Drucksache **19/**

19. Wahlperiode

HESSISCHER LANDTAG

Gesetzentwurf
der Fraktionen CDU und BÜNDNIS 90/ DIE GRÜNEN

für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen

A. Problem

1. Das Landesamt für Verfassungsschutz (Landesamt) leistet einen unverzichtbaren Beitrag zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung sowie den Bestand und die Sicherheit des Landes Hessen, des Bundes und der anderen Länder.
   Angesichts des hohen Bedrohungs- und Gefährdungspotenzials durch terroristische Straftaten und ihre Folgewirkungen kommt der engen und effektiven Zusammenarbeit der Nachrichtendienste, Polizei- und sonstigen Sicherheitsbehörden im Verhältnis von Bund und Ländern existenzielle Bedeutung zu.

2. Als Dienstleister für Politik, Zivilgesellschaft und andere öffentliche Stellen schützt das Landesamt die Verfassung und die Sicherheit des Einzelnen. Kraft seiner Funktion als Frühwarnsystem der Demokratie dient es auch dem Erhalt des gesellschaftlichen Friedens und hilft diejenigen Voraussetzungen zu wahren, unter denen die vor Krieg und Verfolgung auch nach Hessen geflüchteten Menschen erfolgreich integriert werden können.

3. Die Notwendigkeit einer funktionsfähigen Sicherheitsarchitektur haben die verheerenden Terroranschläge im Nachbarland Frankreich (Paris und Nizza), aber auch die Ereignisse von Hannover, Essen, Würzburg, Ansbach, Berlin und Hamburg sowie die entsetzlichen Terroranschläge in London und Manchester deutlich vor Augen geführt. Dass die Zusammenarbeit von Nachrichtendiensten, Polizei- und sonstigen Sicherheitsbehörden zu verbessern ist, war bereits zuvor bei der politischen Aufarbeitung der Mordserie der rechtsextremistischen Terrorgruppe des sogenannten „Nationalsozialistischen Untergrunds“ (NSU) deutlich herausgestellt worden.

4. Das Bundesverfassungsgericht hat in seinem zum Antiterrordateigesetz (ATDG) ergangenen Urteil vom 24. April 2013 (BVerfGE 133, 277ff.) ein „informationelles Trennungsprinzip“ mit Verfassungsrang entwickelt, das der Informationsübermittlung zwischen Verfassungsschutzbehörden und Polizei enge und deutliche Grenzen zieht. Aufgrund dieser Rechtsprechung müssen die Übermittlungsvorschriften des bisherigen Hessischen Gesetzes über das Landesamt für Verfassungsschutz überarbeitet werden.

5. Ferner hat der Bundesgesetzgeber das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) erlassen, das insbesondere Voraussetzungen und Grenzen des in der Öffentlichkeit viel diskutierten Einsatzes von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern sowie Vertrauensleuten festlegt. Damit steht nun eine Richtschnur für Regelungen in den Landesverfassungsschutzgesetzen zur Verfügung.

6. Berücksichtigt wird auch das Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum Bundeskriminalamtgesetz (BKAG) – 1 BvR 966/09. Darin hat das Gericht zahlreiche Befugnisse des Bundeskriminalamts zu verdeckten Überwachungsmaßnahmen, die ihm zur Abwehr von Gefahren des internationalen Terrorismus eingeräumt wurden, zwar im Grundsatz mit den Grundrechten für vereinbar erklärt, die derzeitige Ausgestaltung der Befugnisse aber in verschiedener Hinsicht als nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar beanstandet.

7. Das Hessische Gesetz über das Landesamt für Verfassungsschutz, das in seiner Grundkonzeption aus dem Jahre 1990 stammt, wurde in der Vergangenheit, vor allem bedingt durch die fortschreitende Rechtsprechung des Bundesverfassungsgerichts, bereits mehrfach geändert. Es hat dadurch an Lesbarkeit und Transparenz eingebüßt. Die nun anstehenden weiteren Änderungen geben Gelegenheit zu einer grundlegenden Revision und Neustrukturierung.

8. Neben der organisatorischen Trennung des Landesamts von Polizei und anderen Exekutivbehörden bedarf dessen im Wesentlichen im Verborgenen bleibende Tätigkeit wegen der damit verbundenen geringeren Kontrollmöglichkeiten durch die Öffentlichkeit und die Judikative einer besonderen Kontrolle durch das Parlament.

B. Lösung

1. Die Arbeit des Landesamts erhält durch ein Hessisches Verfassungsschutzgesetz eine neue gesetzliche Grundlage, welche dessen Befugnisse und deren Grenzen klar definiert. Dabei werden die auf Bund- und Länderebene, insbesondere durch die Expertenkommission der Hessischen Landesregierung erarbeiteten Handlungsempfehlungen, sowie die Vorgaben des Bundesverfassungsgerichts aus dem ATDG-Urteil und dem BKAG-Urteil umgesetzt. Über den bisherigen Befugnisrahmen hinaus wird das Landesamt zur sog. Quellen-Telekommunikationsüberwachung (§ 6 Abs. 2 bis 4) und zum verdeckten Zugriff auf informationstechnische Systeme ermächtigt (§ 8).

2. Die Reform des Hessischen Gesetzes über das Landesamt für Verfassungsschutz beschränkt sich nicht auf punktuelle Anpassungen. Durch inhaltliche Umstrukturierung, redaktionelle Überarbeitung und Straffung des Gesetzes soll der Verfassungsschutz in Hessen auf eine trag- und zukunftsfähige gesetzliche Grundlage gestellt werden. Die Neufassung setzt dazu auf bundeseinheitlich geltende rechtsstaatliche Standards, wie sie insbesondere im Artikel 10-Gesetz und dem überarbeiteten Bundesverfassungsschutzgesetz niedergelegt sind.

3. Die vom Bundesgesetzgeber normierten Grenzen für den Einsatz von Verdeckten Mitarbeiterinnen, Verdeckten Mitarbeitern und Vertrauensleuten werden weitestgehend wortgleich in das hessische Landesrecht übernommen (§§ 13 und 14).

4. Die Vorschriften zum Austausch von Informationen zwischen dem Landesamt und anderen Behörden, insbesondere Polizei und Staatanwaltschaft, werden in enger Anlehnung an die Neuregelung des Bundes reformiert (§§ 19ff.).

5. Um die Bedeutung der parlamentarischen Kontrolle und den Grundsatz der Gewaltenteilung zu unterstreichen, wird die bisher als Teil des Gesetzes über das Landesamt für Verfassungsschutz geregelte parlamentarische Kontrolle in ein eigenständiges Gesetz zur parlamentarischen Kontrolle des Verfassungsschutzes in Hessen überführt. Die Regelungen dieses Gesetzes orientieren sich an denen des entsprechenden Gesetzes zur parlamentarischen Kontrolle durch den Bundestag.

C. Befristung

Eine Befristung ist nicht vorgesehen. Das Gesetz dient dem Schutz der Verfassung.

D. Alternativen

Im Rahmen der Zielsetzung: Keine.
Gesetzliche Änderungen sind aufgrund der Rechtsprechung des Bundesverfassungsgerichts erforderlich. Auch die mit hohem Aufwand durchgeführten Untersuchungen des Hessischen Landtags und der Hessischen Landesregierung fordern gesetzgeberische Maßnahmen, um die im Zuge der Aufklärung des NSU-Komplexes erkannten Handlungsbedarfe in der Sicherheitsarchitektur umzusetzen und die gesellschaftliche Akzeptanz der Arbeit des Verfassungsschutzes zu verbessern. Mit der Gesetzesnovelle leistet Hessen den notwendigen Beitrag im Rahmen des sich bundesweit vollziehenden Reformprozesses.

E. Finanzielle Auswirkungen

1. Auswirkungen auf die Liquiditäts- oder Ergebnisrechnung

   Die Kosten, die den zur Auskunft verpflichteten Anbietern von Telekommunikations- und Telemediendiensten, Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge sowie Instituten und Unternehmen des Finanzsektors entstehen (§ 11), werden durch eine Verpflichtung des Landesamts zur finanziellen Entschädigung aufgefangen. Der hieraus entstehende jährliche Kostenaufwand kann im bestehenden Mittelrahmen bewältigt werden.
   Aufgrund des erneuerten Befugnisrahmens sowie erweiterten Mitwirkungs- und Beteiligungsaufgaben wird dem Landesamt weiterhin ein signifikanter personaler Mehraufwand entstehen.

2. Auswirkungen auf die Vermögensrechnung

   Keine.

3. Berücksichtigung der mehrjährigen Finanzplanung

Keine.

4. Auswirkungen für hessische Gemeinden und Gemeindeverbände

Keine.

F. Unmittelbare oder mittelbare Auswirkungen auf die Chancengleichheit von Frauen und Männern

Keine.

G. Besondere Auswirkungen auf behinderte Menschen

Keine. Das Gesetz wurde am Maßstab der UN-Behindertenrechtskonvention überprüft. Es besteht kein Änderungsbedarf.

Der Landtag wolle das folgende Gesetz beschließen:

Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen

Vom

Artikel 1
Hessisches Verfassungsschutzgesetz
(HVSG)

INHALTSÜBERSICHT

PRÄAMBEL

Der Verfassungsschutz dient dem Schutz der freiheitlichen demokratischen Grundordnung. Er ist Dienstleister der Demokratie und hält insbesondere die analytischen Kompetenzen zur Beurteilung jener Gefahren vor, die Demokratie und Menschenrechten durch extremistisches Gedankengut drohen. Er tauscht sich mit Wissenschaft und Gesellschaft aus. Hierzu gehört auch der öffentliche Diskurs. Er berücksichtigt gesellschaftliche Vielfalt und gesellschaftliche Entwicklungen.

ERSTER TEIL

Organisation und Aufgaben des Landesamts

§ 1

Organisation des Landesamts

(1) Das Landesamt für Verfassungsschutz (Landesamt) untersteht als obere Landesbehörde dem für den Verfassungsschutz zuständigen Ministerium. Es darf mit Polizeidienststellen organisatorisch nicht verbunden werden.

(2) Verfassungsschutzbehörden anderer Länder dürfen in Hessen nur im Einvernehmen, das Bundesamt für Verfassungsschutz nur im Benehmen mit dem Landesamt tätig werden. Das Landesamt darf in anderen Ländern nur tätig werden, soweit die Rechtsvorschriften der anderen Länder dies zulassen.

§ 2

Aufgaben des Landesamts

(1) Das Landesamt ist zuständig für die Zusammenarbeit Hessens mit dem Bund und den anderen Ländern in Angelegenheiten des Verfassungsschutzes. Aufgabe des Landesamts ist es, es den zuständigen Stellen zu ermöglichen, rechtzeitig

die erforderlichen Maßnahmen zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu treffen. Das Landesamt hat auch die Aufgabe, den in Abs. 2 genannten Bestrebungen und Tätigkeiten durch Information, Aufklärung und Beratung entgegenzuwirken und vorzubeugen (Prävention). Zur Aufklärung der Öffentlichkeit erstellt das Landesamt mindestens einmal jährlich einen Bericht über Bestrebungen und Tätigkeiten nach Abs. 2 oder tatsächliche Anhaltspunkte hierfür. Der Bericht wird von dem für den Verfassungsschutz zuständigen Ministerium herausgegeben und auf der Internetseite des Landesamts für fünf Jahre bereitgestellt.

(2) Aufgabe des Landesamts ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben,

2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht,

3. Bestrebungen im Geltungsbereich des Grundgesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,

4. Bestrebungen im Geltungsbereich des Grundgesetzes, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 des Grundgesetzes), gerichtet sind,

5. Bestrebungen und Tätigkeiten der Organisierten Kriminalität im Geltungsbereich des Grundgesetzes.

(3) Das Landesamt wirkt mit bei Sicherheitsüberprüfungen und Überprüfungen nach § 3 Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Gesetz vom 16. Juni 2017 (BGBl. I S. 1634).

(4) Das Landesamt ist zuständig für Sicherheitsüberprüfungen nach § 2 Abs. 2 Satz 1 Nr. 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) vom 26. Juni 2001 (BGBl. I S. 1254, 2998), zuletzt geändert durch Gesetz vom 16. Juni 2017 (BGBl. I S. 1634).

§ 3

Begriffsbestimmungen

(1) Die Begriffsbestimmungen des § 4 Abs. 1 Satz 1, 2 und 4 sowie Abs. 2 des Bundesverfassungsschutzgesetzes finden Anwendung.

(2) Organisierte Kriminalität im Sinne dieses Gesetzes ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung für die Rechtsordnung sind, durch mehr als zwei Beteiligte, die auf längere oder unbestimmte Dauer arbeitsteilig tätig werden

1. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

2. unter Anwendung von Gewalt oder durch entsprechende Drohung oder

3. unter Einflussnahme auf Politik, Verwaltung, Justiz, Medien oder Wirtschaft.

ZWEITER TEIL

Befugnisse des Landesamts

§ 4

Informationserhebung

(1) Das Landesamt darf die zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 und 2 erforderlichen Informationen erheben und verarbeiten. Einzelheiten zum Umgang mit den erhobenen Informationen regelt eine von dem für den Verfassungsschutz zuständigen Ministerium zu erlassende Dienstvorschrift.

(2) Das Landesamt darf personenbezogene Daten aus allgemein zugänglichen Quellen erheben und verarbeiten, um zu prüfen, ob tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen.

(3) Liegen bei der betroffenen Person tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vor oder wird das Landesamt nach § 2 Abs. 3 tätig, darf es Auskünfte bei öffentlichen Stellen oder Dritten einholen, wenn die Daten

1. nicht aus allgemein zugänglichen Quellen,

2. nur mit übermäßigem Aufwand oder

3. nur durch eine die betroffene Person stärker belastende Maßnahme

erhoben werden können. Würde durch die Erhebung von Auskünften nach Satz 1 der Zweck der Maßnahme gefährdet oder die betroffene Person unverhältnismäßig beeinträchtigt, darf das Landesamt Akten und Register öffentlicher Stellen einsehen. Im Übrigen gilt § 19.

