ohne jeweils der Abwehr erheblicher Gefahren zu dienen (vgl. Satz 5), sind zu löschen und dürfen nicht an andere Stellen übermittelt werden.

#### Zu Art. 6b Abs. 2 Satz 4

In Satz 4 entspricht im Wesentlichen der bisherige Regelung des Art. 6a Abs. 3 Satz 3.

#### Zu Art. 6b Abs. 2 Satz 5

Das mit einer Wohnraumüberwachung verbundene Risiko des Eingriffs in den Kernbereich privater Lebensgestaltung kann verfassungsrechtlich nur hingenommen werden, wenn aus Verletzungen keine weiteren Folgen entstehen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 183). Satz 5 regelt daher in Ergänzung zu den Erhebungsverboten des Art. 6a Abs. 3 Satz 1 Verwendungsverbote.

Das Bundesverfassungsgericht hat anerkannt, dass es Fälle geben kann, in denen Gespräche einem den Kernbereichsschutz begründenden sozialen Umfeld nicht eindeutig zugeordnet werden können oder es sich im Vorhinein nicht feststellen lässt, ob es sich um gefahrenrelevante Gespräche handelt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 185). Werden die Erhebungsvoraussetzungen eingehalten, ist deshalb verfassungsrechtlich eine nachträgliche Bewertung des Gesprächsinhalts im Rahmen einer ersten „Sichtung“ nicht zu beanstanden (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 151). Ergibt sich dabei jedoch aus der ex post-Sicht, dass ein Eingriff in den Kernbereich privater Lebensgestaltung vorliegt, dürfen die Daten nicht verwendet und müssen unverzüglich gelöscht werden.

Dementsprechend sieht Satz 5 Verwendungsverbote vor für Fälle, in denen sich nachträglich herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben (Nr. 1) bzw. dass die Daten aus einem nach Art. 6a Abs. 3 Satz 1 Nr. 2 a) besonders geschützten Vertrauensverhältnis zu Berufsheimnisträgern stammen (Nr. 2). Durch die Regelung in Nummer 2 werden Gespräche mit den dort genannten Personen selbst dann geschützt, wenn sie einen unmittel-

telbaren Bezug zu Bestrebungen nach Art. 6a Abs. 2 haben, soweit das Recht zur Zeugnisverweigerung reicht. Diese Schutzwirkungen enden allerdings, wenn ein Berufsgeheimnisträger selbst an der Verursachung der Gefahr beteiligt ist.

Schließlich dürfen auch Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und keinen unmittelbaren Bezug zu Bestrebungen oder Tätigkeiten nach Art. 6a Abs. 2 haben (Nr. 3), nicht verwendet werden. Daten, die einen unmittelbaren Bezug zu solchen Bestrebungen oder Tätigkeiten haben, sind grundsätzlich nicht dem geschützten Kernbereich privater Lebensgestaltung zuzurechnen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 137), so dass insofern nur eine Klarstellung erfolgt.

Im präventiven Bereich sind Ausnahmen von den dargelegten Verwendungsverboten erforderlich, wenn eine Verwendung zum Schutz hochwertiger Rechtsgüter nötig ist. Verwendet werden dürfen Gespräche über Bestrebungen oder Tätigkeiten im Sinn des Art. 6a Abs. 2, aus denen auf eine erhebliche Gefährdung von Leib, Leben oder Freiheit geschlossen werden kann. Solche Gespräche gehören ebenso wie Gespräche über begangene Straftaten (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 137), nicht zum unantastbaren Kernbereich privater Lebensgestaltung. Entsprechendes gilt in Fällen, bei denen die Erhebungsvoraussetzungen nicht vorgelegen haben oder bei denen das geschützte Vertrauensverhältnis zu Berufsgeheimnisträgern betroffen ist. Verwendet werden dürfen Informationen aus Gesprächen, auch wenn sie keinen Bezug zu oben genannten Bestrebungen oder Tätigkeiten haben bei erheblichen Gefahren für Leib, Leben und Freiheit. Der Sprachgebrauch des BayVSG wird hierbei an den des PAG angepasst und für eine Weiterverwendung von Daten in diesen Fällen auf eine gegenwärtige Gefahr abgestellt. Eine gegenwärtige Gefahr kann auch dann vorliegen, wenn die Gefahrenlage einen aktuellen Handlungsbedarf ergibt, der unter Berücksichtigung des Gewichts der drohenden Rechtsgrütsbeeinträchtigungen als unaufschiebbar zu bewerten ist. Das Bundesverfassungsgericht hat sich in seiner Entscheidung nur mit den absoluten strafprozessualen Verwertungsverboten befasst (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 181; 184f.). Eine Abwägung zwischen Kernbereichsschutz und Strafverfolgungsinteresse hat es abgelehnt. Im Bereich der Strafverfolgung geht die Menschenwürde in diesem höchstpersönlichen Bereich dem Strafverfolgungsinteresse vor (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 121). Im präventiven Bereich können dagegen Situationen eintreten, in denen sich der Kernbereichsschutz und andere absolut geschützte Rechtsgüter, wie Leben, Gesundheit und Freiheit gegenüberstehen. Zu denken ist etwa an den Fall, dass bei der Auswertung eine Information gewonnen wird, deren Kenntnis die Vereitelung eines unmittelbar drohenden nicht politisch motivierten Mordes und damit den Schutz höchster Rechtsgüter ermöglicht.

Zu Art. 6b Abs. 2 Sätze 6 und 7

In Art. 6a Abs. 6 Satz 6 wird zur verfahrensrechtlichen Sicherung der verfassungsrechtlichen Verwertungsverbote für Eingriffe in den Kernbereich eine richterliche Kontrolle der Daten eingeführt. Der Schutz des Kernbereichs privater Lebensgestaltung erfordert eine Kontrolle auch der Verwertbarkeit von Informationen, die durch eine Wohnraumüberwachung erlangt worden sind, durch eine unabhängige Stelle, wenn Informationen für weitergehende Maßnahmen außerhalb des Verfassungsschutzes genutzt werden. (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 191). Erst recht gilt die richterliche Kontrolle in Fällen der Verwendung ursprünglich zu Unrecht erhobener Daten oder in Fällen eines Zeugnisverweigerungsrechts von Berufsgeheimnisträgern. Art. 6a Abs. 6 Satz 7 sieht auch hier entsprechend

Art. 6a Abs. 5 Satz 2 eine Eilzuständigkeit des Präsidenten des Landesamts für Verfassungsschutz bzw. dessen Stellvertreters vor. Die richterliche Entscheidung über die Zulässigkeit der Verwendung oder die Übermittlung von Daten ist unverzüglich nachzuholen.

Zu Art. 6b Abs. 3

Art. 6b Abs. 3 regelt die Sperrung und Löschung der Daten. Daten, die aus dem Kernbereich privater Lebensgestaltung stammen und für die nach Abs. 2 Satz 5 ein Verwendungsverbot besteht, sind aufgrund verfassungsrechtlicher Vorgaben unverzüglich zu löschen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 135, 186). Auch das Gebot des effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG steht dem nicht entgegen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 186). Dies wird durch Satz 1 klargestellt.

Für sonstige Daten bleibt es bei dem bisher in Art. 6a Abs. 3 Satz 4 der geltenden Fassung geregelten Grundsatz, dass Daten unter der Aufsicht eines Bediensteten des Landesamts für Verfassungsschutz mit Befähigung zum Richteramt zu löschen sind, sobald sie für den festgelegten Zweck oder eine Übermittlung an andere Stellen nicht mehr benötigt werden.

Die Lösungsverpflichtung muss aber zugleich dem Gebot des effektiven Rechtsschutzes aus Art. 19 Abs. 4 genügen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 349). In Satz 2 wird daher entsprechend der bisherigen Regelung in Art. 6a Abs. 3 Sätze 6 und 7 die Lösungsverpflichtung mit der Rechtsschutzgarantie des Art. 19 Abs. 4 GG in Einklang gebracht. Daten sind zunächst zu sperren, soweit die Löschung geeignet ist, die nach Abs. 4 gebotene Mitteilung an den Betroffenen oder eine gerichtliche Kontrolle der Maßnahme zu beeinträchtigen. In Art. 6b Abs. 3 Sätze 4 und 5 wird nunmehr geregelt, wann gesperrte Daten zu löschen sind. Gesperrte Daten dürfen erst gelöscht werden, nachdem sichergestellt ist, dass sie für eine gerichtliche Überprüfung nicht mehr benötigt werden. Im Fall einer Mitteilung an den Betroffenen sind die Daten erst zu löschen, wenn der Betroffene nach Ablauf eines Monats nach seiner Benachrichtigung keine Klage erhebt. Die Monatsfrist dient dem Betroffenen als Entscheidungsfrist darüber, ob er gerichtlichen Rechtsschutz in Anspruch nehmen will. Die Fristsetzung ist erforderlich, um Rechtsklarheit für die Zulässigkeit der Löschung der Daten zu schaffen. Die Löschung muss im Hinblick auf Art. 19 Abs. 4 GG protokolliert werden (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 187).

Zu Art. 6b Abs. 4 Sätze 1 bis 4

In Art. 6b Abs. 4 Satz 1 wurde der bisher in Art. 6a Abs. 5 Satz 1 enthaltene Grundsatz, dass der von einer Wohnraumüberwachung Betroffene nach ihrer Beendigung davon zu benachrichtigen ist, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann, präzisiert. Art. 13 Abs. 1 in Verbindung mit Art. 19 Abs. 4 GG vermittelt den Grundrechtsträgern grundsätzlich einen Anspruch auf Kenntnis von Wohnraumüberwachungen, die sie betreffen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 290). Zu benachrichtigen sind somit zunächst die Adressaten der Maßnahme. Andere Personen sind zu benachrichtigen, soweit von ihnen personenbezogene Daten erhoben werden und diese Daten dann für Zwecke im Sinne des Abs. 2 Satz 3 verwendet werden. Eine Verwendung für andere Zwecke ist dabei durch Abs. 2 Satz 3 bereits generell ausgeschlossen. Diese Regelung schafft einen sachgerechten Ausgleich zwischen dem grundsätzlich bestehenden Informationsinteresse der von Überwachungsmaßnahmen Mitbetroffenen und dem Interesse des Landesamts für Verfassungsschutz, einen unangemessenen und nicht der Aufgabenerfüllung dienenden Aufwand zu vermei-

den. Vor allem aber wird dadurch eine klare und eindeutig vollziehbare Regelung geschaffen, die schwierige Abgrenzungs- und Abwägungsprobleme vermeidet. Gleichzeitig wird damit auch klargestellt, dass mitgehörte Äußerungen von zufällig anwesenden Personen ohne inhaltlichen Belang für die Aufgabenerfüllung des Landesamts (z.B. des Hausmeisters oder des Postboten) schon vom Ansatz her keine Benachrichtigungspflicht auslösen. Dies dient gleichzeitig auch dem Grundrechtsschutz des Adressaten einer Maßnahme, der ein berechtigtes grundrechtlich geschütztes Interesse daran hat, dass außenstehenden Dritten Überwachungsmaßnahmen nicht offenbart werden.

Bei der Wohnraumüberwachung als schwerwiegendem Grundrechtseingriff besteht das Rechtsschutzinteresse auch nach Beendigung der Maßnahme fort (vgl. BVerfG vom 30. April 1997, BVerfGE 96, 27/40; BVerfG vom 05.12.2001, BVerfGE 104, 220/232 f.).

Die Gefahr, durch eine Benachrichtigung den Zweck der Maßnahme zu gefährden, wurde vom Bundesverfassungsgericht als hinreichend gewichtig anerkannt, um eine Einschränkung der verfassungsrechtlich gebotenen Benachrichtigungspflicht zu rechtfertigen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 299). Zur Gewährleistung des effektiven Grundrechtsschutzes muss aber auch die Entscheidung über die Zurückstellung der Mitteilung gerichtlich kontrolliert werden, soweit die Mitteilung mehr als sechs Monate nach Abschluss der Maßnahme zurückgestellt werden muss. Um sicherzustellen, dass die Zurückstellung auch im weiteren Verlauf auf das unbedingt Erforderliche begrenzt bleibt, bedarf es in Zeitabständen einer wiederkehrenden gerichtlichen Überprüfung (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 306). Deshalb ist eine jährliche Überprüfung vorgesehen, es sei denn, das Gericht hat eine abweichende Frist bestimmt (Satz 4).

Zu Art. 6b Abs. 4 Satz 5

Die Ausnahmen von der grundsätzlichen Mitteilungspflicht sind in Satz 5 nunmehr neu geregelt. Die Mitteilung kann mit richterlicher Zustimmung dauerhaft entfallen, wenn der Grundrechtseingriff bei der Zielperson oder bei dem zu benachrichtigenden Beteiligten vertieft würde (Nr. 1) oder wenn die Identitätsfeststellung bzw. die Ermittlung des Aufenthaltsortes nur unter unverhältnismäßigem Aufwand möglich ist (Nr. 2). Diese Gründe sind als hinreichend gewichtig im Sinne des Bundesverfassungsgerichts anzusehen, um ausnahmsweise ein dauerhaftes Unterbleiben der Mitteilung zu rechtfertigen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rd.-Nr. 297). Schließlich kann im Bereich der häufig langfristigen Beobachtungsaufgaben des Verfassungsschutzes eine Mitteilung in Anlehnung an die Regelungen des Artikel 10-Gesetzes mit richterlicher Zustimmung auch dann entfallen, wenn trotz jährlicher Überprüfung nach Ablauf von fünf Jahren mit an Sicherheit grenzender Wahrscheinlichkeit anzunehmen ist, dass auch in absehbarer Zeit eine Mitteilung nicht möglich ist. Diese Regelung dient dazu, rein formale Prüfungen durch die Gerichte ohne Aussicht auf eine positive Entscheidung für eine Mitteilung zu vermeiden.

Zu Art. 6b Abs. 5 bis 7

Die Regelungen in den Abs. 5 bis 7 wurden mit Ausnahme von redaktionellen Änderungen, die die Neufassung des Art. 6a erforderlich machte, im Wesentlichen unverändert vom bisherigen Art. 6a Abs. 6 bis 8 übernommen.

Der Einsatz besonderer technischer Mittel im Schutzbereich des Art. 13 GG zum Schutz von Personen, die für das Landesamt für Verfassungsschutz tätig sind, nach - nunmehr - Art. 6b Abs. 5 unterliegt weniger strengen Anforderungen, da diese Personen

selbst von den Vorgängen in der Wohnung Kenntnis erlangen. Die verfassungsrechtlichen Voraussetzungen ergeben sich aus Art. 13 Abs. 5 GG.

Soweit Daten aus Maßnahmen nach Abs. 5 mit richterlicher Genehmigung – bei der die Rechtmäßigkeit der ursprünglichen Maßnahmen ebenso geprüft wird wie der beabsichtigte Verwendungszweck der Daten – verwertet werden, gelten wie nach bisheriger Rechtslage die Regelungen für den Umgang mit solchen Daten, die nach Art. 6a Abs. 1 erhoben wurden, entsprechend. Im Übrigen sind die Daten unverzüglich zu löschen.

Über die Anordnung von Maßnahmen nach Art. 6a Abs. 1, die Benachrichtigung von Betroffenen und über die Verwertbarkeit von Daten, die aus Maßnahmen nach Abs. 5 gewonnen wurden, entscheidet entsprechend der grundgesetzlichen Vorgaben in Art. 13 Abs. 4 GG – wie bisher – ein Einzelrichter. Ein Spruchkörpervorbehalt ist gemäß Art. 13 Abs. 3 Satz 3 GG nur bei der Wohnraumüberwachung zu repressiven Zwecken erforderlich. Nach Art. 13 Abs. 4 GG genügt die richterliche Entscheidung (vgl. Papier, in: Maunz/Dürig, Grundgesetz, Art. 13, Rn. 98). Aus der Rechtsprechung des Bundesverfassungsgerichts ergeben sich keine Bedenken gegen die bisherige Regelung (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 270 f.). Dem Einzelrichter obliegt auch die neu eingeführte Kontrolle der Verwertbarkeit von Daten nach Abs. 2 Satz 5.

### Zu § 1 Nr. 3 (Art. 6c bis Art. 6h BayVSG)

Der aus Gründen der Übersichtlichkeit nunmehr als Art. 6c neu gefasste bisherige Art. 6b regelt wie bisher Voraussetzungen der Auskunftsbefugnisse des Landesamts für Verfassungsschutz gegenüber Kreditinstituten, Fluggesellschaften, Post-, Telekommunikations- und Teledienstleistern (bzw. Anbietern von Telemedien), differenziert dabei jedoch künftig nach dem Eingriffsgewicht der Maßnahme. Verfahrensregelungen hierzu finden sich in Art. 6f und 6g. Aufgrund der bisherigen bundesrechtlichen Vorgaben in § 8 Abs. 11 BVerfSchG, der den Ländern die Auskunftsbefugnisse nur unter dem Vorbehalt eines gleichwertigen Verwaltungs- und Kontrollverfahrens zugestand, galt bislang für alle Auskunftsbefugnisse des Landesamts für Verfassungsschutz ein einheitliches, an das G 10 angelehntes Anordnungs- und Kontrollverfahren. Nach dem neuen § 8a Abs. 8 BVerfSchG gilt nun Folgendes: Die Auskunftsbefugnisse der Landesbehörden für Verfassungsschutz gegenüber Post-, Telekommunikations- und Teledienstleistern zu Verkehrsdaten stehen wie bisher unter dem Vorbehalt, dass der Landesgesetzgeber das Verfahren, die Beteiligung der G 10-Kommission, die Verarbeitung der erhobenen Daten und die Mitteilung an den Betroffenen gleichwertig wie in § 8a Abs. 5 BVerfSchG regelt und ferner eine § 8a Abs. 6 BVerfSchG gleichwertige parlamentarische Kontrolle sowie eine Verpflichtung zur Berichterstattung über die durchgeführten Maßnahmen an das Parlamentarische Kontrollgremium des Bundes unter entsprechender Anwendung von § 8a Abs. 6 Satz 1 Halbsatz 2 vorsieht. Für Auskunftsbefugnisse der Landesbehörden für Verfassungsschutz gegenüber Kreditinstituten und Fluggesellschaften besteht gemäß § 8a Abs. 8 Satz 2 BVerfSchG lediglich die Vorgabe einer dem § 8a Abs. 6 BVerfSchG gleichwertigen parlamentarischen Kontrolle. Für Auskunftsbefugnisse zu Bestandsdaten bei Postdienstleistern und Anbietern von Telemedien (Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses gespeichert worden sind) gibt es für die Länder keine Vorgaben durch das BVerfSchG mehr. Die Vorgaben des § 8a Abs. 8 BVerfSchG werden in den neuen Art. 6f und 6g umgesetzt.

Entsprechend dem unterschiedlichen Eingriffsgehalt wird in den Art. 6c Abs. 1 und 2 in den sachlichen Anordnungsvoraussetzungen zwischen Bestands- und Verkehrsdaten differenziert. Im Anordnungs- und sonstigen Verfahren wird zwischen Verkehrsdatenauskünften außerhalb (Abs. 2 Satz 1 Nrn. 1 und 2) und im Schutzbereich des Art. 10 GG (Abs. 2 Satz 1 Nrn. 3 bis 5) differenziert. Für Letztere gelten zusätzlich die besonderen Verfahrensvorkehrungen und Beschränkungen des G 10.

Diese neue auf die Schwere des Eingriffs abstellende Systematik führt bei Postbestandsdaten (etwa Postfachinhaberauskunft) zu einer Absenkung der materiellen Anordnungsvoraussetzungen und zu Verfahrensvereinfachungen. Bei Auskünften von Fluggesellschaften und Kreditinstituten führt sie ebenfalls zu Verfahrensvereinfachungen. Für Verkehrsdatenauskünfte im Schutzbereich des Art. 10 GG dagegen werden die besonderen Verfahrensvorkehrungen des G 10 beibehalten. Da die bloße Erhebung von Verkehrsdaten gegenüber der Überwachung von Kommunikationsinhalten von geringerer Eingriffsintensität ist, müssen auch die materiellen Voraussetzungen für diese Auskünfte geringer sein als für die Überwachung von Kommunikationsinhalten. Deshalb werden nicht mehr wie bisher die Voraussetzungen des § 3 Abs. 1 G 10, sondern eine „schwerwiegende Gefahr“ gefordert (Art. 6c Abs. 2).