(4) Das Landesamt muss Ersuchen auf Auskunft oder Einsicht nicht begründen, soweit dies dem Schutz der betroffenen Person dient oder eine Begründung den Zweck der Maßnahme gefährden würde. Es hat die Ersuchen aktenkundig zu machen. Über die Einsichtnahme nach Abs. 3 Satz 2 hat das Landesamt einen Nachweis zu führen, aus dem der Zweck, die ersuchte Behörde und die Aktenfundstelle hervorgehen. Der Nachweis ist gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten.

(5) Zur Beantwortung von Übermittlungsersuchen nach § 21 Abs. 1 Nr. 2 darf das Landesamt personenbezogene Daten nur erheben, soweit dies zur Überprüfung der dem Landesamt bereits vorliegenden Informationen erforderlich ist. Abs. 3 bleibt unberührt.

(6) Werden Daten bei der betroffenen Person oder bei Dritten außerhalb des öffentlichen Bereichs offen erhoben, so ist der Erhebungszweck anzugeben. Die Befragten sind auf die Freiwilligkeit ihrer Angaben und bei einer Sicherheitsüberprüfung nach § 2 Abs. 3 auf eine dienst-, arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht hinzuweisen.

(7) Ein Ersuchen des Landesamts um Übermittlung personenbezogener Daten darf nur diejenigen personenbezogenen Daten enthalten, die für die Erteilung der Auskunft unerlässlich sind. Schutzwürdige Interessen der betroffenen Person dürfen nur in unvermeidbarem Umfang beeinträchtigt werden.

(8) Zur Aufgabenerfüllung nach § 2 dürfen personenbezogene Daten von Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst Bestrebungen oder Tätigkeiten im Sinne des § 2 Abs. 2 nachgehen (Unbeteiligte), nur erhoben, verarbeitet oder genutzt werden, wenn

1. dies für die Erforschung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorübergehend erforderlich ist,

2. die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und

3. überwiegende schutzwürdige Belange der betroffenen Personen nicht entgegenstehen.

Personenbezogene Daten Unbeteiligter dürfen auch erhoben werden, wenn sie mit zur Aufgabenerfüllung erforderlichen Informationen untrennbar verbunden sind.

(9) Daten, die für das Verständnis der zu speichernden Informationen nicht erforderlich sind, sind unverzüglich zu löschen. Dies gilt nicht, wenn die Löschung nicht oder nur mit unvertretbarem Aufwand möglich ist; in diesem Fall dürfen die Daten nicht verwertet werden.

§ 5

Informationserhebung mit nachrichtendienstlichen Mitteln

(1) Das Landesamt darf Informationen mit nachrichtendienstlichen Mitteln erheben. Für personenbezogene Daten gilt dies nur, wenn

1. bei der betroffenen Person tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen und anzunehmen ist, dass auf diese Weise zusätzliche Erkenntnisse erlangt werden können,

2. tatsächliche Anhaltspunkte dafür vorliegen, dass auf diese Weise die zur Erforschung von Bestrebungen und Tätigkeiten nach § 2 Abs. 2 erforderlichen Quellen gewonnen werden können,

3. dies zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Informationsquellen des Landesamts gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist, oder

4. dies zur Überprüfung der Nachrichtenehrlichkeit und der Eignung von Vertrauensleuten erforderlich ist.

(2) Nachrichtendienstliche Mittel sind Mittel und Methoden, die mittelbar oder unmittelbar dem von der betroffenen oder außenstehenden Person nicht erkennbaren Erheben von Daten dienen. Als nachrichtendienstliche Mittel darf das Landesamt einsetzen:

1. Überwachung des Brief-, Post- und Fernmeldeverkehrs im Sinne des Art. 10 des Grundgesetzes einschließlich notwendiger Begleitmaßnahmen nach § 6,

2. technische Mittel zur Wohnraumüberwachung nach § 7,

3. technische Mittel zum Zugriff auf informationstechnische Systeme nach § 8,

4. technische Mittel zur Ortung von Mobilfunkendgeräten nach § 10,

5. besondere Auskunftsersuchen nach § 11 zu

a) den Umständen des Postverkehrs bei Unternehmen, die geschäftsmäßig Postdienstleistungen erbringen oder daran mitwirken,

b) Telekommunikationsverbindungs- und Teledienstenutzungsdaten bei Unternehmen, die geschäftsmäßig Telekommunikationsdienste und Teledienste erbringen oder daran mitwirken,

c) Daten bei Verkehrsunternehmen, Betreibern von Computerreservierungssystemen und globalen Distributionssystemen sowie bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen,

6. Ton- und Bildaufzeichnungen außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes mit und ohne Inanspruchnahme technischer Mittel nach § 12,

7. Verdeckte Mitarbeiterinnen, Verdeckte Mitarbeiter und Vertrauensleute nach den §§ 13 und 14,

8. verdeckte Ermittlungen und Befragungen,

9. Observation,

10. Tarnmittel,

11. Funkbeobachtungen,

12. Beobachtung des Internets; dies beinhaltet auch die verdeckte Teilnahme an der im Internet geführten Kommunikation, insbesondere in Foren und elektronischen Kommunikationsplattformen.

(3) In den Fällen des Abs. 1 Satz 2 Nr. 1 und 3 dürfen nachrichtendienstliche Mittel nicht gezielt gegen Unbeteiligte eingesetzt werden; im Übrigen gilt § 4 Abs. 8 Satz 2 und Abs. 9. Einzelheiten regelt das für den Verfassungsschutz zuständige Ministerium durch Dienstvorschrift, insbesondere die organisatorische Zuständigkeit für die Anordnung von Informationserhebungen mit nachrichtendienstlichen Mitteln. Die Dienstvorschrift ist der Parlamentarischen Kontrollkommission nach § 1 des Verfassungsschutzkontrollgesetzes vom [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes, Fundstelle von Art. 2 dieses Gesetzes*] zu übersenden.

(4) Gemeinden, Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie die Gerichte und Staatsanwaltschaften und das Landesamt leisten sich gegenseitig Amts- und Rechtshilfe. Dies gilt insbesondere für die technische Hilfe bei Tarnmaßnahmen. Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Landesamt nicht zu. Das Landesamt darf auch nicht im Wege der Amtshilfe Polizeibehörden um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.

(5) Zur Erfüllung von Aufgaben aufgrund eines Gesetzes nach Art. 73 Nr. 10 b und c des Grundgesetzes stehen dem Landesamt die Befugnisse zu, die es zur Erfüllung der entsprechenden Aufgaben nach diesem Gesetz hat.

§ 6

Überwachung des Brief-, Post- und Fernmeldeverkehrs und der Telekommunikation

(1) Die Überwachung des Brief-, Post- und Fernmeldeverkehrs im Sinne des Art. 10 des Grundgesetzes richtet sich nach dem Artikel 10-Gesetz mit den in Abs. 3 Satz 2 und 3 bestimmten Maßgaben und dem Hessischen Ausführungsgesetz zum Artikel 10-Gesetz vom 16. Dezember 1969 (GVBl. I S. 303), zuletzt geändert durch Gesetz vom 27. September 2012 (GVBl. I S. 290), in der jeweils geltenden Fassung.

(2) Um eine Maßnahme nach § 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes durchzuführen, darf das Landesamt unter den Voraussetzungen des § 3 des Artikel 10-Gesetzes ohne Wissen der betroffenen Person mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(3) Für die Durchführung einer Maßnahme nach Abs. 2 gelten § 8 Abs. 2 dieses Gesetzes, die §§ 2, 3a bis 4, 9 bis 13, 17 bis 20 des Artikel 10-Gesetzes sowie die §§ 2 bis 5 des Hessischen Ausführungsgesetzes zum Artikel 10-Grundgesetz entsprechend. Dabei ist § 3a Satz 12 des Artikel 10-Gesetzes mit der Maßgabe anzuwenden, dass die Dokumentation sechs Monate nach der Mitteilung oder nach der Feststellung der endgültigen Nichtmitteilung nach Satz 1 in Verbindung mit § 12 Abs. 1 Satz 1 oder 5 des Artikel 10-Gesetzes zu löschen ist. § 4 Abs. 1 Satz 5 des Artikel 10-Gesetzes ist mit der Maßgabe anzuwenden, dass die Protokolldaten sechs Monate nach der Mitteilung oder nach der Feststellung der endgültigen Nichtmitteilung nach Satz 1 in Verbindung mit § 12 Abs. 1 Satz 1 oder 5 des Artikel 10-Gesetzes zu löschen sind.

(4) Bei der Erhebung von Daten nach Abs. 2 sind zu protokollieren

1. das zur Datenerhebung eingesetzte Mittel,

2. der Zeitpunkt des Einsatzes,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen,

4. die Beteiligten der überwachten Telekommunikation sowie

5. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen.

Zudem sind die Gründe zu dokumentieren, wenn eine Mitteilung an die betroffene Person nach § 12 Abs. 1 Satz 2 des Artikel 10-Gesetzes unterbleibt. Die Übermittlung nach Abs. 3 Satz 1 in Verbindung mit § 4 Abs. 4 des Artikel 10-Gesetzes ist zu protokollieren. Die Protokolldaten nach Satz 1 bis 3 dürfen ausschließlich zur Mitteilung nach § 12 des Artikel 10-Gesetzes verwendet werden oder um der betroffenen Person oder der Kommission nach § 4 Abs. 1 Satz 2 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz die Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist. Für die Löschung der Protokolldaten nach Satz 1 bis 3 gelten Abs. 3 Satz 3 sowie § 4 Abs. 1 Satz 7 des Artikel 10-Gesetzes entsprechend.

§ 7

Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung

Das Landesamt darf bei der Erhebung personenbezogener Daten in einer Wohnung verdeckt technische Mittel einsetzen, wenn tatsächliche Anhaltspunkte vorliegen für eine dringende Gefahr für

1. den Bestand oder die Sicherheit des Bundes oder eines Landes,

2. Leib, Leben oder Freiheit einer Person oder

3. Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist.

§ 3 Abs. 2 und die §§ 3a und 3b des Artikel 10-Gesetzes finden zum Schutz des Kernbereichs privater Lebensgestaltung und zeugnisverweigerungsberechtigter Personen entsprechende Anwendung mit der Maßgabe, dass bei Zweifeln über die Verwertbarkeit eine Entscheidung des für die Anordnung zuständigen Gerichts einzuholen ist. § 6 Abs. 3 Satz 2 gilt entsprechend.

§ 8

Verdeckter Zugriff auf informationstechnische Systeme

(1) Das Landesamt darf nach Maßgabe des § 7 mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um

1. Zugangsdaten und verarbeitete Daten zu erheben oder

2. zur Vorbereitung einer Maßnahme nach Nr. 1 spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln.

(2) Durch technische Maßnahmen ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) § 6 Abs. 4 gilt entsprechend.

§ 9

Verfahren bei Maßnahmen nach den §§ 7 und 8

(1) Der Einsatz technischer Mittel nach den §§ 7 und 8 bedarf einer richterlichen Anordnung. Bei Gefahr im Verzug kann die Behördenleitung oder ihre Vertretung die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen.

(2) Die Anordnung ist auf höchstens einen Monat zu befristen. Verlängerungen um jeweils nicht mehr als einen weiteren Monat sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. § 4 Abs. 1 des Artikel 10-Gesetzes gilt entsprechend mit der Maßgabe nach § 6 Abs. 3 Satz 3 dieses Gesetzes, § 4 Abs. 2 Satz 1 und 2 sowie Abs. 3, § 10 Abs. 2 und 3, § 11 Abs. 1 und 2 sowie § 12 Abs. 1 und 3 des Artikel 10-Gesetzes gelten entsprechend; für den Verzicht auf die Kennzeichnung bei der Übermittlung sowie das Unterbleiben und die weitere Zurückstellung der Mitteilung an die betroffene Person gilt Abs. 1 entsprechend. Eine Mitteilung kann auch auf Dauer unterbleiben, wenn überwiegende Interessen einer betroffenen Person entgegenstehen oder wenn die Identität oder der Aufenthaltsort einer betroffenen Person nur mit unverhältnismäßigem Aufwand zu ermitteln ist.

(3) Daten aus Maßnahmen nach den §§ 7 und 8 dürfen nur verwendet werden zur

1. Abwehr von Gefahren im Sinne von § 7 Satz 1,

2. Verhinderung und Verhütung von Straftaten im Sinne von § 100b Abs. 2 der Strafprozessordnung oder

3. Verfolgung von Straftaten, wenn die Voraussetzungen der Strafprozessordnung für die Datenerhebung bei der Erhebung vorgelegen haben und bei der Übermittlung noch vorliegen.

(4) Dient der Einsatz technischer Mittel nach den §§ 7 und 8 ausschließlich dem Schutz der für den Verfassungsschutz bei einem Einsatz in Wohnungen tätigen Personen, erfolgt die Anordnung abweichend von Abs. 1 durch die Behördenleitung oder ihre Vertretung. Eine anderweitige Verwendung der hierbei erlangten Erkenntnisse ist nur zulässig, wenn zuvor richterlich festgestellt wurde, dass die Maßnahme rechtmäßig ist und die Voraussetzungen des § 7 Satz 1 vorliegen; Abs. 1 Satz 2 gilt entsprechend. Im Übrigen sind die Daten unverzüglich zu löschen.