Über die bisherigen Auskunftsbefugnisse hinausgehend sieht Art. 6c nunmehr auch Auskünfte zu Bestandsdaten von Nutzern von Telemedien (Abs. 1) und Standortdaten von mobilen Anschlüssen unabhängig von einer Verbindung (Abs. 2 Satz 1 Nr. 4) vor.

Des Weiteren wird der Anwendungsbereich der Auskunftsbefugnisse, der bei den Beobachtungsaufgaben nach Art. 3 Abs. 1 Satz 1 Nr. 1 bislang auf militante Bestrebungen beschränkt war, entsprechend der neuen Bundesregelung auf volksverhetzende Bestrebungen erweitert. Dies ist notwendig, um internationale Verflechtungen (Kommunikationsbeziehungen, Reisebewegungen der führenden Protagonisten), Finanzflüsse, Produktions- und Vertriebsstrukturen der arbeitsteilig, konspirativ und international organisierten rechtsextremistischen Vertriebszene für Hasspropaganda aufzuklären zu können. Erfasst werden auch islamistische Hassprediger und zwar auch dann, wenn ihre Propaganda nicht die Völkerverständigung betrifft, sondern sich beispielsweise gegen „Ungläubige“ richtet.

Abweichend von der bisherigen Regelung wird nunmehr im Gesetzestext selbst klargestellt, dass den Auskunftsbefugnissen des Landesamts für Verfassungsschutz eine Auskunftspflicht der Unternehmen korrespondiert (Abs. 1 und 2). Dies entspricht dem Gebot der Normenklarheit. Nach der Begründung des Terrorismusbekämpfungsergänzungsgesetzes (BT-Drs. 16/2921, S. 14) soll zwar von einer Klärung der bestrittenen Auskunftspflicht auf Bundesebene abgesehen werden, da nach dem Evaluierungsbericht bislang keine Probleme aufgetreten seien. Den weiteren Ausführungen der Begründung ist jedoch zu entnehmen, dass der Bundesgesetzgeber selbst von einer Auskunftspflicht ausgeht. Aus Gründen der Klarstellung wird in Fortführung der bisherigen Rechtslage, aber über § 8a BVerfSchG hinaus ausdrücklich die Unentgeltlichkeit der Auskünfte festgeschrieben. Im durch das Terrorismusbekämpfungsgesetz neu formulierten § 8a BVerfSchG ist die Frage eines Entgelts für Auskünfte keiner Regelung zugeführt worden und inhaltlich offen geblieben. Der Aufwand für Regelung und Durchführung eines Erstattungsverfahrens stünde außer Verhältnis zu den mit den Auskünften verbundenen eher geringen Belastungen. Unberührt von der Unentgeltlichkeit bleiben die Entschädigungen nach § 113 TKG aufgrund einer noch zu erlassenden Verordnung nach § 110 Abs. 9

TKG, da die hiervon betroffenen Auskünfte nicht in Art. 6c Abs. 1 und 2 geregelt sind.

Durch das Inkrafttreten des Telemediengesetzes zum 01.03.2007 ist der Begriff der Teledienste im Begriff der Telemedien aufgegangen. Die noch an der früheren Rechtslage orientierte Terminologie des § 8a BVerfSchG ist insoweit nicht mehr aktuell. Es wird vorliegend daher nicht mehr der Begriff der Teledienste verwendet, sondern durch den der Telemedien ersetzt.

Auch für den Einsatz des IMSI-Catchers werden in Art. 6c Abs. 4 die Voraussetzungen stärker an dessen Eingriffsgewicht ausgerichtet. Da hierbei keine Überwachung von Kommunikationsinhalten erfolgt und auch kein Eingriff in den Schutzbereich des Art 10 GG vorliegt (vgl. BVerfG vom 22.08.2006 – 2 BvR 1345/03), erscheinen die bislang nach Art. 6b Abs. 4 geltenden Sachvoraussetzungen nach dem G 10 nicht angemessen.

#### Zu Art. 6c Abs. 1

Der neue Abs. 1 trifft in Parallele zu § 8a BVerfSchG eine gesonderte Regelung für Postbestandsdaten und Bestandsdaten von Telemedienanbietern. Dabei wird die Begrifflichkeit an die durch das Inkrafttreten des Telemediengesetzes geänderte Rechtslage angepasst und nicht mehr der Begriff der Teledienste verwendet, der im Begriff der Telemedien aufgegangen ist. Die Auskunftspflicht zu diesen Bestandsdaten besteht entsprechend der Auskunftspflicht zu Telekommunikationsbestandsdaten nach § 113 TKG und zur bereits bestehenden Regelung zu Telemedienbestandsdaten in § 14 TMG unter der Voraussetzung, dass die Auskunft zur Aufgabenerfüllung des Landesamts für Verfassungsschutz erforderlich ist. Damit wird die Schwelle für Auskünfte für Postbestandsdaten, die nach dem bisherigen Abs. 1 Satz 1 in Verbindung mit dem bisherigen § 8 Abs. 6 BVerfSchG an die hohen Sachvoraussetzungen des G 10 geknüpft war, gesenkt. Die bisher verlangten Voraussetzungen des § 3 Abs. 1 G 10 sind auf die Überwachung von Kommunikationsinhalten zugeschnitten, für bloße Bestandsdatenauskünfte aber unter Verhältnismäßigkeitserwägungen nicht geboten. Mit der Angleichung der Schwelle für Auskünfte an § 113 TKG und der uneingeschränkten Erstreckung der Auskunft über Postbestandsdaten auf alle Beobachtungsaufgaben des Art. 3 Abs. 1 Satz 1 wird ein eigenständiger Anwendungsbereich auch für Auskünfte über Postbestandsdaten eröffnet.

Als künftige Anwendungsfälle kommen etwa Postfächer in Betracht, die in rechtsextremistischen Publikationen teils als Kontaktadressen benannt werden. Postfächer spielen ferner bei der Bestellung und dem Vertrieb von rechtsextremistischer Skinhead-Musik und Fancines eine Rolle.

Die neu geschaffene Auskunftspflicht zu Telemedienbestandsdaten ergänzt die bereits bestehende Auskunftspflicht zu Telemediaverkehrsdaten (bisher Abs. 1 Satz 1 in Verbindung mit § 8 Abs. 8 BVerfSchG a. F.). Nachdem die Gesetzesbegründung zu § 14 TMG ausdrücklich von einer „Anordnung der zuständigen“ Stellen ausgeht, wird die Vorschrift zur Vermeidung von Zweifelsfragen in Ergänzung zur bundesrechtlichen Regelung so formuliert, dass das Landesamt für Verfassungsschutz auch als zuständige Stelle für eine solche Anordnung festgelegt wird. Als Anwendungsfälle kommen etwa Auskünfte über Vertragsdaten bei Internetauktionshäusern und -tauschbörsen zum Handel und Vertrieb volksverhetzender Propagandamaterialien in Betracht. So gibt es Internetunternehmen, die die Möglichkeit eröffnen, auf ihrer Plattform einen eigenen virtuellen „Verkaufsraum“ einzurichten. Entsprechend wäre die Information relevant, ob eine Person bei solchen Unternehmen als so genannter „Powerseller“ registriert ist, also regelmäßig Waren in größerem Umfang an- und verkauft. Hieraus können eventuelle Rückschlüsse auf die Beschaffung von Finanzmitteln gezogen werden.

Zu Art. 6c Abs. 2

Der neue Abs. 2 regelt im Gleichklang mit § 8a BVerfSchG nunmehr die materiellen Voraussetzungen für Verkehrsauskünfte gegenüber Kreditinstituten, Fluggesellschaften, Post-, Telekommunikationsleistern sowie Anbietern von Telemedien. Damit wird von der bisherigen Regelung abgewichen, die in Abs. 1 Satz 1 lediglich auf die entsprechenden Regelungen des bisherigen § 8 Abs. 5 bis 8 BVerfSchG verwiesen hat, und eine eigenständige Regelung im Landesrecht getroffen. Dabei werden – abweichend vom bisherigen Recht, das bei den materiellen Voraussetzungen zwischen Auskünften gegenüber Kreditinstituten und Fluggesellschaften einerseits (Abs. 1 Satz 1 in Verbindung mit dem bisherigen § 8 Abs. 5 und 7 BVerfSchG a. F.) und Auskünften gegenüber Post- und Telekommunikationsdienstleistern sowie Anbietern von Telemedien andererseits (Abs. 1 Satz 1 in Verbindung mit § 8 Abs. 6 und 8 BVerfSchG a. F.) differenziert hat –, nunmehr alle Auskunftsbefugnisse an die materiellen Voraussetzungen geknüpft, die bislang für Auskunftsbefugnisse gegenüber Kreditinstituten und Fluggesellschaften galten. Entsprechend dem neuen § 8a Abs. 2 Satz 1 BVerfSchG besteht künftig für alle Auskunftsbefugnisse die einheitliche Sachvoraussetzung, dass tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in Art. 3 Abs. 1 Satz 1 genannten Schutzgüter bestehen (Satz 1). Dies führt dazu, dass die Einsatzschwelle für Verkehrsauskünfte gegenüber Post-, Telekommunikationsdienstleistern sowie Anbietern von Telemedien, für die bislang die Voraussetzungen des § 3 Abs. 1 G 10 galten (bisheriger Abs. 1 Satz 1 in Verbindung mit bisherigem § 8 Abs. 6 und 8 BVerfSchG), gesenkt wird. Maßgeblich ist, dass keine Kommunikationsinhalte erhoben werden und eine andere abstrakte Verhältnismäßigkeitsabwägung als nach dem G 10 angezeigt ist. Der spezifischen Sensibilität dieser Informationen wird dadurch Rechnung getragen, dass es bei den besonderen Verfahrensvorkehrungen des G 10 bleibt (Art. 6f).

Die Voraussetzung der „schwerwiegenden Gefahr“ im Satz 1 enthält eine schutzgutbezogene Qualifizierung. Erforderlich sind tatsächliche Anhaltspunkte für solche Bestrebungen oder Tätigkeiten, die geeignet sind, die in Art. 3 Abs. 1 Satz 1 genannten Schutzgüter erheblich zu beschädigen. Dies ist unter den Voraussetzungen des § 3 Abs. 1 G 10 der Fall, geht aber insofern darüber hinaus, als kein konkreter Straftatenbezug gegeben sein muss. Als Beispiele sind organisierte, erhebliche Geldsammlungen zur Unterstützung militanter Organisationen oder proliferationsrelevante Sachverhalte anzuführen. Schwerwiegende Gefahren gehen insbesondere von Bestrebungen aus, die die qualifizierenden Voraussetzungen des Satz 2 erfüllen.

Der Entwurf nimmt in Umsetzung des § 113b TKG Bezug auf § 113a TKG. Dort werden Mindestspeicherfristen für Verkehrsdaten festgelegt. Nach § 113b TKG ist ein Zugriff auf solche Daten nur zulässig, wenn § 113a TKG in der entsprechenden Befugnisnorm zitiert wird. Der Beschluss des Bundesverfassungsgerichts vom 11.03.2008 (1 BvR 256/08), mit der im Wege der einstweiligen Anordnung eine Anwendung des § 113b TKG bis zu einer Entscheidung in der Hauptsache teilweise außer Kraft gesetzt wurde, steht der Regelung nicht entgegen. Der Beschluss des Bundesverfassungsgerichts schränkt die Datennutzung nur für repressive Zwecke ein. Eine Datennutzung zu präventiven Zwecken wurde nicht näher geprüft.

Die neue – § 8a Abs. 2 Satz 1 Nr. 1 BVerfSchG neu weitgehend entsprechende – Formulierung der Auskunftgegenstände bei Auskünften von Fluggesellschaften in Satz 1 Nr. 1 verdeutlicht, dass sich die „Umstände“ auf die in Anspruch genommenen Transportleistungen beziehen. Als Beispiele für solche Umstände von Transportleistungen werden im Gesetz Zeitpunkt von Abfertigung und Abflug und Buchungsweg genannt. Durch die von § 8a Abs. 2

Satz 1 Nr. 1 BVerfSchG geringfügig abweichende Formulierung „von Kunden“ statt „des Kunden“ soll eindeutig klargestellt werden, dass im Einzelfall auch die Herausgabe von Passagierlisten von der Vorschrift mit umfasst ist.

Bei den bisher in einem Absatz (bisheriger Abs. 1 Satz 1 in Verbindung mit § 8 Abs. 8 BVerfSchG a.F.) geregelten Auskunftsbefugnissen gegenüber Telekommunikations- und Teledienstleistern wird entsprechend der bundesrechtlichen Regelung an die fachrechtlichen Regelungen zu Verkehrsdaten (§ 96 TKG) und Nutzungsdaten (§ 15 TMG) angeknüpft und jeweils eine eigenständige Regelung in den Nrn. 4 und 5 vorgenommen. Die Verkehrs- und Nutzungsdaten werden dabei bedarfsbezogen eingeschränkt: Bei der Auskunftspflicht von Telekommunikationsdienstleistern (Nr. 4) bleiben die zur Entgeltabrechnung notwendigen Verkehrsdaten (§ 96 Abs. 1 Nr. 5 Alternative 2 TKG) ausgenommen. Die Auskunftspflicht von Anbietern von Telemedien (Nr. 5) wird auf die in § 15 TMG konkret aufgeführten Datenarten beschränkt.

Die neue Formulierung in Nr. 4 „und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten“ statt der bisherigen Formulierung „Kennung des anrufenden und angerufenen Anschlusses“ (§ 8 Abs. 8 Satz 3 Nr. 1 BVerfSchG a.F.) verdeutlicht die ursprüngliche Absicht des Gesetzgebers, dass die Auskunftspflicht von Telekommunikationsdienstleistern auch die „Stand-by-Daten“ von Mobiltelefonen umfasst, weil einem Mobilfunknetz zum Zweck des Aufbaus einer Telekommunikation zu einem Mobiltelefon, dessen Standort – zumindest grob – bekannt sein muss. Zu einem aktiv geschalteten Mobiltelefon können also unabhängig vom Verbindungsaufbau Angaben gemacht werden. Standortdaten eines Mobiltelefons im Fall einer konkreten Verbindung sind durch die Verweisung auf § 96 Abs. 1 Nr. 1 TKG von der Auskunftspflicht umfasst.

Im Unterschied zur bisherigen Bundesregelung standen dem Landesamt für Verfassungsschutz die neu geschaffenen Auskunftsbefugnisse schon bisher auch für die Beobachtung des gewaltbezogenen Inlandsextremismus nach Art. 3 Abs. 1 Satz 1 Nr. 1 BayVStG zu. In der Begründung zum Gesetz zur Änderung des Bayerischen Verfassungsschutzgesetzes vom 24. Dezember 2002 (LT-Drs. 14/10180) war hierzu ausgeführt: „Es ist nicht begründbar, die genannten Auskunftsbefugnisse zwar zur Beobachtung von gewaltgeneigten Bestrebungen einzuräumen, die die ausländischen Belange der Bundesrepublik gefährden, nicht jedoch bei gewaltgeneigten Bestrebungen, die die freiheitliche demokratische Grundordnung, die Sicherheit des Bundes oder eines Landes gefährden.“ Aufgrund neuer Entwicklungen, insbesondere dem Phänomen des home-grown-terrorism sowie der Eignung und Angemessenheit dieser Befugnisse auch für die Beobachtungsaufgaben nach § 3 Abs. 1 Nr. 1 BVerfSchG, wurden die Auskunftsbefugnisse des Bundesamts für Verfassungsschutz durch das Terrorismusbekämpfungsergänzungsgesetz auch auf dessen Aufgaben nach § 3 Abs. 1 Nr. 1 BVerfSchG erstreckt, außerhalb von Bestandsdaten allerdings beschränkt auf volksverhetzende und militante Bestrebungen (§ 8a Abs. 2 Satz 2 BVerfSchG neu). Als volksverhetzende Bestrebungen im Sinn des Art. 3 Abs. 1 Satz 1 Nr. 1 gelten dabei in Anlehnung an die Regelung des Aufenthaltsgesetzes zu „Hasspredigern“ (§ 55 Abs. 2 Nr. 8 Buchst. b AufenthG) und der Aufgabenbestimmung in Art. 3 Abs. 1 Satz 1 Nr. 4 solche Bestrebungen, die bezwecken und aufgrund ihrer Wirkungsweise geeignet sind, zu Hass- oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumdungen anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören (Abs. 2 Satz 2 Nr. 1).

In der Nr. 2 wird der bereits im bisherigen Art. 6b Abs. 2 Satz 1 enthaltene Begriff der Vorbereitungshandlung in Anlehnung an die vereinsgesetzlichen Verbotstatbestände des § 14 Abs. 2 Nr. 4 und 5 VereinsG konkretisiert.

Zu Art. 6c Abs. 3

Der neu eingefügte und § 8a Abs. 3 BVerfSchG entsprechende Abs. 3 grenzt, teils in Anlehnung an die Regelungen im G 10, den Kreis der Personen ein, deren Daten durch die eingriffsgewichtigeren Maßnahmen nach Abs. 2 erhoben werden dürfen. Der Begriff „Personen“ schließt Personenvereinigungen und juristische Personen (z.B. Konto einer extremistischen Organisation) mit ein.

Nr. 1 bezeichnet die eigentlichen Zielpersonen der Maßnahmen. Zielpersonen können danach – ungeachtet des Gewichts und der Dauer des Gefährdungsbeitrags – alle Personen sein, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie zu einer schwerwiegenden Gefährdung der Verfassungsschutzgüter beitragen. Nachdem es bereits um schwerwiegende Gefahren geht wird, anders als in § 8 Abs. 3 BVerfSchG, darauf verzichtet zusätzlich eine Nachdrücklichkeit des Förderns derartiger Gefahren zu verlangen. Personenbezogene Daten der Zielperson, die zugleich als personenbezogene Daten anderer Personen zu bewerten sind dürfen mit erhoben werden, soweit dies für die verfolgte Aufgabe erforderlich ist. So darf etwa eine Kontoauskunft nur zum Konto der Zielperson eingeholt werden, dabei darf dann aber auch erhoben werden, an wen und von wem Überweisungen erfolgt sind. Im Übrigen ist das Vorliegen tatsächlicher Anhaltspunkte ausreichend. Liegen Hinweise dafür vor, dass ein Terrorist einen bestimmten Flug genutzt hat, liegen damit solche Anhaltspunkte zu den Passagieren dieses Fluges vor, die dazu berechtigen, die Übermittlung der Passagierliste zu verlangen, wenn dies zur weiteren Klärung erforderlich ist, weil zunächst unbekannt ist, welchen Namen der Terrorist bei seiner Flugreise verwendet hat. Ein Fördern schwerwiegender Gefahren durch Passagiere ergibt sich in diesem Fall zwar nicht aus der Tatsache dass ohne Wissen der Passagiere Terroristen an Bord sind, es bestehen dann jedoch für jeden einzelnen Passagier tatsächliche Anhaltspunkte, dass er der noch nicht enttarnte Terrorist sein kann.

Die Nr. 2 orientiert sich an der Regelung des § 3 Abs. 2 Satz 2 G 10 und überträgt den zugrunde liegenden Gedanken im Buchstaben a auch auf die Auskünfte gegenüber Kreditinstituten, Fluggesellschaften und Teledienstleistern.

Zu Art. 6c Abs. 4

Satz 1 verweist in Parallele zu § 9 Abs. 4 BVerfSchG hinsichtlich der materiellen Voraussetzungen für den Einsatz des IMSI-Catchers nunmehr auf Abs. 2 und nicht mehr wie bisher auf die Voraussetzungen nach § 3 Abs. 1 G 10. Dabei ist maßgeblich, dass nicht der Inhalt der Kommunikation überwacht wird. Die Vorschrift ermöglicht nicht das Abhören von Gesprächen mit Hilfe des IMSI-Catchers. Deshalb sind die nach dem G 10 aufgestellten Sachvoraussetzungen nicht angemessen. Der Einsatz des IMSI-Catchers dient in erster Linie lediglich der Vorbereitung von G 10-Maßnahmen bzw. der Vorbereitung von Verbindungsauskünften. Daneben ermöglicht er die ungefähre Ortung eines aktiv geschalteten Mobiltelefons. Unter diesem Gesichtspunkt sind an die Maßnahme auch keine höheren Voraussetzungen zu knüpfen. Durch die Verweisung auf die Voraussetzungen des Abs. 2 wird der Anwendungsbereich des IMSI-Catchers der bislang schon für militante Bestrebungen im Sinn des bisherigen Abs. 2 galt, nunmehr auch auf volksverhetzende Bestrebungen ausgedehnt. Auch bei derartigen volksverhetzenden Bestrebungen sind Verbindungen zwischen Zielpersonen und deren Aufenthalt von gleichem Aufklärungsinteresse.