(5) Zuständig für richterliche Entscheidungen nach den Abs. 1 bis 4 ist das Amtsgericht am Sitz des Landesamts; über Beschwerden entscheidet das in § 120 Abs. 4 Satz 2 des Gerichtsverfassungsgesetzes bezeichnete Gericht. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), zuletzt geändert durch Gesetz vom 1. Juni 2017 (BGBl. I S. 1396), entsprechend; die Rechtsbeschwerde ist ausgeschlossen.

§ 10

Ortung von Mobilfunkendgeräten

(1) Das Landesamt darf technische Mittel zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts oder zur Ermittlung der Geräte- oder Kartennummer einsetzen, soweit tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für die von § 2 umfassten Schutzgüter vorliegen.

(2) § 3 Abs. 2 und die §§ 9 und 10 Abs. 1 bis 3 des Artikel 10-Gesetzes gelten entsprechend.

§ 11

Besondere Auskunftsersuchen

(1) Das Landesamt darf im Einzelfall, soweit dies zur Erfüllung seiner Aufgaben nach § 2 erforderlich ist, bei denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder Telemedien anbieten oder daran mitwirken, Auskünfte über Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien gespeichert worden sind, einholen.

(2) Das Landesamt darf im Einzelfall zur Erfüllung seiner Aufgaben nach § 2, wenn tatsächliche Anhaltspunkte für Bestrebungen und Tätigkeiten nach § 2 Abs. 2 vorliegen, bei

1. Verkehrsunternehmen sowie Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge 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, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und über Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge,

einholen. Im Fall des § 2 Abs. 2 Nr. 1 gilt dies nur für Bestrebungen, die bezwecken oder aufgrund ihrer Wirkungsweise geeignet sind,

1. zu Hass- oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden 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.

(3) Das Landesamt darf, soweit dies zur Erfüllung seiner Aufgaben nach § 2 erforderlich ist, von denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, Auskünfte über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 27. Juni 2017 (BGBl. I S. 1963), in der jeweils geltenden Fassung erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes). Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes). Die Auskunft darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes). Die Auskunft darf nur verlangt werden, wenn die gesetzlichen Voraussetzungen für das Nutzen der Daten vorliegen.

(4) Das Landesamt darf im Einzelfall zur Erfüllung seiner Aufgaben nach § 2 unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes bei Personen und Unternehmen, die geschäftsmäßig

1. Postdienstleistungen erbringen oder daran mitwirken, Auskünfte zu Namen, Anschriften und Postfächern und sonstigen Umständen des Postverkehrs,

2. Telekommunikationsdienste erbringen oder daran mitwirken, Auskünfte zu Verkehrsdaten nach § 96 Abs. 1 Satz 1 Nr. 1 bis 5 des Telekommunikationsgesetzes

3. Telemedien anbieten oder daran mitwirken, Auskünfte über

a) Merkmale zur Identifikation des Nutzers von Telemedien,

b) Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und

c) die vom Nutzer in Anspruch genommenen Telemedien

einholen.

(5) Auskünfte nach Abs. 3, soweit Daten nach § 113 Abs. 1 Satz 2 und 3 des Telekommunikationsgesetzes betroffen sind, und Auskünfte nach Abs. 4 dürfen nur auf Anordnung des für den Verfassungsschutz zuständigen Ministeriums eingeholt werden. Die Anordnung ist durch die Behördenleitung schriftlich zu beantragen. Der Antrag ist zu begründen. Das Ministerium unterrichtet unverzüglich die G10-Kommission nach § 2 Abs. 1 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz über die Anordnung vor deren Vollzug und holt deren Zustimmung ein. Bei Gefahr im Verzug kann das Ministerium den Vollzug der Anordnung auch bereits vor Unterrichtung der Kommission anordnen. Die G10-Kommission prüft von Amts wegen oder aufgrund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 15 Abs. 5 des Artikel 10-Gesetzes ist entsprechend anzuwenden. Anordnungen, welche die G10-Kommission für unzulässig erklärt, hat das Ministerium unverzüglich aufzuheben.

(6) Bei Maßnahmen nach Abs. 2 bis 4 ist § 4 des Artikel 10-Gesetzes mit der Maßgabe nach § 6 Abs. 3 Satz 3 dieses Gesetzes anzuwenden, die §§ 9, 10, 11 Abs. 1 und 2, § 12 Abs. 1 und 3, § 17 Abs. 3 des Artikel 10-Gesetzes sowie § 2 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz sind entsprechend anzuwenden. Abweichend von § 10 Abs. 3 des Artikel 10-Gesetzes genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre. Soweit dem Verpflichteten keine Entschädigung nach besonderen Bestimmungen zusteht, findet § 20 des Artikel 10-Gesetzes entsprechende Anwendung. Im Übrigen hat der Verpflichtete die Auskunft unentgeltlich zu erteilen.

(7) Die zur Erteilung der Auskunft erforderlichen Daten müssen unverzüglich, vollständig und richtig übermittelt werden. Das Auskunftsersuchen und die übermittelten Daten dürfen der betroffenen Person oder Dritten vom Verpflichteten nicht mitgeteilt werden.

(8) Auf Auskünfte nach Abs. 4 Nr. 2 sind die Vorgaben des § 8b Abs. 8 Satz 4 und 5 des Bundesverfassungsschutzgesetzes anzuwenden. Für die Erteilung von Auskünften nach Abs. 1, 2 und 4 Nr. 3 gilt die Nachrichtendienste-Übermittlungsverordnung vom 11. Oktober 2012 (BGBl. I S. 2117) in der jeweils geltenden Fassung.

(9) Dem Verpflichteten ist es verboten, allein aufgrund eines Auskunftsersuchens einseitige Handlungen vorzunehmen, die für die betroffene Person nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen. Die Anordnung ist mit dem ausdrücklichen Hinweis auf dieses Verbot und darauf zu verbinden, dass das Auskunftsersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten hat oder ein darauf gerichteter Verdacht bestehen müsse.

§ 12

Ton- und Bildaufzeichnungen außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes

Das Landesamt darf das nichtöffentlich gesprochene Wort außerhalb des Schutzbereichs der Art. 10 und 13 des Grundgesetzes mit oder ohne Inanspruchnahme technischer Mittel mithören, abhören und aufzeichnen, wenn dies im Einzelfall zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 und 2 erforderlich ist. Satz 1 gilt entsprechend für einen verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen.

§ 13

Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter

(1) Das Landesamt darf eigene Mitarbeiterinnen und Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende (Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter) einsetzen.

(2) Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter dürfen weder zur Gründung von Bestrebungen nach § 2 Abs. 2 noch zur steuernden Einflussnahme auf derartige Bestrebungen eingesetzt werden. Sie dürfen in Personenzusammenschlüssen oder für diese tätig werden, auch wenn dadurch ein Straftatbestand verwirklicht wird. Im Übrigen dürfen Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter im Einsatz bei der Beteiligung an Bestrebungen solche Handlungen vornehmen, die

1. nicht in Individualrechte eingreifen,

2. von den an den Bestrebungen Beteiligten derart erwartet werden, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich sind, und

3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen.

Sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass eine Verdeckte Mitarbeiterin oder ein Verdeckter Mitarbeiter rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht hat, wird ihr oder sein Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet. Über Ausnahmen von Satz 4 entscheidet die Behördenleitung oder ihre Vertretung.

(3) Bei Einsätzen zur Erfüllung der Aufgabe nach § 2 Abs. 2 Nr. 5 gilt § 9a Abs. 3 des Bundesverfassungsschutzgesetzes entsprechend.

(4) Für Mitarbeiterinnen und Mitarbeiter, die verdeckt Informationen in sozialen Netzwerken und sonstigen Kommunikationsplattformen im Internet erheben, gelten Abs. 2 und 3 sowie § 9a Abs. 3 des Bundesverfassungsschutzgesetzes entsprechend, auch wenn sie nicht unter einer auf Dauer angelegten Legende tätig werden.

§ 14

Vertrauensleute

(1) Für den Einsatz von Privatpersonen, deren planmäßige, dauerhafte Zusammenarbeit mit dem Landesamt Dritten nicht bekannt ist (Vertrauensleute), ist § 13 Abs. 1 bis 3 entsprechend anzuwenden.

(2) Über die Verpflichtung von Vertrauensleuten entscheidet die Behördenleitung oder ihre Vertretung. Vertrauensleute müssen nach ihren persönlichen und charakterlichen Voraussetzungen für die Zusammenarbeit mit dem Verfassungsschutz geeignet sein. Diese Eignung ist fortlaufend durch das Landesamt zu überprüfen. Als Vertrauensleute dürfen Personen nicht angeworben und eingesetzt werden, die

1. nicht voll geschäftsfähig, insbesondere minderjährig sind,

2. von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden,

3. an einem Aussteigerprogramm teilnehmen,

4. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder Mitarbeiterin oder Mitarbeiter eines solchen Mitglieds sind oder

5. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

Die Behördenleitung oder ihre Vertretung kann eine Ausnahme von Satz 4 Nr. 5 zulassen, wenn die Verurteilung nicht als Täter eines Totschlags (§§ 212, 213 StGB) oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist und der Einsatz zur Aufklärung von Bestrebungen unerlässlich ist, die auf die Begehung von in § 3 Abs. 1 des Artikel 10-Gesetzes oder § 100b Abs. 2 der Strafprozessordnung bezeichneten Straftaten gerichtet sind. Im Falle einer Ausnahme nach Satz 5 ist der Einsatz nach höchstens sechs Monaten zu beenden, wenn er zur Erforschung der in Satz 5 genannten Bestrebungen nicht zureichend gewichtig beigetragen hat. Auch im Weiteren ist die Qualität der gelieferten Informationen fortlaufend zu bewerten.

§ 15

Verhältnismäßigkeit

(1) Von mehreren möglichen und geeigneten Maßnahmen hat das Landesamt diejenige zu treffen, die den Einzelnen und die Allgemeinheit am wenigsten beeinträchtigt.

(2) Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

(3) Eine Maßnahme ist nur zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

DRITTER TEIL

Speicherung, Sperrung, Löschung und Übermittlung personenbezogener Daten

§ 16

Geltung des Hessischen Datenschutzgesetzes

Das Hessische Datenschutzgesetz in der jeweils geltenden Fassung bleibt unberührt, soweit dieses Gesetz nichts anderes bestimmt. Die Vorschriften des Hessischen Datenschutzgesetzes über das Recht der betroffenen Person auf Gegenvorstellung aufgrund eines schutzwürdigen besonderen persönlichen Interesses und über die Beteiligung der datenverarbeitenden Stelle an gemeinsamen Verfahren finden keine Anwendung.

§ 17

Speicherung, Sperrung und Löschung

(1) Das Landesamt darf zur Erfüllung seiner Aufgaben personenbezogene Daten in Dateien speichern, verändern und nutzen, wenn

1. tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen,

2. dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 erforderlich ist oder

3. das Landesamt nach § 2 Abs. 3 tätig wird.

Unterlagen, die nach Satz 1 gespeicherte Angaben belegen, dürfen auch gespeichert werden, wenn in ihnen weitere personenbezogene Daten Dritter enthalten sind. Eine Abfrage von Daten Dritter ist unzulässig.

(2) Umfang und Dauer der Speicherung personenbezogener Daten sind auf das für die Aufgabenerfüllung des Landesamts erforderliche Maß zu beschränken.

(3) Das Landesamt darf Daten über eine minderjährige Person unter 14 Jahren in Dateien und zu ihrer Person geführten Akten nur speichern, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie eine der in § 3 Abs. 1 und 1a des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat.

(4) In Dateien oder zu ihrer Person geführten Akten gespeicherte Daten über eine minderjährige Person sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, dass nach Eintritt der Volljährigkeit weitere Erkenntnisse angefallen sind, die eine Fortdauer der Speicherung rechtfertigen. Nicht erforderliche Daten sind zu löschen.

(5) Personenbezogene Daten, die erhoben worden sind, um zu prüfen, ob Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen, dürfen in Dateien erst gespeichert werden, wenn sich tatsächliche Anhaltspunkte für derartige Bestrebungen oder Tätigkeiten ergeben haben. Bis zu diesem Zeitpunkt dürfen auch keine zur Person geführten Akten angelegt werden.

(6) Das Landesamt prüft bei der Einzelfallbearbeitung und im Übrigen nach von ihm festgesetzten angemessenen Fristen, spätestens jedoch nach fünf Jahren, ob gespeicherte personenbezogene Daten zur Aufgabenerfüllung noch erforderlich sind. Gespeicherte personenbezogene Daten über Bestrebungen nach § 2 Abs. 2 Nr. 1 und 3 bis 5 sind spätestens 15 Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, die Behördenleitung trifft im Einzelfall ausnahmsweise eine andere Entscheidung. Enthalten Sachakten oder Akten zu anderen Personen personenbezogene Daten, die nach Satz 2 zu löschen sind, dürfen sie nicht mehr verwendet werden. Soweit Daten automatisiert verarbeitet oder Akten automatisiert erschlossen werden, ist auf den Ablauf der Fristen nach Satz 1 und 2 hinzuweisen. Nicht erforderliche Daten sind zu löschen.

(7) Personenbezogene Daten sind nicht zu löschen, sondern nur zu sperren, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden,

2. die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind oder

3. die Verwendung der Daten zu wissenschaftlichen Zwecken erforderlich ist.

In den Fällen des Satz 1 Nr. 3 sind die Daten zum frühestmöglichen Zeitpunkt zu anonymisieren.

(8) In dem Verfahrensverzeichnis über automatisierte personenbezogene Textdateien ist die Zugriffsberechtigung auf Personen zu beschränken, die unmittelbar mit Arbeiten auf dem Gebiet betraut sind, dem die Textdateien zugeordnet sind; Auszüge aus Textdateien dürfen nicht ohne die dazugehörenden erläuternden Unterlagen übermittelt werden.