Satz 2 regelt entsprechend dem bisherigen Abs. 4 Satz 2 die Subsidiarität dieser Maßnahme.

Der neue Satz 3 trifft eine Regelung zur Richtung der Maßnahme. Es wird dabei auf die entsprechenden Regelungen bei Auskünften nach Abs. 2 verwiesen. Die Regelung des Satz 5 entspricht der des bisherigen Art. 6b Abs. 4 Satz 3. Abweichend von der bisherigen Regelung in Art. 6b Abs. 4 Satz 4, der die Verwendung von aus technischen Gründen unvermeidbar erhobener Daten Dritter ausschließlich zur Verhütung und Verfolgung von Straftaten im Sinne des § 138 StGB zuließ, normiert der neue Satz 5, entsprechend der Regelung auf Bundesebene, ein absolutes Verwendungsverbot dieser Daten. Ihre Nutzung – etwa zur Einholung der Rufnummer oder zur sonstigen Herstellung eines Personenbezugs – ist verboten.

**Zu Art. 6d**

In Art 6d wird für das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes mit dem verdeckten Einsatz technischer Mittel außerhalb von Wohnräumen und außerhalb des Schutzbereichs von Art. 10 GG eine ausdrückliche gesetzliche Regelung geschaffen. Es handelt sich hier einem Sonderfall des Einsatzes nachrichtendienstlicher Mittel im Sinn von Art. 6 BayVSG. Auch wenn sich die Eingriffsintensität einer solchen Maßnahme im Regelfall nicht wesentlich von der Eingriffstiefe bei anderen unbenannten nachrichtendienstlichen Mitteln unterscheidet, kann sich im konkreten Einzelfall, insbesondere auch nach Auswertung der Maßnahme eine höhere Intensität eines Grundrechtseingriffs ergeben. Dabei ist davon auszugehen, dass die konkrete Grundrechtsintensität einer derartigen Maßnahme vor allem von den jeweiligen Umständen des Einzelfalls abhängt. Um dem Rechnung zu tragen, stellt Art. 6d nochmals ausdrücklich auf die besondere Berücksichtigung des Verhältnismäßigkeitsgrundsatzes im Einzelfall ab.

Nähere Verfahrensregelungen, die auch einen sachgerechten Grundrechtsschutz sicherstellen sollen finden sich in Art. 6f.

**Zu Art. 6e**

Abs. 1 enthält eine Befugnis, die das Landesamt für Verfassungsschutz dazu ermächtigt, mit technischen Mitteln verdeckt auf informationstechnische Systeme zuzugreifen, um gespeicherte Daten sowie Zugangsdaten zu erheben. Diese Befugnis trägt den Anforderungen des Bundesverfassungsgerichts an einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Rechnung (Entscheidung vom 27.02.2008 (1 BvR 307/07)). Insbesondere setzt ein Eingriff das Vorliegen tatsächlicher Anhaltspunkte für konkrete Gefahren für ein überragend wichtiges Rechtsgut voraus, es wird ein grundsätzlicher Richtervorbehalt eingeführt und es sind weitreichende Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung vorgesehen.

Der in der öffentlichen Diskussion in diesem Zusammenhang bislang vielfach benutzte Begriff der „Online-Durchsuchung“ wird bewusst vermieden, da die Datenerhebung des Verfassungsschutzes, anders als eine Durchsuchung im Rahmen einer Strafverfolgung oder zur Gefahrenabwehr durch die Polizei, nicht unmittelbar darauf abzielt, eine Bestrafung eines Straftäters oder weitere Exekutivmaßnahmen der Polizei zu ermöglichen. Zielrichtung ist vielmehr die Nachrichtenbeschaffung. Der Begriff der Durchsuchung würde hier unrichtige Assoziationen hervorrufen. Es handelt sich bei der Maßnahme vielmehr um einen Sonderfall der Datenerhebung mit nachrichtendienstlichen Mitteln.

Satz 1 legt fest, dass das Landesamt für Verfassungsschutz verdeckt mit technischen Mitteln auf informationstechnische Systeme zugreifen darf mit dem Ziel der Datenerhebung. Die Ergänzung

um die Zugangsdaten soll sicherstellen, dass die notwendigen technischen Maßnahmen ergriffen werden dürfen, um eine Datenerhebung zu ermöglichen. Insbesondere sollen auch Tastatureingaben, über die etwa Kennwörter eingegeben werden, um auf kryptierte oder anderweitig vor unberechtigtem Zugriff geschützte Daten zugreifen zu können, ebenso umfasst sein wie Daten zur Überwindung anderer Zugangssicherungen. Namentlich erfasst hiervon ist auch der Einsatz sog. Keylogger, die darauf abzielen, entsprechende Zugangscodes, die nicht zwingend in Speichermedien enthalten sind, zu ermitteln.

Die Befugnis besteht nur bei Erfüllung hoher materiellrechtlicher Voraussetzungen. In Umsetzung des Urteils des Bundesverfassungsgerichts und in Bezugnahme hierauf wird zum einen das „Vorliegen tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut“ verlangt (vgl. Rn 242 und 249 des Urteils). Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen (Rn 247). Es genügt, dass bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein solches Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt (Rn 242). Zur weiteren Konkretisierung der Eingriffsschwelle und möglicher Eingriffstatbestände wird zusätzlich verlangt, dass die Voraussetzungen des Art. 6a Abs. 2, der nähere materiellrechtliche Anforderungen bei einer Wohnraumüberwachung aufstellt, erfüllt werden. Es müssen daher zusätzlich tatsächliche Anhaltspunkte für den Verdacht der Planung und Begehung von Straftaten eines eng umrissenen Straftatenkatalogs vorliegen, aus denen sich die jeweilige Gefährdung im Einzelfall ergibt.

Satz 1 betont, dass eine derartige Datenerhebung nur einzelfallbezogen durchgeführt werden darf. Das ergäbe sich zwar bereits aus den weiteren Anordnungsvoraussetzungen, die eine Einzelfallprüfung voraussetzen. Zur Verdeutlichung, dass die genannte Form der Datenerhebung auf Einzelfälle beschränkt ist und keine flächendeckende Datenerhebung aus Speichermedien ermöglicht wird, werden dennoch die Worte „im Einzelfall“ im Gesetzestext aufgenommen.

Auch wenn bei den genannten Voraussetzungen vom Grundsatz her stets auch eine polizeiliche Maßnahme in Betracht käme, bedarf es zur Wahrnehmung der gesetzlich zugewiesenen Aufgaben des Landesamts für Verfassungsschutz gleichwohl auch einer eigenständigen Befugnis des Landesamts für Verfassungsschutz. Maßnahmen müssen im Einzelfall bereits ergriffen werden, wenn ein Gefahren Eintritt in näherer Zukunft sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt. In einem solchen Stadium bestehen die zu treffenden Maßnahmen vor allem in einer weiteren Aufklärung der konkreten Gefahrenlage, die im jeweiligen Einzelfall aus Gründen der Effektivität oder des Quellenschutzes bei der Sicherheitsbehörde verbleiben soll, die schon bisher mit dem Sachverhalt befasst war. Dabei ist auch zu berücksichtigen, dass sich die tatsächlichen Anhaltspunkte für entsprechende konkrete Gefahren aus Hinweisen anderer Nachrichtendienste ergeben können, für die keine Weitergabebefugnis an andere Behörden besteht. Damit wird sichergestellt, dass die auf Grundlage dieses Gesetzes erhobenen Informationen für weitere gefahrenabwehrende Maßnahmen der Polizei an diese übermittelt werden können.

Satz 2 stellt klar, dass die Maßnahme nur eingesetzt werden darf, wenn eine Sachverhaltsaufklärung sonst aussichtslos oder wesent-

lich erschwert wäre und sich nur gegen Verdächtige und ihre Nachrichtenmittler richten darf.

Satz 3 legt die Richtung der Maßnahme fest. Sie darf sich nur gegen Personen richten, die im Verdacht stehen, Straftaten des Straftatenkatalogs nach Art. 6a Abs. 2 zu planen oder zu begehen, sowie gegen Nachrichtenmittler. Nachrichtenmittler sind Personen, die für Verdächtige in diesem Sinn bestimmte Mitteilungen oder von diesen herrührende Mitteilungen entgegennehmen oder entgegengenommen haben oder solche Mitteilungen weitergeben oder weitergegeben haben.

Satz 4 trägt dem Gesichtspunkt des Schutzes der Berufsheimnisträger dadurch Rechnung, dass diese, soweit sie ein Zeugnisverweigerungsrecht nach den §§ 53, 53a StPO besitzen, als Nachrichtenmittler nicht Zielperson einer verdeckten Online-Datenerhebung sein dürfen.

Satz 5 stellt klar, dass selbst in Fällen, in denen zunächst nicht erkennbar war, dass das Vertrauensverhältnis zu einem Berufsheimnisträger betroffen ist, die weitere Durchführung der Maßnahme unzulässig ist, soweit in ein durch die §§ 53, 53a StPO geschütztes Vertrauensverhältnis eingegriffen wird, es sei denn, die Maßnahme ist gegen Berufsheimnisträger selbst gerichtet oder sie ist erforderlich, um eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person abzuwehren.

Satz 6 trägt dem Kernbereichsschutz auf der Ebene der Datenerhebung Rechnung. Eine Maßnahme ist unzulässig, wenn nicht alle informationstechnischen und ermittlungstechnischen Möglichkeiten ergriffen werden, um die Erhebung von Kernbereichsdaten zu vermeiden. Das Bundesverfassungsgericht hält es zwar für praktisch unvermeidbar, beim heimlichen Zugriff auf ein informationstechnisches System Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, und betont daher den hinreichenden Schutz in der Auswertungsphase (Rn 277). Gleichzeitig wird jedoch auf die Zweistufigkeit des Kernbereichsschutzes verwiesen und ausgeführt, dass die gesetzliche Regelung darauf hinzuwirken hat, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen (Rn 281).

Satz 7 stellt überdies grundsätzlich klar, dass Online-Datenerhebungen insoweit unzulässig sind, als sie in den Kernbereich privater Lebensgestaltung eingreifen und dies erkennbar wird. Dies gilt dann nicht, wenn Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern und solche Daten somit dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen. Dies entspricht der Auffassung des BVerfG in seinem Urteil von 27.02.2008 (Rn 281)

Absatz 2 normiert die Befugnis zum Einsatz von technischen Mitteln zur Identifikation und Lokalisation von informationstechnischen Systemen. Diese Regelung ist angesichts der Entwicklungen auf dem Gebiet der Informationstechnik erforderlich, da bei der Planung und Begehung von schwerwiegenden Straftaten, die überragend wichtige Rechtsgüter bedrohen, insbesondere von Angehörigen gewaltbereiter extremistischer Gruppen zunehmend informationstechnische Systeme eingesetzt werden, deren spezifische Kennungen und Standorte den Sicherheitsbehörden nicht bekannt sind. Eine Spezifizierung der informationstechnischen Systeme ist allerdings im Regelfall Voraussetzung für die Durchführung einer Maßnahme nach Abs. 1. Daneben ist die Bezeichnung des informationstechnischen Systems Voraussetzung für eine Anordnung des Zugriffs auf informationstechnische Systeme zur Datenerhebung, so dass die Befugnis zur Ermittlung der erforder-

lichen Daten eingeräumt werden muss. Gleiches gilt für die Bestimmung des Standorts eines informationstechnischen Systems. Der Einsatz von Geräten, wie etwa des sog. „WLAN-Catchers“ zur Bestimmung von spezifischen Kennungen bzw. des Standortes eines informationstechnischen Systems, wird an die strengen Voraussetzungen des Abs. 1 geknüpft, da er zur Vorbereitung einer der dort genannten Maßnahmen dient. Dies gilt auch für die Subsidiaritätsregelung in Abs. 1 Satz 2. Soweit aus technischen Gründen unvermeidbar Daten Dritter erhoben werden, sind diese unverzüglich zu löschen.

Umfangreiche verfahrensrechtliche Regelungen finden sich in Anlehnung an das Verfahren bei der Wohnraumüberwachung in Art. 6f Abs. 5 in Verbindung mit Art. 6b. Dadurch wird eine intensive unabhängige Kontrolle des Instruments der verdeckten Datenerhebung aus informationstechnischen Systemen mit technischen Mitteln ermöglicht und sichergestellt, dass sein Einsatz auf die notwendigen Fälle eng begrenzt bleibt. Gleichzeitig wird hier den Rechten der Betroffenen und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung getragen.

#### Zu Art. 6f

Art. 6f sieht für verschiedene nachrichtendienstliche Maßnahmen mit erhöhter Eingriffsintensität besondere Verfahrensregelungen vor, um auch durch das jeweilige Verfahren einen angemessenen Grundrechtsschutz sicherzustellen:

Abs. 1 sieht für Auskunftersuchen nach Art. 6c Abs. 2 und den Einsatz des IMSI-Catchers zwingend einen entsprechend begründeten Antrag durch den Präsidenten des Landesamtes oder seinen Vertreter vor. Die Entscheidung über diesen Antrag trifft das Staatsministerium des Innern. Damit wird eine zusätzliche verfahrensrechtliche Beschränkung aufgestellt, mit der Sorge dafür getragen wird, dass Grundrechtsbeeinträchtigungen auf das unvermeidlich gebotene Maß beschränkt bleiben. Abweichend von der neuen Bundesregelung in § 8a Abs. 4 BVerfSchG gilt der strikte Antragsvorbehalt für Behördenleiter bzw. dessen Vertreter sowie die Anordnungszuständigkeit des Innenministeriums für alle Auskünfte nach Art. 6c Abs. 2.

Abs. 2 legt für die in Abs. 1 genannten Maßnahmen eine Gültigkeitsdauer von getroffenen Anordnungen von maximal drei Monaten fest. Soweit bei Auskunftersuchen nach Art. 6c Abs. 2 Dritte als Verpflichtete eingeschaltet sind, dürfen diesen Daten übermittelt werden, soweit dies zur Erfüllung der Verpflichtung erforderlich ist. Die Regelungen zur Anordnungsdauer (Satz 1) und zur Verlängerbarkeit der Anordnung (Satz 2) orientieren sich an der Regelung des § 10 Abs. 5 G 10. Der neue Satz 3 bestimmt entsprechend § 10 Abs. 6 G 10, dass dem Verpflichteten lediglich der Anordnungstenor, nicht auch die Begründung, mitzuteilen ist. Satz 4 entspricht dem bisherigen Abs. 1 Satz 10.

In Abs. 3 wird für Auskunftersuchen nach Art. 6c Abs. 2 Satz 1 Nr. 3 bis 5, den Einsatz des IMSI-Catchers und für verdeckte Online-Datenerhebungen ein Verfahren festgelegt, das dem G 10-Verfahren entspricht. Entsprechende Anordnungen des Staatsministeriums des Innern dürfen danach erst dann vollzogen werden, wenn die G 10-Kommission zugestimmt hat. Bei Gefahr in Verzug kann das Staatsministerium des Innern zwar einen Sofortvollzug anordnen, muss aber der Kommission eine nachträgliche Entscheidung ermöglichen. Soweit die Kommission Maßnahmen billigt, sind getroffene Maßnahmen unverzüglich aufzuheben, die erhobenen Daten unterliegen dann einem absoluten Verwendungsverbot und sind unverzüglich zu löschen. Entsprechend der Regelung des Artikel 10-Gesetzes (und des AGG 10) hat die G 10-Kommission umfassende Kontrollbefugnisse, Auskunftsrechte und Einsichtsrechte in Unterlagen. Es gelten die besonderen Da-

tenverarbeitungsregelungen des Artikel 10-Gesetzes mit Prüf-, Kennzeichnungs- und Löschungspflichten sowie besonderen Übermittlungsregelungen mit entsprechender Zweckbindung. Die Betroffenen sind in gleicher Weise wie bei einer Maßnahme nach dem G 10-Gesetz zu unterrichten, auf eine solche Unterrichtung kann nur nach den dortigen Maßgaben verzichtet werden.

Auch wenn beim Einsatz des IMSI-Catchers kein Eingriff in Art. 10 GG vorliegt (vgl. BVerfG vom 22.08.2006 – 2 BvR 1345/03), wird – neben der spezifischen Einsatzschwelle einer schwerwiegenden Gefahr für die Verfassungsgut – wegen der engen Verknüpfung zu Verkehrsdatenauskünften und der Parallelregelung in § 9 Abs. 4 BVerfSchG an den besonderen Verfahrensvorkehrungen des G 10 festgehalten.

Bei Auskünften nach Art. 6c Abs. 2 Nrn. 1 und 2 (u.a. von Luftfahrtunternehmen, Kreditinstituten) findet Abs. 2 keine Anwendung. Es wird damit auch auf eine § 8a Abs. 4 Satz 7 BVerfSchG entsprechende Regelung über eine Benachrichtigung der Betroffenen verzichtet. Wegen der geringen Intensität des mit dieser Datenerhebung verbundenen Grundrechtseingriffs soll im Interesse der Wahrung der Arbeitsfähigkeit des Verfassungsschutzes auf eine Benachrichtigung und den damit verbundenen Prüf- und Ermittlungsaufwand verzichtet werden.

Für die Auskünfte nach Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5 ergibt sich die Ausgestaltung des Verfahrens aus den Vorgaben des neuen § 8a Abs. 8 BVerfSchG, der auch eine der Bundesregelung gleichwertige Regelung des Verfahrens im Landesrecht fordert.

Abs. 4 Satz 1 sieht für Maßnahmen nach Art. 6d (Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb des Schutzbereichs von Art. 10 und 13 GG) vor, dass Daten hieraus nur mit Genehmigung durch den Präsidenten des Landesamtes oder seines Vertreters erhoben und verwendet werden dürfen. Dies trägt vor allem dem Umstand Rechnung, dass sich bei solchermaßen erhobenen Daten nach Auswertung entsprechender Aufzeichnungen eine besondere Grundrechtsintensität im Einzelfall ergeben kann, dem durch diese verfahrensrechtliche Verwendungsbeschränkung Rechnung getragen wird.

Die Sätze 2 bis 6 treffen eine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung für Maßnahmen nach Art. 6d. Aufgrund des besonderen Charakters der Maßnahmen ist es nicht völlig unwahrscheinlich, dass im Einzelfall in den Kernbereich privater Lebensgestaltung eingegriffen wird. Daten aus diesem Kernbereich dürfen grundsätzlich nicht verwendet werden und sind zu löschen, ebenso wie Daten, bei denen die Voraussetzungen für ihre Erhebung nicht vorgelegen haben. Eine ausnahmsweise Verwendung kommt ausschließlich in Betracht zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person. Der Begriff der Gegenwartigkeit ist in gleicher Weise zu verstehen wie bei Art. 6a Abs. 6 Satz 5. Eine solche ausnahmsweise Verwendung von Kernbereichsdaten bedarf der Zustimmung der G 10-Kommission. In Eilfällen kann die Amtsleitung des Landesamts für Verfassungsschutz die Entscheidung treffen, die Unterrichtung und Entscheidung der Kommission ist dann unverzüglich nachzuholen. Soweit Kernbereichsdaten ausnahmsweise verwendet werden, sind sie zu kennzeichnen und die Betroffenen über die Maßnahme zu unterrichten.

Abs. 5 regelt großteils durch Verweisung auf die Vorschriften der Wohnraumüberwachung, zum Teil auch durch eigenständige Vorgaben eine unabhängige Kontrolle der Maßnahmen der verdeckten Online-Datenerhebung, weitreichende Prüf- und Kennzeichnungspflichten mit Verwendungsverboten und Lösungsgeboten bei den erhobenen Daten sowie den Schutz des Kernbereichs privater Lebensgestaltung im Rahmen der Auswertungsphase.

Eine Online-Datenerhebung bedarf insbesondere einer grundsätzlich vorherigen richterlichen schriftlichen Anordnung, die entsprechend zu begründen ist (Abs. 5 in Verbindung mit Art. 6b Abs. 1). Art, Umfang und Dauer der Maßnahme sind in ihr anzugeben (Abs. 5 in Verbindung mit Art. 6b Abs. 1 Satz 3). Name und Anschrift des Betroffenen sowie die Bezeichnung des informationstechnischen Systems sind soweit möglich anzugeben (Satz 2). Die erstmalige Anordnung der Maßnahme ist auf maximal drei Monate zu befristen (Satz 2), eine Verlängerung um jeweils einen Monat ist möglich (Abs. 5 in Verbindung mit Art. 6b Abs. 1 Satz 4 Halbsatz 2). Für die erhobenen Daten bestehen umfassende Prüf- und Kennzeichnungspflichten; entsprechende Verwendungsbeschränkungen knüpfen hier an.