(9) Die Verpflichtung nach § 8 Abs. 1 und 2 des Hessischen Archivgesetzes vom 26. November 2012 (GVBl. S. 458) in der jeweils geltenden Fassung bleibt unberührt.

(10) Zum Zweck der gegenseitigen Information über den Einsatz von Vertrauenspersonen darf das Landesamt zusammen mit den Verfassungsschutzbehörden des Bundes und der anderen Länder eine Übersicht als gemeinsame Datei führen. Die Übersicht kann Angaben über wesentliche Eigenschaften der Vertrauenspersonen und deren Einsatzbereiche enthalten. Das Landesamt und das Hessische Landeskriminalamt koordinieren den jeweiligen Einsatz von Vertrauenspersonen; Näheres regeln gemeinsame Richtlinien.

§ 18

Zweckbindung

(1) Das Landesamt darf personenbezogene Daten nur zum Zweck der Aufgabenerfüllung des Verfassungsschutzes im Sinne des § 2 übermitteln. Zu anderen Zwecken dürfen personenbezogene Daten nur nach Maßgabe der §§ 21 bis 24 übermittelt werden.

(2) Personenbezogene Daten dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen übermittelt und in dem dafür erforderlichen Umfang verwendet werden.

§ 19

Informationsübermittlung durch öffentliche Stellen an das Landesamt

(1) Die Behörden, Gerichte hinsichtlich der dort geführten Register, sonstigen öffentlichen Stellen des Landes Hessen sowie die Gemeinden, Gemeindeverbände und sonstigen der Aufsicht des Landes Hessen unterstehenden juristischen Personen des öffentlichen Rechts haben dem Landesamt die ihnen bei Erfüllung ihrer Aufgaben bekanntgewordenen Informationen einschließlich personenbezogener Daten auch ohne vorheriges Ersuchen des Landesamts zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Informationen für die Erfüllung der Aufgaben des Landesamts erforderlich sein können. § 18 Abs. 1a und 1b des Bundesverfassungsschutzgesetzes bleibt unberührt. Die Übermittlung kann auch durch Einsichtnahme des Landesamts in Akten und Dateien der jeweiligen öffentlichen Stelle erfolgen, soweit die Übermittlung in sonstiger Weise den Zweck der Maßnahme gefährden oder einen übermäßigen Aufwand erfordern würde. Über die Einsichtnahme in amtlich geführte Dateien führt das Landesamt einen Nachweis, aus dem der Zweck und die eingesehene Datei hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu löschen. Unter den Voraussetzungen von Satz 1 übermitteln die Staatsanwaltschaften außerdem Anklageschriften und Urteile.

(2) Das Landesamt überprüft die übermittelten Informationen nach ihrem Eingang unverzüglich darauf, ob sie für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, dass die Informationen nicht erforderlich sind, werden sie unverzüglich gelöscht. Die Löschung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand erfolgen kann; in diesem Fall dürfen die nicht erforderlichen Informationen nicht verwendet werden.

(3) Die Übermittlung personenbezogener Daten nach Abs. 1, die aufgrund einer Maßnahme nach § 100a der Strafprozessordnung bekannt geworden sind, ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass jemand eine der in § 3 Abs. 1 und 1a des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat. Auf die dem Landesamt nach Satz 1 übermittelten Kenntnisse und Unterlagen findet § 4 Abs. 1 und 4 bis 6 des Artikel-10-Gesetzes entsprechende Anwendung.

(4) Die in Abs. 1 genannten Stellen sind zur Übermittlung verpflichtet, wenn im Einzelfall ein Ersuchen des Landesamts nach § 4 Abs. 3 vorliegt. Hält die ersuchte Stelle das Verlangen nach Auskunft oder Einsichtnahme nach § 4 Abs. 3 nicht für rechtmäßig, so teilt sie dies dem Landesamt mit. Besteht dieses auf dem Verlangen nach Auskunft oder Einsichtnahme, so entscheidet die für die ersuchte Stelle zuständige oberste Aufsichtsbehörde, soweit gesetzlich nichts anderes bestimmt ist.

§ 20

Informationsübermittlung durch das Landesamt an übergeordnete Behörden

(1) Das Landesamt unterrichtet die Ministerien und die Staatskanzlei über Bestrebungen und Tätigkeiten nach § 2 Abs. 2 oder tatsächliche Anhaltspunkte hierfür, die für deren Zuständigkeitsbereich von Bedeutung sind. Dabei dürfen auch personenbezogene Daten übermittelt werden.

(2) Das für den Verfassungsschutz zuständige Ministerium und das Landesamt dürfen personenbezogene Daten zum Zweck der Aufklärung der Öffentlichkeit über Bestrebungen und Tätigkeiten nach § 2 Abs. 2 oder tatsächliche Anhaltspunkte hierfür öffentlich bekanntgeben, wenn die Bekanntgabe für das Verständnis des Zusammenhangs oder der Darstellung von Organisationen erforderlich ist und das Allgemeininteresse das schutzwürdige Interesse der betroffenen Person überwiegt.

§ 21

Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs

(1) Das Landesamt darf Informationen einschließlich personenbezogener Daten, auch wenn sie mit nachrichtendienstlichen Mitteln erhoben wurden, an inländische öffentliche Stellen übermitteln, wenn der Empfänger die Informationen benötigt

1. zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit oder der Strafverfolgung oder

2. zur Erfüllung anderer ihm zugewiesener Aufgaben, sofern er dabei auch zum Schutz der freiheitlichen demokratischen Grundordnung beizutragen oder Gesichtspunkte der öffentlichen Sicherheit oder auswärtige Belange zu würdigen hat, insbesondere bei

a) der Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können,

b) der Sicherheitsüberprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder beschäftigt werden sollen,

c) der Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben, mit deren Einwilligung,

d) der sicherheitsbehördlichen Überprüfung von Einbürgerungsbewerberinnen und Einbürgerungsbewerbern,

e) der sicherheitsbehördlichen Überprüfung von Ausländerinnen und Ausländern im Rahmen der Bestimmungen des Ausländerrechts,

f) der Überprüfung der Zuverlässigkeit von Personen nach dem Luftsicherheits-, Atom-, Waffen-, Jagd- und Sprengstoffrecht,

g) der Überprüfung der Zuverlässigkeit von Personen nach den bewachungs- und gewerberechtlichen Vorschriften, insbesondere

aa) der Zulassung von Personen für den zugangsgeschützten Sicherheitsbereich von Veranstaltungen,

bb) von an der Hessischen Erstaufnahmeeinrichtung für Flüchtlinge und ihren Außenstellen beschäftigtem Sicherheitspersonal,

cc) von an kommunalen Flüchtlingsunterkünften eingesetztem Wachpersonal,

h) der Überprüfung der Zuverlässigkeit von an der Hessischen Erstaufnahmeeinrichtung für Flüchtlinge und ihren Außenstellen beschäftigten Dolmetscherinnen und Dolmetschern,

i) der Überprüfung der Zuverlässigkeit von Personen,

aa) die in mit Landesmitteln geförderten Beratungsstellen zur Prävention und Intervention gegen verfassungsfeindliche Bestrebungen oder in mit Landesmitteln geförderten Projekten eingesetzt sind oder eingesetzt werden sollen,

bb) die als Mitwirkende in beratenden Gremien zur Prävention und Intervention gegen verfassungsfeindliche Bestrebungen tätig sind oder tätig werden sollen,

mit deren Einwilligung,

j) der Zuverlässigkeitsüberprüfung von anstaltsfremden Personen nach den hessischen Vollzugsgesetzen, soweit im Einzelfall erforderlich,

k) Ordensverfahren zur Verleihung des Verdienstordens der Bundesrepublik Deutschland – mit Ausnahme der Verdienstmedaille – und des Hessischen Verdienstordens,

l) sonstigen Zuverlässigkeitsüberprüfungen und Überprüfungen von Personen, soweit dies gesetzlich vorgesehen ist,

m) im besonderen öffentlichen Interesse liegenden sonstigen Überprüfungen von Personen mit deren Einwilligung.

(2) Informationen, die mit nachrichtendienstlichen Mitteln erhoben wurden, dürfen an die Staatsanwaltschaften, die Finanzbehörden nach § 386 Abs. 1 der Abgabenordnung, die Polizeien, die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Gesetz über die Bundespolizei vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), zuletzt geändert durch Gesetz vom 5. Mai 2017 (BGBl. I S. 1066) wahrnehmen, nur übermittelt werden

1. zur Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

2. zur Verhinderung, sonstigen Verhütung oder Verfolgung von Straftaten von erheblicher Bedeutung oder

3. wenn der Empfänger die Informationen auch mit eigenen Befugnissen in gleicher Weise hätte erheben können.

Unter Straftaten von erheblicher Bedeutung nach Satz 1 Nr. 2 fallen Verbrechen im Sinne des § 12 Abs. 1 des Strafgesetzbuches vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 17. Juli 2017 (BGBl. I S. 2442), und schwerwiegende Vergehen im Sinne des § 12 Abs. 2 des Strafgesetzbuchs, wenn die Straftat im Einzelfall mindestens dem Bereich der mittleren Kriminalität zuzurechnen ist, sie den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigten. Unter den Voraussetzungen des § 20 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes ist das Landesamt zur Übermittlung verpflichtet.

(3) Soweit Informationen übermittelt werden, die mit Maßnahmen nach den §§ 7 oder 8 gewonnen wurden, gilt § 9 Abs. 1 entsprechend. Der Empfänger darf die Informationen nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung hinzuweisen.

(4) Zur Übermittlung nach den Abs. 1 und 2 ist auch das für den Verfassungsschutz zuständige Ministerium befugt; Abs. 3 gilt entsprechend.

§ 22

Informationsübermittlung durch das Landesamt an Stationierungsstreitkräfte und an ausländische öffentliche Stellen

(1) Das Landesamt darf Informationen einschließlich personenbezogener Daten, auch wenn sie mit nachrichtendienstlichen Mitteln erhoben wurden, an Dienststellen der Stationierungsstreitkräfte übermitteln, soweit die Bundesrepublik Deutschland dazu im Rahmen des Art. 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. 1961 II S. 1183, 1218) in der jeweils geltenden Fassung verpflichtet ist.

(2) Das Landesamt darf Informationen im Sinne des Abs. 1 auch übermitteln an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen, wenn die Übermittlung zur Wahrung erheblicher Sicherheitsinteressen des Emp-

fängers erforderlich ist, es sei denn, auswärtige Belange der Bundesrepublik Deutschland stehen der Übermittlung entgegen.

(3) Soweit Informationen übermittelt werden, die mit Maßnahmen nach den §§ 7 oder 8 gewonnen wurden, gilt § 9 Abs. 1 entsprechend. Der Empfänger darf die Informationen nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Landesamt sich vorbehält, Auskunft über die Verwendung der Daten zu verlangen.

(4) Zur Übermittlung nach den Abs. 1 bis 3 ist auch das für den Verfassungsschutz zuständige Ministerium befugt; Abs. 3 gilt entsprechend.

§ 23

Informationsübermittlung durch das Landesamt an Stellen außerhalb des öffentlichen Bereichs

(1) Das Landesamt darf personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs nicht übermitteln, es sei denn, dass dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen nach § 2 Abs. 3 Nr. 2 erforderlich ist und das für den Verfassungsschutz zuständige Ministerium im Einzelfall seine Zustimmung erteilt hat. Das Landesamt führt über die Auskunft nach Satz 1 einen Nachweis, aus dem der Zweck der Übermittlung, die Fundstelle und der Empfänger hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten. Der Empfänger darf die übermittelten personenbezogenen Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt wurden. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Landesamt sich vorbehält, Auskunft über die Verwendung der Daten zu verlangen. Satz 1 bis 4 finden keine Anwendung, wenn personenbezogene Daten zum Zwecke von Datenerhebungen nach § 4 übermittelt werden.

(2) Soweit Informationen übermittelt werden, die mit Maßnahmen nach den §§ 7 oder 8 gewonnen wurden, gilt § 9 Abs. 1 entsprechend. Der Empfänger darf die Informationen nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Landesamt sich vorbehält, Auskunft über die Verwendung der Daten zu verlangen.

(3) Zur Übermittlung nach Abs. 1 ist auch das für den Verfassungsschutz zuständige Ministerium befugt; Abs. 2 gilt entsprechend.

§ 24

Übermittlungsverbote

(1) Die Übermittlung von Informationen nach diesem Teil unterbleibt, wenn

1. erkennbar ist, dass unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Interesse der Allgemeinheit oder des Empfängers an der Übermittlung überwiegen,

2. überwiegende Sicherheitsinteressen, insbesondere Gründe des Quellenschutzes oder des Schutzes operativer Maßnahmen, dies erfordern oder

3. besondere gesetzliche Regelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(2) Ein Überwiegen im Sinne von Abs. 1 Nr. 1 und 2 liegt nicht vor, soweit die Übermittlung von Informationen erforderlich ist zur

1. Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im besonderen öffentlichen Interesse geboten ist, oder

2. Verfolgung einer besonders schweren Straftat im Sinne von § 100b Abs. 2 der Strafprozessordnung,

es sei denn, dass durch die Übermittlung eine unmittelbare Gefährdung von Leib oder Leben einer Person zu besorgen ist und diese Gefährdung nicht abgewendet werden kann. Die Entscheidung trifft in den Fällen von Satz 1 die Behördenleitung oder ihre Vertretung, die unverzüglich das für den Verfassungsschutz zuständige Ministerium unterrichtet. Das für den Verfassungsschutz zuständige Ministerium unterrichtet die Parlamentarische Kontrollkommission.

§ 25

Minderjährigenschutz

(1) Personenbezogene Daten minderjähriger Personen dürfen nach den Vorschriften dieses Gesetzes übermittelt werden, solange die Voraussetzungen ihrer Speicherung erfüllt sind. Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig, wenn sie zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer der in § 100a der Strafprozessordnung genannten Straftaten erforderlich ist.