Abs. 5 Sätze 3 und 4 sehen hinsichtlich der Datensichtung ergänzende Vorschriften vor, die über die Regelung bei der Wohnraumüberwachung hinausgehen (vgl. BVerfG aaO Rn 283). Im Rahmen einer Sichtung der erhobenen Daten ist zu unterscheiden:

- Entweder werden die Daten, unter Beachtung der Maßgaben des Art. 6b Abs. 3, unverzüglich gelöscht, etwa weil sie nicht benötigt werden oder weil eine Kernbereichsverletzung offensichtlich ist oder
- die Daten werfen unter dem Gesichtspunkt Kernbereichsschutz bzw. Schutz von Berufsgeheimnisträgern keine besonderen Fragen auf, dann gelten die allgemeinen Prüf-, Kennzeichnungs- und Verwendungsregelungen wie bei Daten aus einer Wohnraumüberwachung oder
- es bestehen Anhaltspunkte für eine mögliche Zuordnung zum Kernbereich privater Lebensgestaltung bzw. für eine Zuordnung zu einem Vertrauensverhältnis zu Berufsgeheimnisträgern.

Im letztgenannten Fall ist eine gerichtliche Entscheidung über die Datenverwendung herbeizuführen. Zuständig ist der Richter, der auch für Anordnung der Online-Datenerhebung zuständig wäre, es gelten auch die gleichen Verfahrensregelungen.

Eine Ausnahme vom grundsätzlichen Verwendungsverbot und Lösungsgebot bei kernbereichsrelevanten Daten besteht nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person (Abs. 5 in Verbindung mit Art. 6b Abs. 2, 3). Die Betroffenen sind über eine getroffene Maßnahme zu unterrichten. Von einer solchen Unterrichtung kann nur mit richterlicher Zustimmung abgesehen werden (Abs. 5 in Verbindung mit Art. 6b Abs. 4).

Die Unterrichtung des Parlamentarischen Kontrollgremiums und des Landtags ist in Art. 6h Abs. 1 vorgesehen.

#### Zu Art. 6g

Art. 6g dient in großem Umfang nur der Klarstellung. Bereits nach bestehender Rechtslage ist davon auszugehen, dass notwendige Begleitmaßnahmen von den jeweiligen Befugnissen zur verdeckten Datenerhebung - unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes - grundsätzlich mit umfasst sind. Als notwendige Begleitmaßnahmen nach Satz 1 kommen insbesondere in Betracht die Durchsuchung von Sachen, das Betreten und die Durchsuchung der Wohnung des Betroffenen und die Installation der erforderlichen Abhörtechnik. Mit umfasst ist auch die heimliche Durchsuchung der Wohnung zur Auffindung eines Notebooks und das Anbringen von Hardwarekomponenten, wenn dies unerlässliche Begleitmaßnahme ist. Insbesondere für die Fälle, in denen die Begleitmaßnahme selbständig in das Grundrecht aus Art. 13 eingreift, erscheint eine ausdrückliche Regelung angezeigt. Daher wird ausdrücklich die Zulässigkeit von Begleitmaßnahmen festgeschrieben. Es gelten hier grundsätzlich die gleichen materiellen Voraussetzungen wie für die beabsichtigte Hauptmaßnahme. Bei

Maßnahmen nach dem G 10 ist bei Begleitmaßnahmen, die in Art. 13 eingreifen, zusätzlich das Vorliegen einer dringenden Gefahr verlangt, um dem Schutzgehalt von Art. 13 GG Rechnung zu tragen. G 10-Maßnahmen, bei denen solche Begleitmaßnahmen in Betracht kommen, sind Maßnahmen der Quellen-Telekommunikationsüberwachung, bei der auf Telekommunikationsendgeräte unmittelbar zugegriffen wird. Zur verfahrensmäßigen Absicherung der Rechte des Betroffenen besteht ein Richtervorbehalt und in der richterlichen Anordnung sind Art, Umfang und Dauer der Maßnahme genau zu bestimmen. Auch für die Unterrichtung gelten entweder dieselben Regeln wie bei der Hauptmaßnahme oder, bei Maßnahmen nach dem G 10, die Regeln der verdeckten Online-Datenerhebung.

#### Zu Art. 6h

Abs. 1 regelt die Unterrichtung des Parlamentarischen Kontrollgremiums des Bayerischen Landtags über getroffene Maßnahmen nach Art. 6c Abs. 2 (Auskunftsersuchen) und Art. 6c Abs. 4 (IM-SI-Catcher). Es ist hier eine halbjährliche Berichtspflicht vorgesehen, wie es schon bisher bei den Auskunftsersuchen geltende Rechtslage war. Über alle Maßnahmen des Abhörens und Aufzeichnens des nichtöffentlich gesprochenen Wortes mit dem verdeckten Einsatz technischer Mittel, bei denen Daten länger als sechs Monate gespeichert werden und Maßnahmen nach Art. 6e (Online-Datenerhebungen) ist ein jährlicher Bericht vorgesehen. Bei Maßnahmen nach Art. 6d wird damit eine parlamentarische Kontrolle gewährleistet, wenn sie mit einem länger fortdauernden Grundrechtseingriff verbunden sind. Soweit nach Art. 6d erhobene Daten früher gelöscht werden, beispielsweise weil sich nach Übersetzung und Auswertung einer Aufzeichnung herausstellt, dass sie für die Aufgabenerfüllung des Landesamts ohne Bedeutung sind, was im Zeitpunkt der Aufzeichnung nicht erkennbar war, bedarf es keiner Unterrichtung des Gremiums.

Abs. 2 normiert in Erfüllung der Vorgaben des § 8a Abs. 8 Satz 1 BVerfSchG eine Berichtspflicht an das Parlamentarische Kontrollgremium des Bundes. Abweichend von den bisherigen Vorgaben des § 8 Abs. 11 BVerfSchG a. F. besteht diese Berichtspflicht, die neben die in Abs. 1 geregelten Berichtspflichten gegenüber dem Parlamentarischen Kontrollgremium im Landtag tritt, nur noch bei Auskünften nach Art. 6c Abs. 2 Satz 1 Nr. 3 bis 5.

#### Zu § 1 Nr. 4 (Art. 9 Abs. 1 BayVSG)

Der neu eingefügte Satz 3 stellt klar, dass in Fällen, die die Erhebung, Verarbeitung und Nutzung von Daten betreffen, die gemäß Art. 2 Abs. 2 AGG 10 der Kontrollkompetenz der G 10-Kommission und nicht der des Landesbeauftragten für den Datenschutz (vgl. Art. 30 Abs. 3 BayDSG) unterfallen, die Errichtungsanordnung und wesentliche Verfahrensänderungen auch der G 10-Kommission zur Ermöglichung der Vorabkontrolle mitzuteilen sind.

#### Zu § 1 Nr. 5 (Art. 11 Abs. 1 BayVSG)

In Art. 11 Abs. 1 wird eine neue Regelung zur Auskunft über die beim Landesamt für Verfassungsschutz gespeicherten Daten getroffen, die sich an den entsprechenden Auskunftsregelungen der Verfassungsschutzgesetze der anderen Länder, des Verfassungsschutzgesetzes des Bundes sowie an den Auskunftsregelungen in Art. 48 PAG und Art. 10 BayDSG orientiert.

#### Zu Art. 11 Abs. 1 Satz 1 BayVSG

In Satz 1 erhält der Bürger nunmehr im Grundsatz einen Anspruch auf Auskunft über die zu seiner Person beim Landesamt für Verfassungsschutz sowohl in Dateien als auch in Akten gespeicherten

personenbezogenen Daten, der lediglich unter den Voraussetzungen des neuen Satzes 2 (Verletzung der Mitwirkungspflicht) oder bei Vorliegen der Versagungsgründe des weiter geltenden Abs. 3 entfällt. Nach dem bisherigen Satz 1 bestand kein (genereller) Anspruch auf Auskunft über die beim Landesamt für Verfassungsschutz in Dateien oder Akten gespeicherten Informationen. Auch bei einem besonderen Interesse des Betroffenen an einer Auskunft über die zu seiner Person gespeicherten Daten und bei Nichtvorliegen eines Versagungsgrundes nach Abs. 3 sah der bisherige Satz 2 lediglich eine Entscheidung des Landesamts für Verfassungsschutz nach pflichtgemäßem Ermessen vor. Die bisherige Regelung griff das Urteil des Bundesverwaltungsgerichts vom 20.02.1990 (Az.: 1 C 42/83) auf, in dem entschieden wurde, dass es keinen generellen Rechtsanspruch auf Auskunft gegenüber Verfassungsschutzbehörden geben könne und nur dann eine Ermessensentscheidung zu treffen sei, wenn der Betroffene ein besonderes Interesse an der Auskunft habe.

Der Bayerische Verfassungsgerichtshof hat in seiner Entscheidung vom 11.11.1997 (Az.: Vf. 22-VII-94) zur Verfassungsmäßigkeit einzelner Bestimmungen des Bayerischen Verfassungsschutzgesetzes und des Bayerischen Datenschutzgesetzes die Verfassungskonformität u.a. des bisherigen Art. 11 Abs. 1 ausdrücklich bestätigt. Der Landesbeauftragte für den Datenschutz hat zur Stärkung der Rechte der Bürger gleichwohl eine Änderung von Art. 11 Abs. 1 gefordert.

Der neue Satz 1 mit einem grundsätzlichen Auskunftsanspruch übernimmt die Regelung der Verfassungsschutzgesetze anderer Länder sowie des § 15 BVerfSchG und verbessert damit die Rechte des Bürgers.

Satz 1 bestimmt nunmehr auch, dass die Auskunftserteilung selbst kostenfrei erfolgt. Da die Erteilung der Auskunft an sich eine kostenpflichtige Amtshandlung nach Art. 1 Abs. 1 KG darstellt, wird damit eine dem Kostengesetz vorgehende Sonderregelung (vgl. Art. 27 Abs. 1 KG) zugunsten des Bürger getroffen. Die Kostenfreiheit der Auskunftserteilung entspricht der bisherigen Praxis des Bayerischen Landesamts für Verfassungsschutz und den Regelungen anderer Verfassungsschutzgesetze. Die Ablehnung oder Rücknahme eines Auskunftsanspruchs bleibt im Hinblick auf etwaige missbräuchliche Antragsteller zwar grundsätzlich kostenpflichtig, die Möglichkeit des Verzichts auf eine Kostenfestsetzung aus Billigkeitsgründen und unter Wirtschaftlichkeitsgesichtspunkten (Art. 8 Abs. 3, 16 Abs. 2 und 3 KG) bleibt jedoch bestehen.

Zu Art. 11 Abs. 1 Sätze 2 und 3 BayVSG

Um dem Landesamt für Verfassungsschutz eine Prüfung des Auskunftsbegehrens zu ermöglichen und so einer Ausforschung vorbeugen zu können, verlangt Satz 2 der Neufassung entsprechend bisheriger Rechtslage, dass ein besonderes Interesse an der Auskunft dargelegt wird. Kommt er dieser Mitwirkungspflicht nicht nach, so hat dies die Verweigerung der Auskunft zur Folge.

Der neue Satz 3 stellt klar, dass „die zu seiner Person [...] gespeicherten Daten“ im Gegensatz zu Art. 10 Abs. 1 Satz 1 Nr. 1 BayDSG nicht die Angaben über Herkunft und Empfänger der Daten umfassen. Die allgemeine datenschutzrechtliche Auskunftsnorm und damit auch Art. 10 Abs. 1 Satz 1 Nr. 3 BayDSG findet bei der Erfüllung der gesetzlich festgelegten Aufgaben durch das Landesamt für Verfassungsschutz gemäß Art. 10 BayVSG keine Anwendung. Diese inhaltliche Begrenzung der Auskunftspflicht trägt den spezifischen Geheimhaltungsinteressen des Landesamts für Verfassungsschutz Rechnung.

Zu Art. 11 Abs. 1 Satz 4 BayVSG

Satz 4 der Neufassung stellt wie bisher das Verfahren der Auskunftserteilung, insbesondere deren Form, entsprechend den Regelungen in Art. 48 Abs. 1 Satz 3 PAG und Art. 10 Abs. 3 Satz 3 BayDSG in das pflichtgemäße Ermessen des Landesamts für Verfassungsschutz. Das Verfahren betrifft das „Wie“ der Auskunftserteilung und nicht das „Ob“, für das der neue Satz 1 nunmehr eine gebundene Entscheidung vorsieht. Zur Frage des „Wie“ gehört etwa auch die Entscheidung darüber, dass bei Anträgen von Personen, zu denen mehrere hundert Einzelinformationen vorliegen, die Auskunft dadurch erteilt wird, dass anstelle einer vollumfänglichen Auflistung der Einzelinformationen eine „zusammengefasste“ Auskunft erteilt wird.

Der Bayerische Verfassungsgerichtshof hat in seiner Entscheidung vom 11.11.1997 die Verfassungskonformität des Art. 10 Abs. 3 Satz 3 BayDSG ausdrücklich bestätigt.

**Zu § 1 Nr. 6 Buchst. a (Art. 14 Abs. 1 Satz 4 BayVSG)**

Es wird lediglich der Sprachgebrauch des Gesetzes redaktionell berichtigt und das Wort „Übermittlung“ durch das Wort „Weitergabe“ ersetzt.

Zu § 1 Nr. 6 Buchst. b (Art. 14 Abs. 6 BayVSG)

Nach dem Wortlaut der bisherigen Regelung in Art. 14 wäre allein das Landesamt für Verfassungsschutz befugt, Datenübermittlungen an die entsprechenden Stellen durchzuführen. Es entsprach jedoch bisher einer gefestigten Verwaltungspraxis, dass insbesondere in Verfahren der Prüfung der Verfassungstreue im öffentlichen Dienst sowie in Ausländer- und Einbürgerungsverfahren belastende Erkenntnisse durch das Staatsministerium des Innern anstelle des Landesamts an die zuständigen Stellen übermittelt wurden. Die Einbeziehung des Innenministeriums in den Übermittlungsvorgang als „Datenmittler“ in Fällen, in denen sensible personenbezogene Daten mit womöglich folgenschweren Auswirkungen für den Betroffenen weitergegeben werden, diene der erneuten objektiven Überprüfung der Rechtmäßigkeit und Notwendigkeit der Datenübermittlung durch die Aufsichtsbehörde des Landesamts für Verfassungsschutz. Sie diene damit gerade dem Schutz des Betroffenen. Die Zulässigkeit dieser Vorgehensweise wurde vom Bayerischen Verfassungsgerichtshof in einer Entscheidung vom 09.04.2003 (Az.: 24 B 02.646) grundsätzlich bestätigt. Das Bundesverwaltungsgericht hat im Urteil vom 09.03.2005 (Az.: 6 C 3.04) jedoch die Weitergabe von Erkenntnissen des Verfassungsschutzes durch das Bayerische Staatsministerium des Innern anstelle des Landesamts für Verfassungsschutz als Eingriff in das Recht auf informationelle Selbstbestimmung ohne gesetzliche Ermächtigung erachtet und für rechtswidrig erklärt. Für die Zukunft wird daher die Datenübermittlung durch das über das Bayerische Landesamt für Verfassungsschutz aufsichtsführende Staatsministerium des Innern gesetzlich verankert.

**Zu § 1 Nr. 7 (Art. 15 Satz 1 BayVSG)**

Entsprechend der Praxis der meisten anderen Verfassungsschutzbehörden berichtet auch das Landesamt für Verfassungsschutz – in teleologischer Auslegung des Wortlauts des Art. 15 Satz 1 – bereits dann über verfassungsfeindliche Bestrebungen und Aktivitäten im Verfassungsschutzbericht, wenn ihm tatsächliche Anhaltspunkte für solche Bestrebungen bzw. Aktivitäten vorliegen. Dieser Praxis liegt die Auffassung zugrunde, dass die Voraussetzungen

für die Veröffentlichung im Verfassungsschutzbericht mit den Voraussetzungen für die Aufnahme und Aufrechterhaltung von Beobachtungen identisch sind. Die Verfassungsschutzbehörden könnten aber die ihnen von der Verfassung zugewiesene Aufgabe nicht effektiv wahrnehmen, wenn sie untätig bleiben müssten, bis sich die Verfassungsfeindlichkeit ihrer Beobachtungsobjekte beweisen ließe. Daher darf das Landesamt für Verfassungsschutz Bestrebungen bereits dann beobachten, wenn es tatsächliche Anhaltspunkte für eine verfassungsfeindliche Zielsetzung gibt. Die Praxis der Berichterstattung des Landesamts für Verfassungsschutz wurde von bayerischen Gerichten bislang nicht in Frage gestellt. Im Urteil vom 6. April 2006 (Az.: 3 B 3.99) hat das Obergerverwaltungsgericht Berlin-Brandenburg aber die Vorschrift des § 26 Satz 1 LVerfSchG Berlin, der wie die bisherige bayerische Regelung nur von Bestrebungen spricht und eine dieser vergleichbare Verweisungsstruktur aufweist, eng ausgelegt und entschieden, dass eine Berichterstattung im Rahmen des Verfassungsschutzberichts ausschließlich bei sicherem Vorliegen von Bestrebungen zulässig ist. In Satz 1 soll daher klargestellt werden, dass eine Berichterstattung bereits bei Vorliegen tatsächlicher Anhaltspunkte zulässig ist. Unabhängig hiervon besteht bei der Berichterstattung der Öffentlichkeit gegenüber bereits verfassungsrechtlich die Verpflichtung, von verfassungsfeindlichen Bestrebungen und Aktivitäten bei verschiedenen Beobachtungsobjekten unterschiedlich dichte und belastbare Erkenntnislagen in der Darstellung hinreichend deutlich zu machen (vgl. BVerfG vom 24.05.2005, Az.: 1 BvR 1072/01, Rd.-Nr. 89).

#### **Zu § 2**

##### **Änderung des Ausführungsgesetzes Art. 10-Gesetz**

Die Neufassung der Auskunftsbefugnisse des Landesamts für Verfassungsschutz in § 1 Nr. 3 (Art. 6c BayVSG), die entsprechend den geänderten bundesrechtlichen Vorgaben in § 8a Abs. 8 BVerfSchG nunmehr lediglich die Auskünfte gegenüber Post-, Telekommunikations- und Teledienstleistern der Kontrolle der G 10-Kommission unterstellt sowie die Normierung weiterer Befugnisse in Art. 6d bis 6g, macht eine Änderung der entsprechenden Verweisungsvorschrift erforderlich.

#### **Zu § 3**

##### **Änderung des Parlamentarischen Kontrollgremium-Gesetzes**

Die Neufassung der Art. 6a bis 6h BayVSG bedingt eine Änderung der entsprechenden Verweisungsvorschriften im PKGG (Art. 1 Abs. 1 Satz 1, Art. 3 Abs. 2 Satz 1 und Abs. 4). Des Weiteren wird in § 1 Nr. 1b durch Schaffung des neuen Art. 6 Abs. 1 die Kontrolltätigkeit des Parlamentarischen Kontrollgremiums auf die Dienstvorschrift über zulässige nachrichtendienstliche Mittel erweitert. Komplementär zur dort normierten Verpflichtung, das Parlamentarische Kontrollgremium zu unterrichten, muss in Art. 3 Abs. 4 Satz 1 PKGG das Recht des Gremiums auf diese Unterrichtung ergänzend eingefügt werden.

#### **Zu § 4**

##### **Zitiergebot**

Nachdem durch Art. 6b Abs. 2 BayVSG teilweise die Voraussetzungen für Datenerhebungen bei Post-, Telekommunikations- und Teledienstleistern abgesenkt wurden und in Art. 6a, b BayVSG die Wohnraumüberwachung neu geregelt wurde, schränkt das vorliegende Gesetz die genannten Grundrechte ein.

#### **Zu § 5**

##### **Inkrafttreten**

Insbesondere die Schaffung einer Befugnis zur Datenerhebung aus informationstechnischen Systemen mit technischen Mitteln, die Anpassung des bisherigen Art. 6b an die durch das Terrorismusbekämpfungsergänzungsgesetz auf Bundesebene geschaffenen Verfahrensvereinfachungen sowie materiellen Erleichterungen bei den für die Terrorismusbekämpfung wichtigen Auskunftsbefugnissen gegenüber Kreditinstituten, Fluggesellschaften, Post-, Telekommunikations- und Teledienstleistern sind dringlich. Das Gesetz ist deshalb dringlich.