(2) Personenbezogene Daten minderjähriger Personen dürfen nach den Vorschriften dieses Gesetzes nicht an ausländische oder über- oder zwischenstaatliche Stellen übermittelt werden.

§ 26

Nachberichtspflicht

Erweisen sich personenbezogene Daten nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig, sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, wenn dies zu einer anderen Bewertung der Daten führen könnte oder zur Wahrung schutzwürdiger Interessen der betroffenen Person erforderlich ist.

§ 27

Auskunft

(1) Das Landesamt erteilt der betroffenen Person über zu ihrer oder seiner Person gespeicherte Daten auf Antrag unentgeltlich Auskunft, soweit die betroffene Person hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt. Legt die betroffene Person nach Aufforderung ein besonderes Interesse nicht dar, entscheidet das Landesamt nach pflichtgemäßem Ermessen. Die Auskunft erstreckt sich nicht auf

1. die Herkunft der Daten und die Empfänger von Übermittlungen und

2. Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, der Betroffene macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem von der betroffenen Person dargelegten Auskunftsinteresse.

Das Landesamt bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Die Auskunftserteilung unterbleibt, soweit durch sie

1. eine Gefährdung der Erfüllung der Aufgaben zu besorgen ist,

2. Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamts zu befürchten ist,

3. die öffentliche Sicherheit gefährdet oder sonst dem Wohl des Bundes oder eines Landes ein Nachteil bereitet würde oder

4. Daten oder die Tatsache ihrer Speicherung preisgegeben werden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Die Entscheidung trifft die Behördenleitung oder eine von ihr besonders beauftragte Mitarbeiterin oder ein von ihr besonders beauftragter Mitarbeiter.

(3) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. Sie enthält einen Hinweis auf die Rechtsgrundlage für das Fehlen der Begründung und darauf, dass sich die betroffene Person an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen der oder des Hessischen Datenschutzbeauftragten an die betroffene Person dürfen ohne Zustimmung des Landesamts keine Rückschlüsse auf den Kenntnisstand des Landesamts zulassen.

VIERTER TEIL

Schlussvorschriften

§ 28

Einschränkung von Grundrechten

Aufgrund dieses Gesetzes können die Grundrechte auf Versammlungsfreiheit (Art. 8 Abs. 1 des Grundgesetzes, Art. 14 Abs. 1 der Verfassung des Landes Hessen), Brief-, Post- und Fernmeldegeheimnis (Art. 10 Abs. 1 des Grundgesetzes, Art. 12 der Verfassung des Landes Hessen) und Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 des Grundgesetzes, Art. 8 der Verfassung des Landes Hessen) eingeschränkt werden.

§ 29

Aufhebung bisherigen Rechts

Das Gesetz über das Landesamt für Verfassungsschutz vom 19. Dezember 1990 (GVBl. I S. 753)[*], zuletzt geändert durch Gesetz vom 27. Juni 2013 (GVBl. S. 444), wird aufgehoben.

§ 30

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Artikel 2
Gesetz zur parlamentarischen Kontrolle des Verfassungsschutzes in Hessen (Verfassungsschutzkontrollgesetz)

§ 1

Parlamentarische Kontrolle

(1) Die Landesregierung unterliegt hinsichtlich der Tätigkeit des Landesamts für Verfassungsschutz der parlamentarischen Kontrolle. Sie wird von der Parlamentarischen Kontrollkommission ausgeübt.

(2) Der Landtag wählt zu Beginn jeder Wahlperiode die Mitglieder der Parlamentarischen Kontrollkommission aus seiner Mitte.

(3) Er bestimmt die Zahl der Mitglieder, die Zusammensetzung und die Arbeitsweise der Parlamentarischen Kontrollkommission.

(4) Gewählt ist, wer die Stimmen der Mehrheit der Mitglieder des Landtags auf sich vereint.

(5) Scheidet ein Mitglied aus dem Landtag oder seiner Fraktion aus oder wird es Mitglied der Landesregierung, so verliert es seine Mitgliedschaft in der Parlamentarischen Kontrollkommission. Für dieses Mitglied ist unverzüglich ein neues Mitglied zu wählen; das Gleiche gilt, wenn ein Mitglied aus der Parlamentarischen Kontrollkommission ausscheidet.

(6) Die Parlamentarische Kontrollkommission wählt eine Vorsitzende oder einen Vorsitzenden aus ihrer Mitte und gibt sich eine Geschäftsordnung. Sie oder er wird durch eine bei der Präsidentin oder dem Präsidenten des Landtags eingerichtete Geschäftsstelle unterstützt.

[*] Hebt auf FFN 18-3

(7) Im Übrigen bleiben die Rechte des Landtags unberührt.

§ 2

Geheimhaltung, Protokollierung, Verwendung von mobilen Geräten

(1) Die Beratungen der Parlamentarischen Kontrollkommission sind geheim; das Sicherstellen der Geheimhaltung obliegt jedem Mitglied der Parlamentarischen Kontrollkommission. Hierauf weist die oder der Vorsitzende vor Beginn jeder Sitzung hin. Die Mitglieder sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit in der Parlamentarischen Kontrollkommission bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden.

(2) Die Sitzungen werden durch die Kanzlei des Landtags protokolliert. Zum Zwecke der Protokollierung werden die Sitzungen aufgezeichnet. Die Aufzeichnung ist spätestens zwei Wochen nach Fertigstellung des Protokolls zu löschen. Die Vorschriften der Verschlusssachenanweisung bleiben unberührt. Die oder der Vorsitzende leitet das Protokoll nach Fertigstellung der von der Präsidentin oder dem Präsidenten des Landtags bestimmten Stelle zur Registrierung und Verwaltung zu. Je eine Ausfertigung des Protokolls wird beim Landesamt für Verfassungsschutz sowie bei der Präsidentin oder dem Präsidenten des Landtags als Verschlusssache archiviert.

(3) Den Mitgliedern ist gestattet, sich für die Beratungen während der Sitzungen handschriftliche Notizen anzufertigen. Aus Gründen des Geheimschutzes stellt die oder der Vorsitzende im Anschluss an jede Sitzung die Einziehung und Vernichtung der handschriftlichen Notizen mit Sitzungsbezug sicher, soweit von der Erstellerin oder dem Ersteller der Notizen eine Verwahrung durch die Landtagsverwaltung nicht gewünscht wird. Wird Verwahrung gewünscht, übergibt das Mitglied der oder dem Vorsitzenden die Unterlagen in einem verschlossenen Umschlag. Die von der Präsidentin oder dem Präsidenten des Landtags bestimmte Stelle zur Registrierung und Verwaltung von Verschlusssachen verwahrt die handschriftlichen Notizen mit dem Protokoll der Sitzung. Jedem Mitglied ist auf Verlangen Einsicht in seine Notizen zu gewähren.

(4) Der Gebrauch von Mobiltelefonen, tragbaren elektronischen Datenverarbeitungsgeräten oder sonstigen Geräten zur Aufzeichnung von Bild- und Tondaten während der Sitzung ist nicht gestattet. Die oder der Vorsitzende stellt vor Beginn der Sitzung sicher, dass keine der in Satz 1 genannten Geräte eingesetzt werden können.

§ 3

Pflicht der Landesregierung zur Unterrichtung

(1) Das für den Verfassungsschutz zuständige Ministerium unterrichtet die Parlamentarische Kontrollkommission umfassend über die allgemeine Tätigkeit des Landesamts für Verfassungsschutz und über Vorgänge von besonderer Bedeutung. Das für den Verfassungsschutz zuständige Ministerium berichtet zu einem konkreten Thema aus dem Aufgabenbereich des Landesamts für Verfassungsschutz, sofern die Parlamentarische Kontrollkommission dies wünscht.

(2) Zeit, Art und Umfang der Unterrichtung der Parlamentarischen Kontrollkommission werden unter Beachtung des notwendigen Schutzes der Quellen durch die politische Verantwortung der Landesregierung bestimmt.

(3) Das für den Verfassungsschutz zuständige Ministerium unterrichtet die Parlamentarische Kontrollkommission

1. im Abstand von höchstens sechs Monaten über Auskunftsersuchen nach § 11 des Hessischen Verfassungsschutzgesetzes vom [*einsetzen: Datum und Fundstelle des Hessischen Verfassungsschutzgesetzes*], insbesondere durch einen Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen,

2. in jährlichem Abstand durch einen Lagebericht zu

a) Maßnahmen nach den §§ 7, 8 und 10 des Hessischen Verfassungsschutzgesetzes und

b) dem Einsatz von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern sowie Vertrauensleuten nach den §§ 13 und 14 des Hessischen Verfassungsschutzgesetzes

3. über die Dienstvorschrift des Landesamts für Verfassungsschutz für die Zusammenarbeit mit und insbesondere die Führung von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern sowie Vertrauensleuten nach den §§ 13 und 14 des Hessischen Verfassungsschutzgesetzes.

(4) Das für den Verfassungsschutz zuständige Ministerium erstattet dem Parlamentarischen Kontrollgremium des Bundes im Abstand von höchstens sechs Monaten einen Bericht nach § 8b Abs. 10 Satz 1 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Gesetz vom 16. Juni 2017 (BGBl. I

S. 1634), über die Durchführung von Maßnahmen nach § 11 Abs. 4 Nr. 2 und 3 des Hessischen Verfassungsschutzgesetzes; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben.

(5) Das für den Verfassungsschutz zuständige Ministerium unterrichtet die Parlamentarische Kontrollkommission über den Vollzug des Wirtschaftsplans im Haushaltsjahr.

§ 4

Befugnisse der Parlamentarischen Kontrollkommission

(1) Jedes Mitglied der Parlamentarischen Kontrollkommission kann die Einberufung einer Sitzung und die Unterrichtung der Parlamentarischen Kontrollkommission verlangen. Diese hat Anspruch auf entsprechende Unterrichtung durch die Landesregierung.

(2) Jedem Mitglied der Parlamentarischen Kontrollkommission ist Akteneinsicht zu gewähren. Die Akteneinsicht erstreckt sich auch auf vom Landesamt für Verfassungsschutz amtlich verwahrte Schriftstücke sowie die Einsicht in Daten des Landesamts für Verfassungsschutz. Soweit im Rahmen der Akteneinsicht erforderlich, ist den Mitgliedern der Parlamentarischen Kontrollkommission Zutritt zu den Dienststellen des Landesamts für Verfassungsschutz zu gewähren.

(3) Die Parlamentarische Kontrollkommission kann im Einzelfall zur Wahrnehmung ihrer Kontrollaufgaben mit der Mehrheit von zwei Dritteln ihrer Mitglieder nach Anhörung der Landesregierung beschließen, eine sachverständige Person mit der Durchführung von Untersuchungen zu beauftragen. Die sachverständige Person hat der Parlamentarischen Kontrollkommission über das Ergebnis der Untersuchungen zu berichten. Die Landesregierung ist der sachverständigen Person gegenüber in gleicher Weise zur Auskunft und Mitwirkung verpflichtet wie der Parlamentarischen Kontrollkommission. Insbesondere ist der sachverständigen Person auf Verlangen Akteneinsicht zu gewähren. § 2 Abs. 1 Satz 3 und 4 gilt entsprechend für die sachverständige Person.

(4) Die Parlamentarische Kontrollkommission kann der oder dem Hessischen Datenschutzbeauftragten Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben.

(5) Der Haushaltsplan des Landesamts für Verfassungsschutz wird der Parlamentarischen Kontrollkommission zur Mitberatung überwiesen.

§ 5

Mitarbeiterinnen und Mitarbeiter

(1) Die Mitglieder der Parlamentarischen Kontrollkommission haben das Recht, zur Unterstützung ihrer Arbeit je eine Mitarbeiterin oder einen Mitarbeiter ihrer Fraktion nach Anhörung der Landesregierung mit Zustimmung der Parlamentarischen Kontrollkommission zu benennen. Voraussetzung für diese Tätigkeit ist die Ermächtigung zum Umgang mit Verschlusssachen und die förmliche Verpflichtung zur Geheimhaltung.

(2) Die benannten Mitarbeiterinnen und Mitarbeiter sind befugt, die Beratungsgegenstände der Parlamentarischen Kontrollkommission mit den Mitgliedern der Parlamentarischen Kontrollkommission zu erörtern. Sie haben grundsätzlich keinen Zutritt zu den Sitzungen der Parlamentarischen Kontrollkommission. Die Parlamentarische Kontrollkommission kann im Einzelfall mit der Mehrheit von zwei Dritteln ihrer Mitglieder beschließen, dass Mitarbeiterinnen und Mitarbeiter der Fraktionen an bestimmten Sitzungen teilnehmen können.

§ 6

Berichterstattung

Die Parlamentarische Kontrollkommission erstattet dem Landtag mindestens in der Mitte und am Ende jeder Wahlperiode einen Bericht über ihre Kontrolltätigkeit. Dabei nimmt sie insbesondere dazu Stellung, ob die Landesregierung ihrer Unterrichtungspflicht zu Vorgängen von besonderer Bedeutung nachgekommen ist. Die Parlamentarische Kontrollkommission erstattet dem Landtag jährlich einen Bericht über die Durchführung sowie Art, Umfang und Anordnungsgründe der Auskunftsersuchen und Maßnahmen nach den §§ 7, 8, 10 und 11 des Hessischen Verfassungsschutzgesetzes; dabei sind die Grundsätze des § 2 Abs. 1 zu beachten.

§ 7

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Artikel 3
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

Zu Artikel 1 (Hessisches Verfassungsschutzgesetz)

A. Allgemeines

I. Anlass und Zielsetzung

1. Der signifikante Reformbedarf, der bei der Zusammenarbeit von Nachrichtendiensten, Polizei- und sonstigen Sicherheitsbehörden besteht, ist spätestens bei der politischen Aufarbeitung der Taten des sogenannten „Nationalsozialistischen Untergrunds“ (NSU) zutage getreten. Die Geschehnisse waren und sind Gegenstand umfassender parlamentarischer Untersuchungen.

Vor dem Hintergrund eines gesamtgesellschaftlichen Diskurses hat sich seit dem Jahr 2012 ein tiefgreifender Reformprozess der Verfassungsschutzbehörden vollzogen. In dessen Folge wurden nicht nur interne Geschäftsprozesse und Dienstvorschriften geprüft. Vielmehr hat auch eine gesellschaftliche Öffnung des Verfassungsschutzes eingesetzt, der besonders augenscheinlich in einer verstärkten Präventions- und Öffentlichkeitsarbeit zutage tritt. Neben der klassischen Informationsbeschaffung zu extremistischen Bestrebungen erstellt das Landesamt künftig verstärkt fundierte Gefahrenanalysen und darauf basierende Entwicklungsprognosen. Hierfür ist eine weitere Stärkung der Analysefähigkeit unabdingbar. Dies hat unter anderem in der Neugestaltung der Ausbildungswege für Verfassungsschützer Niederschlag gefunden. Weiterhin kamen nahezu sämtliche Formate der Zusammenarbeit innerhalb der Sicherheitsarchitektur auf den Prüfstand und wurden – wo notwendig – modifiziert und ergänzt.

2. Dessen ungeachtet hat sich herausgestellt, dass insbesondere im praktischen Zusammenwirken der Zentralstelle des Bundes und 16 Landesbehörden noch weiterer Optimierungsbedarf besteht. Diesen Handlungsbedarf und weitere praktische Defizite haben die Bund-Länder-Kommission Rechtsterrorismus (BLKR), der Bundestagsuntersuchungsausschuss „Rechtsterrorismus“ (NSU I) sowie die Expertenkommission der Hessischen Landesregierung (Expertenkommission) nachdrücklich aufgezeigt. Mithin ist es maßgebliches Ziel der vorliegenden Gesetzesnovelle, durch Umsetzen der in den jeweiligen Abschlussberichten ausgesprochenen Handlungsempfehlungen ein größtmögliches Maß an Harmonisierung und Zusammenarbeit auf dem Gebiet des Verfassungsschutzes zu erreichen.

Ausgehend von diesen Empfehlungen ergeben sich für die vorzunehmende Reform der gesetzlichen Grundlagen des Verfassungsschutzes in Hessen folgende Leitlinien:

- konsequente Beibehaltung des Trennungsgebots (BLKR-Abschlussbericht Rn. 793 f.)

- Harmonisierung bestehender gesetzlicher Übermittlungsvorschriften auf Landes- und Bundesebene/ Zusammenarbeit zwischen Polizeibehörden und Verfassungsschutz in der Praxis (BLKR-Abschlussbericht Rn. 798 f.).

Nach Einschätzung der Expertenkommission kommt der Verbesserung des Informationsaustauschs zwischen den Verfassungsschutzbehörden und den Strafverfolgungs- und Polizeibehörden entscheidende Bedeutung zu (Empfehlungen 33.01 bis 33.05, Rn. 349ff.). Die Regelungen zur Informationsübermittlung durch den Verfassungsschutz an die Polizei werden daher insbesondere im Lichte des Urteils des Bundesverfassungsgerichts vom 24. April 2013 zum Antiterrordatei-Gesetz (ATDG, BVerfGE 133, 277 ff.) geprüft und reformiert. Die BLKR hat zur Verbesserung des Informationsaustauschs weiter empfohlen, die Übermittlungsvorschriften in Bund und Ländern zu vereinheitlichen, so dass alle Sicherheitsbehörden auf Bundes- und Landesebene von einem einheitlichen Rechtsstandard ausgehen können.

- Quellenschutz (BLKR-Abschlussbericht Rn. 721 und 802, Expertenkommission Empfehlungen 47.01 bis 47.03, Rn. 489ff.)

Die BLKR und die Expertenkommission stimmen in ihren Abschlussberichten darin überein, dass der Quellenschutz nicht absolut sein kann, vielmehr der Schutz von Leib und Leben der Quellen und die Arbeitsfähigkeit der Verfassungsschutzbehörden mit den berechtigten Belangen der Strafverfolgung und Gefahrenabwehr in ein angemessenes Verhältnis zueinander zu bringen sind. Dem Postulat der Expertenkommission, wonach einer Überbewertung des Quellenschutzes entgegenzuwirken ist, wird auf gesetzlicher Ebene durch eine Anlehnung der Vorschriften zum Austausch von Informationen an den Verfassungsschutzverbund entsprochen. Hierdurch wird der gesetzliche Rahmen gesetzt, unter dem einschlägige untergesetzliche Maßnahmen wie insbesondere das Prinzip der „asymmetrischen Devolution“ weiter gestärkt werden können (vgl. Expertenkommission-Abschlussbericht, Rn. 496 f.).

- Verdeckte Informationsgewinnung durch V-Leute (BLKR-Abschlussbericht Rn. 802)

BLKR und Expertenkommission kommen zu dem Schluss, dass die Befugnis der Sicherheitsbehörden zum Einsatz von V-Leuten beibehalten werden soll. Allerdings seien einheitliche Standards erforderlich, zum Beispiel im Hinblick auf einen einheitlichen Sprachgebrauch für menschliche Quellen, einheitliche Vorgaben hinsichtlich der Auswahl (u.a. Vorstrafen), des Anwerbens und Führens von V-Leuten sowie des Beendigens der Zusammenarbeit. Ergänzend bestehe gesetzgeberischer Handlungsbedarf, einheitliche Rahmenbedingungen für den Einsatz menschlicher Quellen zur verdeckten Informationsgewinnung zu schaffen. Aus Gründen der Rechtsklarheit und Rechtssicherheit werden die Vorschriften zur Anordnung des Einsatzes Verdeckter Mitarbeiterinnen und Verdeckter Mitarbeiter und langfristiger Observationen entsprechend den Regelungen der Strafprozessordnung in den Polizeigesetzen von Bund und Ländern harmonisiert. Die gesetzliche Regelung der Übermittlungsverbote wird im Hinblick darauf, dass der Quellenschutz nicht absolut sei, angepasst.

- Überarbeitung der Vorschriften für die Datenspeicherung und Datenlöschung, Aktenhaltung und Aktenvernichtung

Zu diesem Themenbereich hat der NSU-Untersuchungsausschuss des Deutschen Bundestags (NSU I) die Forderung nach mehr Rechtsklarheit in den gesetzlichen Grundlagen der Nachrichtendienste für die Datenspeicherung und Datenlöschung, Aktenhaltung und Aktenvernichtung erhoben; es müssten Vorschriften geschaffen werden, die für die Bearbeiterinnen und Bearbeiter verständlich und möglichst unkompliziert handhabbar seien (BT-Drs. 17/14600 S. 864 Nr. 35 und 36).

3. Am 24. April 2013 hat das Bundesverfassungsgericht das Urteil zum Antiterrordatei-Gesetz (ATDG) verkündet. Darin hat das Gericht aus dem Grundrecht auf informationelle Selbstbestimmung ein „informationelles Trennungsprinzip“ herausgeschält und die Übermittlung von Informationen der Nachrichtendienste an die Polizei für operative polizeiliche Zwecke vom Vorliegen „eines herausragenden öffentlichen Interesses“ abhängig gemacht. Die so entfaltete Dogmatik des Verfassungsrechts gibt einerseits weiteren Anlass, die gesetzlichen Regelungen zum Informationsaustausch zwischen Verfassungsschutz und Sicherheitsbehörden zu reformieren, zieht aber andererseits den im Rahmen der Aufarbeitung des NSU-Komplexes entwickelten Vorschlägen, die künftige Zusammenarbeit zwischen den betroffenen Behörden effektiv auszugestalten, enge und deutliche Grenzen (vgl. die Nachbemerkung der BLKR zum ATDG-Urteil im Abschlussbericht S. 363).

4. Das Hessische Verfassungsschutzgesetz stammt in seiner Grundkonzeption aus dem Jahre 1990 (GVBl. I S. 323) und wurde seither mehrfach geändert. Durch die zahlreichen, teils umfangreichen Änderungen hat der Gesetzestext insgesamt an Lesbarkeit und Normenklarheit eingebüßt. Zwischenzeitig hat der Bundesgesetzgeber durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) dem aus der parlamentarischen Untersuchung, der Arbeit der BLKR und dem ATDG-Urteil des Bundesverfassungsgerichts aufgezeigten gesetzlichen Reformbedarf Rechnung getragen. Da dem Bund nach Art. 73 Abs. 1 Nr. 10 des Grundgesetzes hinsichtlich der Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes die ausschließliche Gesetzgebungskompetenz zukommt, enthält das reformierte Bundesverfassungsschutzgesetz auch für die Landesbehörden verbindliche Vorgaben.

5. Neben den dargelegten verfassungsrechtlichen und gesetzgeberischen Erwägungen soll der vorliegende Entwurf auch einen Mentalitätswandel im Landesamt für Verfassungsschutz unterstützen. Dazu gehören eine gezielte Öffentlichkeitsarbeit und das aktive Hinzutreten auf politische Entscheidungsträger und parlamentarische Kontrollgremien ebenso wie langfristig und strategisch ausgelegte Präventionsarbeit in der Gesellschaft. Ziel ist eine Philosophie, wonach sich das Landesamt nicht nur auf seine tradierte Aufgabe als Nachrichtendienst beschränkt, sondern sich als aktiver Partner und Dienstleister in der Mitte der Gesellschaft versteht. Nur dadurch kann das Vertrauen aller in Hessen und Deutschland lebenden Menschen in die Arbeit des Verfassungsschutzes gestärkt werden.

Durch die Bekämpfung jedweder Form des politischen, weltanschaulichen und religiösen Extremismus leistet das Landesamt einen unverzichtbaren Beitrag für den gesellschaftlichen Frieden und die persönliche Sicherheit des Einzelnen. Von der Vereitelung künftiger Straftaten wie denen von Hannover, Essen, Würzburg, Ansbach, Berlin und Hamburg wird die nachhaltig erfolgreiche Integration der vor Krieg und Bedrohung auch nach Hessen geflüchteten Menschen abhängen. Denn der Terrorismus und seine verheerenden gesellschaftlichen Folgewirkungen – u.a. ein erhöhtes Gewaltpotenzial rechtsextremistischer und islamfeindlicher Gruppierungen nebst linksextremistisch motivierter Resonanzstraftaten – bedrohen den Bestand der freiheitlich verfassten Demokratie insgesamt.

II. Inhalt und Systematik des Gesetzentwurfs

1. Das Landesamt für Verfassungsschutz stellt ein unverzichtbares Instrument der wehrhaften Demokratie in Hessen dar. Innerhalb der hessischen Sicherheitsarchitektur ergänzt das Landesamt als Nachrichtendienst ohne exekutiv-polizeiliche Befugnisse die Arbeit der Polizei und sonstigen Sicherheitsbehörden, indem es verfassungsfeindliche Bestrebungen im Vorfeld aufklärt und als Ansprechpartner für andere Nachrichtendienste im In- und Ausland zur Verfügung steht. Im Unterschied dazu besteht die Aufgabe der Polizei- und sonstigen Sicherheitsbehörden darin, die sich bereits zur konkreten Gefahr verdichteten Bestrebungen zu verhindern und daraus resultierende Straftaten aufzuklären, ohne dass ihnen dabei in gleicher Weise wie dem Verfassungsschutz der Einsatz nachrichtendienstlicher Mittel gestattet wäre. Demgemäß geht der Gesetzentwurf vom sogenannten Trennungsgebot aus: Das Landesamt ist als eigenständige Landesoberbehörde unter der Aufsicht des zuständigen Ministeriums ausgestaltet (§ 1 Abs. 1). Es bleibt somit von der im HSOG gesetzlich festgelegten Organisationsstruktur der Polizei getrennt und verfügt ausdrücklich über keine polizeilichen Exekutivbefugnisse (§ 5 Abs. 4). Aus der organisatorischen Trennung bei unterschiedlicher Reichweite der Eingriffsbefugnisse hat das Bundesverfassungsgericht im ATDG-Urteil das „informationelle Trennungsprinzip“ herausgeschält, das insoweit die Grenze für eine Informationsübermittlung durch das Landesamt an Strafverfolgungs- und Sicherheitsbehörden sowie sonstige Behörden und Stellen zieht (§§ 20ff.).

2. Die dem Landesamt eingeräumten Befugnisse zum Erheben von Informationen werden konsequent an den Vorgaben der Rechtsprechung des Bundesverfassungsgerichts ausgerichtet. Über den Rahmen der bisherigen Befugnisse hinaus werden dem Landesamt die Quellen-Telekommunikationsüberwachung (§ 6 Abs. 2 bis 4) und der verdeckte Zugriff auf informationstechnische Systeme (§ 8) erlaubt.

3. Um einerseits die Handlungsfähigkeit des Landesamts angesichts des hohen Bedrohungspotenzials durch den Terrorismus und seine Folgewirkungen auch in Zukunft sicherzustellen, andererseits aber auch das durch die Aufdeckung der NSU-Morde beeinträchtigte Vertrauen der Öffentlichkeit in die Arbeit des Verfassungsschutzes zu stärken, setzt der Gesetzentwurf auf eine moderne, scharf konturierte Gesetzesfassung, der eine klar strukturierte Systematik zugrunde liegt. Durch eine verbesserte Normenklarheit soll die Rechtssicherheit erhöht und die Grundlage für eine stärkere gesellschaftliche Akzeptanz geschaffen werden. Zugleich erhalten auch die Mitarbeiterinnen und Mitarbeiter des Landesamts für ihre tägliche Arbeit einen anwenderfreundlicheren gesetzlichen Rahmen.

a) Zum Erreichen der vorgenannten Ziele bindet der Gesetzentwurf das Hessische Verfassungsschutzgesetz stärker in den vom Bundesgesetzgeber für die Zusammenarbeit innerhalb des Verfassungsschutzverbunds geschaffenen Regelungskomplex ein (§§ 1 und 2 des Bundesverfassungsschutzgesetzes). Die Aufgabenbeschreibung (§ 2) übernimmt weitgehend die vom Bund genannte Elementaraufgabe des Sammelns und Auswertens von Informationen über verfassungsfeindliche Bestrebungen (§ 3 Abs. 1 des Bundesverfassungsschutzgesetzes) und ergänzt diese um das Beobachten der Organisierten Kriminalität (§ 2 Abs. 2 Nr. 5). Auch die Begriffsdefinitionen des Bundes (§ 4 des Bundesverfassungsschutzgesetzes) werden im Verweisungswege in das Landesrecht eingeführt (§ 3 Abs. 1).

b) Der Gesetzentwurf hält an der bisherigen Gliederung in vier Teile fest, strukturiert aber deren Inhalte neu. Die bislang zusammenhängend geregelten Aufgaben und Befugnisse werden – entsprechend der im Polizei- und Sicherheitsrecht bewährten Unterscheidung – getrennt normiert:

Der Erste Teil regelt die Organisation und die Aufgaben des Landesamts, der Zweite Teil dessen Befugnisse. Im Dritten Teil sind die Regelungen zur Speicherung, Sperrung, Löschung und Übermittlung personenbezogener Daten normiert. Im abschließenden Vierten Teil finden sich die üblichen Schlussvorschriften.

Die gesetzliche Regelung über die parlamentarische Kontrolle des Verfassungsschutzes wird – um die Gewaltenteilung stärker zu betonen – einem gesonderten Gesetz vorbehalten.

c) Bei den nachrichtendienstlichen Mitteln, die sich durch eine erhöhte Grundrechtssensibilität auszeichnen, setzt der Entwurf auf bundesweit einheitlich geltende rechtsstaatliche Standards. So enthält die Vorschrift über den verdeckten Einsatz technischer Mittel im Schutzbereich des Wohnungsgrundrechts (Art. 13 des Grundgesetzes, Art. 8 der Verfassung des Landes Hessen) einen Verweis auf bestimmte, vom Bundesverfassungsgericht im Urteil zum Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG-Urteil vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09) explizit anerkannte Rechtsgüter, für deren dringende Gefährdung tatsächliche Anhaltspunkte vorliegen müssen.

Beim Einholen von Auskünften von Telekommunikationsdiensteanbietern verweist der Gesetzentwurf auf § 8b Abs. 8 Satz 4 und 5 des Bundesverfassungsschutzgesetzes, so dass hinsichtlich der Pflicht zu Vorkehrungen für die technische und organisatorische Umsetzung der Auskunftsverpflichtung und hinsichtlich der technischen Einzelheiten die Vorschrift des § 110 des Telekommunikationsgesetzes und die dazu erlassene Rechtsverordnung sowie die Technische Richtlinie nach § 110 Abs. 3 des Telekommunikationsgesetzes gelten. Außerdem wird für das Erteilen von Auskünften der Telemediendiensteanbieter, Verkehrsunternehmen, Kreditinstitute u.ä. die Nachrichtendienste-Übermittlungsverordnung (NDÜV) des Bundes für anwendbar erklärt. Das Heranziehen bundeseinheitlich geltender Maßstäbe erleichtert den Austausch zwischen den Verfassungsschutzbehörden und hält die mit der Auskunftserteilung verbundene Belastung der verpflichteten Unternehmen so gering wie möglich. Zum Schutz der Betroffenen wird ein dem § 8b Abs. 5 des Bundesverfassungsschutzgesetzes entsprechendes Benachteiligungsverbot eingeführt.

Hinsichtlich der materiellen Grenzen (Schutz des Kernbereichs privater Lebensführung, Schutz zeugnisverweigerungsberechtigter Personen, Eingriff als “ultima ratio“ etc.) und des Verfahrens (Antrag, Durchführung, Mitteilung an Betroffene etc.) verwendet der Gesetzentwurf soweit möglich dynamische Rechtsgrundverweisungen auf das Gesetz zur Beschränkung des Brief-, Post und Fernmeldegeheimnisses – Artikel 10-Gesetz. Dieses enthält eine bundesweit geltende Grundlage für Maßnahmen der Nachrichtendienste sowohl des Bundes als auch der Länder im Schutzbereich des Art. 10 des Grundgesetzes und ist daher aus diesem Bereich den Mitarbeiterinnen und Mitarbeitern des Landesamts bereits vertraut. Das Artikel 10-Gesetz wurde im Jahre 1999 einer verfassungsgerichtlichen Überprüfung unterzogen (BVerfGE 100, 313ff.) und im Jahre 2001 aufgrund der vom Bundesverfassungsgericht aufgezeigten Vorgaben des Grundgesetzes beim Umgang mit personenbezogenen Daten verschärft (vgl. BT-Drs. 14/5655, S. 13).

Auf die zu Art. 10 des Grundgesetzes entwickelten Maßstäbe rekurriert das Bundesverfassungsgericht später in seinem Urteil zur akustischen Wohnraumüberwachung (BVerfGE 109, 279ff., insb. 63ff., 374ff.). Auf letzteres verweist wiederum das Urteil zur Online-Durchsuchung (BVerfGE 120, 274, 332ff.).

Dass für Daten, die durch einen Eingriff in Art. 10 Abs. 1 des Grundgesetzes, in Art. 13 Abs. 1 des Grundgesetzes oder in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes) gewonnen werden, in weiten Teilen vergleichbar strenge Anforderungen gelten, hat das Bundesverfassungsgericht im ATDG-Urteil nochmals deutlich gemacht (BVerfGE 133, 277 Rn. 225f.). Auch wenn für Eingriffe in Art. 13 Abs. 1 des Grundgesetzes und für den verdeckten Zugriff auf informationstechnische Systeme teilweise, insbesondere aufgrund des Richtervorbehalts, noch strengere Voraussetzungen gelten als für Maßnahmen im Schutzbereich des Art. 10 des Grundgesetzes, bietet es sich an, die Vorschriften des Artikel 10-Gesetzes, soweit in ihnen Anforderungen normiert wurden, die für besonders grundrechtssensible Maßnahmen unterschiedslos gelten, als rechtsstaatlichen bundeseinheitlichen Standard auch einheitlich den einzelnen Befugnisnormen zugrunde zu legen. Dadurch lassen sich die komplizierten Vorschriften des bisherigen Gesetzes zu Anforderungen an den Einsatz besonderer nachrichtendienstlicher Mittel erheblich vereinfachen.

Die Regelungstechnik des dynamischen Verweises auf Vorschriften des Artikel 10-Gesetzes wird bereits im bisherigen Gesetz verwendet, ebenso vom Bundesgesetzgeber. Der Gesetzentwurf setzt diese Regelungstechnik konsequent weiter um. Dies bietet auch den Vorteil, dass eventuelle Änderungen des Artikel 10-Gesetzes durch den Bundesgesetzgeber, welche in der Regel durch die Fortentwicklung der Rechtsprechung des Bundesverfassungsgerichts ausgelöst werden, automatisch in das Landesrecht übernommen werden. Der Landtag hätte dennoch jederzeit die Möglichkeit, auf unerwünschte Änderungen des Artikel 10-Gesetzes durch eine Änderung der Verweisungsnormen im HVSG zu reagieren.

d) Besonders hohen Wert legt der Gesetzentwurf darauf, bundeseinheitliche Standards für den Einsatz von Verdeckten Mitarbeiterinnen, Verdeckten Mitarbeitern und Vertrauensleuten zu normieren. Daher übernimmt der Entwurf die entsprechenden Vorschriften des Bundes (§§ 9a und 9b des Bundesverfassungsschutzgesetzes) weitestgehend wörtlich (§§ 13 und 14). Darin hat der Bundesgesetzgeber die diesbezüglichen Empfehlungen der BLKR zur Stärkung der Akzeptanz (Abschlussbericht Rn. 650) aufgegriffen und den Einsatzrahmen gesetzlich festgelegt (vgl. BT-Drs. 18/4654, S. 25ff.). Die im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zu Verdeckten Mitarbeiterinnen, Verdeckten Mitarbeitern und Vertrauensleuten waren im Zuge des Gesetzgebungsverfahrens nochmals verschärft worden (vgl. BT-Drs. 18/5415, S. 9, Ausschussdrucksache 18(4)350). Die nunmehrige Gesetzesfassung beruht auf einem breiten Konsens auf Bundesebene. Soweit dieser Gesetzentwurf geringfügig im Wortlaut abweicht, ist dies der anderen Gesetzessystematik, den funktionellen Unterschieden zwischen Bundes- und Landesamt für Verfassungsschutz sowie der Rechtssicherheit und -klarheit geschuldet.

4. Im Interesse der erforderlichen Verbesserung der Zusammenarbeit des Verfassungsschutzes mit den Strafverfolgungs- und Sicherheitsbehörden sieht der Gesetzentwurf eine ausdrückliche Klarstellung der entsprechenden Verpflichtung im Rahmen und in den Grenzen des Trennungsprinzips vor (§ 5 Abs. 4). Zur weiteren Harmonisierung der Übermittlungsvorschriften lehnt sich der Gesetzentwurf hinsichtlich der Informationsübermittlung durch das Landesamt (§§ 20ff.) eng an die im Hinblick auf das ATDG-Urteil des Bundesverfassungsgerichts überarbeitete Vorschrift für das Bundesamt für Verfassungsschutz an (§ 19 des Bundesverfassungsschutzgesetzes). Auch die Regelung der Übermittlungsverbote (§ 24) stimmt weitgehend wörtlich mit dem Bundesgesetz überein (§ 23 des Bundesverfassungsschutzgesetzes). Zudem wird die kraft Bundesrechts für die länderübergreifende Zusammenarbeit bestehende Pflicht zur Übermittlung von Informationen (§ 21 Abs. 1 des Bundesverfassungsschutzgesetzes) auf die Zusammenarbeit innerhalb Hessens ausgedehnt (§ 21 Abs. 2 Satz 2).

5. Um die Rechtsklarheit zu verbessern und die Transparenz zu erhöhen, werden die Vorschriften über die Speicherung, Löschung und Archivierung von Dateien und Akten enger an das allgemeine Datenschutzrecht angebunden. Die Ausnahmen von der Anwendbarkeit des Hessischen Datenschutzgesetzes (§ 16) werden zurückgenommen und Sonderregelungen auf das im Hinblick auf die Funktion des Landesamts als Nachrichtendienst Notwendige beschränkt.

6. Die Auswirkungen der Entscheidung des Bundesverfassungsgerichts vom 20. April 2016 zum BKA-Gesetz wurden wie folgt berücksichtigt:

Die angegriffenen Befugnisse ermächtigen das Bundeskriminalamt (BKA) im Rahmen der Gefahrenabwehr und Straftatenverhütung zur heimlichen Erhebung personenbezogener Daten und begründen – je nach Befugnis – Eingriffe in die Grundrechte

der Unverletzlichkeit der Wohnung, des Telekommunikationsgeheimnisses und der informationellen Selbstbestimmung sowie in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht). Die dem BKA eingeräumten Befugnisse werden vom Grundsatz her vom Bundesverfassungsgericht nicht beanstandet, unterliegen als Ausfluss der Verhältnismäßigkeit jedoch bestimmten vom Gericht formulierten Anforderungen, die insbesondere in § 6 Abs. 3 und 4 HVSG berücksichtigt werden.

B. Zu den einzelnen Vorschriften

Zum Ersten Teil (Organisation und Aufgaben des Landesamts)

Zu § 1 (Organisation des Landesamts)

§ 1 entspricht weitgehend dem bisherigen § 1. Nach Abs. 1 handelt es sich beim Landesamt um eine Landesoberbehörde, die dem Geschäftsbereich des für den Verfassungsschutz zuständigen Ministeriums zu- und diesem unmittelbar nachgeordnet ist. Das Landesamt ist als eine von der Organisationsstruktur der Polizei getrennte eigenständige Behörde ausgestaltet. Abs. 2 regelt die Zusammenarbeit mit den Verfassungsschutzbehörden anderer Länder und dem Bundesamt für Verfassungsschutz.

Zu § 2 (Aufgaben des Landesamts)

In § 2 wird der Aufgabenkreis des Landesamts festgelegt. Insoweit besteht in Inhalt und Umfang kein Unterschied zur bisherigen Rechtslage.

In § 2 Abs. 1 Satz 1 wird die aus Art. 73 Nr. 10 des Grundgesetzes, § 1 des Bundesverfassungsschutzgesetzes folgende Zusammenarbeitsverpflichtung dem Landesamt zugewiesen. Verschiedene andere Länder (vgl. etwa § 3 Abs. 1 Landesverfassungsschutzgesetz Rheinland-Pfalz oder § 3 Abs. 1 Hamburgisches Verfassungsschutzgesetz) haben Entsprechendes bereits normiert. Sicherheitsbedrohungen machen nicht an Landesgrenzen halt. Dementsprechend ist im Abschlussbericht des Bundestagsuntersuchungsausschusses „Rechtsterrorismus“ (NSU I) auf S. 864 (Empfehlung Nr. 32) zu lesen: „Künftig muss sichergestellt sein, dass im Verfassungsschutzverbund vorliegende Informationen von länderübergreifender Bedeutung zentral zusammengeführt und auch tatsächlich gründlich ausgewertet werden sowie die Ergebnisse dieser Auswertung allen zuständigen Verfassungsschutzbehörden zur Verfügung stehen. Zur Vermeidung von Doppelarbeit muss für eine effiziente Abstimmung im Verfassungsschutzverbund Sorge getragen sein.“ Ein zeitgemäßes Föderalismusverständnis bezieht die gewollte Vielfalt bei der sicherheitspolitischen Verantwortung ohne Verlust von Effektivität in gemeinsame Lösungen ein. Das Vorgehen von 16 Landesbehörden und dem Bund verlangt vor allem eine ständige gegenseitige Informations- und Kooperationsbereitschaft.

Neben der bestehenden Zusammenarbeitspflicht wird sich Hessen auch künftig in den auf Bundesebene bestehenden Zentren engagieren. Bereits 2004 wurde das „Gemeinsame Terrorismusabwehrzentrum (GTAZ)“ als Analyse- und Informationsstelle von Polizei und Nachrichtendiensten eingerichtet. Nach der Aufdeckung der NSU-Morde haben der Bund und die Länder 2011 das „Gemeinsame Abwehrzentrum Rechtsextremismus“ (GAR) geschaffen. Das GAR ist im November 2012 mit der Aufnahme des Wirkbetriebs des „Gemeinsamen Extremismus- und Terrorismusabwehrzentrums“ (GETZ) um die Bereiche Ausländerextremismus, Linksextremismus/Linksterrorismus und Spionage/Proliferation erweitert worden. Nunmehr findet eine effiziente und effektive Kommunikation zwischen den Sicherheitsbehörden von Bund und Ländern in allen Phänomenbereichen statt. Hierdurch wird auch die Wahrnehmung der Koordinierungsfunktion des Bundesamts für Verfassungsschutz erleichtert.

Hessen beteiligt sich durch Verbindungsbeamte an den genannten Zentren. Innerhalb Hessens ist die Zusammenarbeit der Verfassungsschutz- und Polizeibehörden auf allen Verwaltungs- und Hierarchieebenen langjährige Praxis. Bis zur Sachbearbeiterebene gibt es vielfältige Kooperationen und Informationswege. Besondere Erwähnung verdient das bereits 2006 eingerichtete „Gemeinsame Informations- und Analysezentrum“ (GIAZ) im Landespolizeipräsidium. Behördenübergreifend werden im GIAZ zwischen Polizei und Verfassungsschutz gemeinsam erarbeitete und abgestimmte Informationen relevanter Bereiche der politisch motivierten Kriminalität und des Extremismus den politischen Entscheidungsträgern zur Verfügung gestellt. Ziel ist dabei eine empfängerorientierte Aufbereitung und Auswertung von nachrichtendienstlichen und polizeilichen Erkenntnissen. Im GIAZ versehen Polizeibeamtinnen und Polizeibeamte sowie Beamtinnen und Beamte des Verfassungsschutzes anlassbezogen Dienst. Die Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten üben hierbei keine polizeiliche Tätigkeit aus.

Durch Abs. 1 Satz 2 wird die bislang in § 2 Abs. 1 Satz 1 beschriebene Aufgabe unverändert fortgeführt. Dagegen normiert § 2 Abs. 1 Satz 3 nun explizit den Präventionsauftrag des Landesamts. Bereits dem bisherigen § 2 Abs. 1 Satz 1 („… rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung … zu treffen,“) konnte in Verbindung mit den Vorschriften über die Unterrichtung der Öffentlichkeit nach § 9 die Zulässigkeit der Präventionsarbeit beziehungsweise ein entsprechender Auftrag entnommen werden. Ausdrücklich gesetzlich normiert war dieser Auftrag bisher jedoch nicht. Durch diesen nun formulierten gesetzlichen Auftrag zur Prävention wird ein deutliches Signal zum Ausbau der amtsinternen Präventionsstrukturen in allen Phänomenbereichen gesetzt, aber auch die Grundlage für eine effektive und dauerhafte Unterstützung des Hessischen Informations- und Kompetenzzentrums gegen Extremismus (HKE)

geschaffen, das die Hessische Landesregierung mit Kabinettbeschluss vom 4. Februar 2013 zur Koordinierung und Vernetzung der Programme und Projekte gegen jeglichen Extremismus eingerichtet hat. Die Innenministerkonferenz (IMK) hat sich bereits im Rahmen ihrer Sitzung vom 8./9. Dezember 2011 zur Notwendigkeit von Präventionsarbeit im Verfassungsschutz bekannt (TOP 22, Beschluss Ziffer 1). Präventionsarbeit einer Verfassungsschutzbehörde besteht einerseits darin, die Öffentlichkeit über die Erscheinungen von Extremismus und Terrorismus aufzuklären. Das kann in Podiumsveranstaltungen, bei der Lehrerfortbildung oder durch Besuche in Schulen erfolgen. Einen allgemeinen Bildungsauftrag hat die Verfassungsschutzbehörde nicht. Hier sind die Bildungsinstitutionen des Landes, der kommunalen und freien Träger gefordert. Prävention im engeren Sinne ist andererseits ein zielgerichtetes Tätigwerden zum Verhindern des Ausbreitens extremistischer oder terroristischer Bestrebungen. Hier geht es vor allem um Gespräche mit und Kontakte zu gesellschaftlichen Gruppen und Gremien, allgemein und in konkret veranlassten Einzelfällen.

Nachdem die Notwendigkeit der Extremismus-Prävention als eigene Aufgabe inzwischen unbestritten ist, soll sie auch gesetzlich verankert werden. Der neue § 2 Abs. 1 Satz 3 umfasst die bisherigen Tätigkeiten des Landesamts und ist gleichzeitig die Grundlage für weitere Präventionsprogramme und -aktivitäten. Die Veröffentlichung des Jahresberichts entstammt systematisch ebenfalls dem Präventionsbereich, weshalb die vormals in § 9 Abs. 3 befindliche Regelung nunmehr in § 2 Abs. 1 Satz 4 normiert wird.

Der in § 2 Abs. 2 Nr. 1 bis 4 genannte Beobachtungsauftrag ist deklaratorischer Natur und gibt die dem Landesamt bereits durch § 3 Abs. 1 des Bundesverfassungsschutzgesetzes zugewiesene Aufgabe wieder.

§ 2 Abs. 2 Nr. 5 erweitert den Kreis der in § 3 Abs. 1 des Bundesverfassungsschutzgesetzes normierten Beobachtungsaufgaben für Hessen um die Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität (OK). Die Bedrohung durch die OK erfordert einen ganzheitlichen und nachhaltigen Bekämpfungsansatz. Im Rahmen der Bekämpfung der OK gilt es, die Einflussnahme der OK auf Politik, Medien, öffentliche Verwaltung, Justiz und Wirtschaft zu verhindern. Dabei kann der Verfassungsschutz bei niedriger Einschreitschwelle bereits im Vorfeld konkreter Gefahrenlagen sowie im Vorfeld der Begehung und Aufklärung von Straftaten tätig werden.

Die Beobachtung durch den Verfassungsschutz ist langfristig angelegt und nicht auf Ermittlungsverfahren ausgerichtet. Dies ermöglicht eine nachhaltige Beobachtung, etwa auch nach dem Abschluss von polizeilichen Ermittlungsverfahren. Insbesondere unter Einbeziehung von Erkenntnissen aus den unterschiedlichen Extremismus-Phänomenbereichen können Bezüge zur OK frühzeitig erkannt werden, so z.B. im Rahmen islamistisch geprägter terroristischer Erkenntnisse im Zusammenhang mit dem internationalen Waffenhandel und der Geldwäsche.

Durch seine in Deutschland und Europa zentrale wirtschaftsgeographische Lage, den internationalen Finanzplatz Frankfurt am Main sowie das dortige Luftverkehrskreuz (FRA) ist Hessen auch Schauplatz international verflochtener Kriminalität. Regelmäßig verschieben sich die Schwerpunkte der OK-Beobachtung. Während lange Zeit das Hauptaugenmerk insbesondere russischen und italienischen OK-Gruppen galt, bilden nunmehr in Hessen tätige kriminelle Rockergruppen, sog. Outlaw Motorcycle Gangs (OMCG), einen Beobachtungsschwerpunkt des Landesamts (vgl. Verfassungsschutz in Hessen – Bericht 2015, S. 158f.). Vor diesem Hintergrund hat sich die im Jahr 2002 eingeschlagene Strategie bewährt, auch das Landesamt zur präventiven Bekämpfung der OK einzusetzen.

Das Landesamt arbeitet hierbei eng mit seinen Partnerbehörden zusammen (vgl. Gemeinsamer Runderlass des Hessischen Ministeriums des Innern und für Sport und des Hessischen Ministeriums der Justiz, für Integration und Europa über Richtlinien zur Zusammenarbeit von Polizei, Justiz und Verfassungsschutz bei der Beobachtung der OK vom 23. Dezember 2013, StAnz. 2014, S. 94). Die Vorteile einer Beobachtung der OK durch den Verfassungsschutz ergeben sich dabei aus dem speziellen, nachrichtendienstlichen Wissen des Verfassungsschutzes und den ihm als eigenständige, die Arbeit der Polizei ergänzende Sicherheitsbehörde gesetzlich zugewiesenen Aufgaben und Befugnissen. Ähnlich wie terroristische Organisationen und ausländische Geheimdienste arbeitet die OK konspirativ und beruht auf einem System von Steuerungsstrukturen, weshalb es erforderlich ist, mit nachrichtendienstlichen Mitteln Täter und Strukturen zu identifizieren. Da die Schwelle zum Tätigwerden für das Landesamt für Verfassungsschutz im Hinblick auf die klassische Aufgabe der Vorfeldbeobachtung bereits bei tatsächlichen Anhaltspunkten für eine Beeinträchtigung gesetzlicher Schutzgüter erreicht wird, kann der Verfassungsschutz früher als die Polizei tätig werden.

Bei der Bekämpfung der OK arbeitet das Landesamt mit Nachrichtendiensten anderer Länder zusammen. In rechtssystematischer Ausnahme von § 5 Abs. 5 des Bundesverfassungsschutzgesetzes ist der unmittelbare Dienstverkehr mit zuständigen Stellen anderer Staaten, also insbesondere ausländischen Nachrichtendiensten zulässig, weil die OK-Bekämpfung nicht zu dem Kreis der in § 3 Abs. 1 des Bundesverfassungsschutzgesetzes normierten Beobachtungsaufgaben zählt. In mehreren Nachbarstaaten und fast allen Mitgliedstaaten der Europäischen Union sind die Inlandsnachrichtendienste umfassend oder in Teilbereichen mit der Beobachtung der OK befasst. Für diese bildet das Landesamt einen adäquaten Ansprechpartner.

Da die OK ihre Aktivitäten in der Regel nicht nur lokal entfaltet, sondern länderübergreifend, bundesweit und meist auch international vernetzt ist, erstreckt sich die Beobachtung der OK auf den gesamten Geltungsbereich des Grundgesetzes.

Nach § 2 Abs. 3 wirkt das Landesamt nach § 3 Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes bei Sicherheitsüberprüfungen, Zuverlässigkeitsüberprüfungen und Überprüfungen in sonstigen gesetzlich bestimmten Fällen mit. Es handelt sich hierbei um die im bisherigen § 2 Abs. 5 geregelten sog. Mitwirkungsaufgaben, bei denen das Landesamt grundsätzlich auf der Basis seiner bereits vorhandenen Daten arbeitet (§ 4 Abs. 5). Während § 2 Abs. 3 zunächst eine rein deklaratorische Aufgabenbenennung enthält, finden sich die zugehörigen Übermittlungsbefugnisse sowie diesbezüglich konkretisierende Verfahrensregelungen in der Vorschrift zur Informationsübermittlung innerhalb des öffentlichen Bereichs (§ 21 Abs. 1 Nr. 2).

§ 2 Abs. 4 entspricht § 2 Abs. 6 des bisherigen Gesetzes.

Zu § 3 (Begriffsbestimmungen)

§ 3 überführt die bisher in § 2 Abs. 3 gesondert definierten Begrifflichkeiten in eine sich eng am Wortlaut des Bundesgesetzgebers orientierende eigenständige Vorschrift.

In Abs. 1 werden die Begriffsbestimmungen aus § 4 Abs. 1 Satz 1, 2 und 4 sowie Abs. 2 des Bundesverfassungsschutzgesetzes für den Anwendungsbereich des Hessischen Verfassungsschutzgesetzes übernommen. Dies verdeutlicht, dass es sich hierbei um gemeinsame Rechtsgüter des Bundes und aller Länder handelt, denen ein bundesweit einheitliches Begriffsverständnis zugrunde liegt. Der Bundesgesetzgeber hat hinsichtlich der Begriffe der freiheitlichen demokratischen Grundordnung und des Bestands und der Sicherheit des Bundes oder eines Landes auf die Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 2, 1ff. und 5, 85ff.) sowie die gesetzliche Regelung in § 92 StGB zurückgegriffen (BT-Drs. 11/4306, S. 60).

Die Zulässigkeit der Beobachtung durch das Landesamt hängt dabei nicht von individuellen und subjektiven Beiträgen der betroffenen Person oder deren intentionalen Beteiligung an Handlungen zur Beseitigung der freiheitlichen demokratischen Grundordnung ab. Es werden demgemäß keine Voraussetzungen verlangt, die über die Mitgliedschaft in dem Personenzusammenschluss hinausgehen (vgl. BVerwGE 135, 275 Rn. 66). Die Zulässigkeit einer Beobachtung von Personen, die nicht Mitglied in einem solchen Personenzusammenschluss sind (Einzelpersonen), ist in § 4 Abs. 1 Satz 4 des Bundesverfassungsschutzgesetzes geregelt.

§ 4 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes bestimmt, dass Personen beobachtet werden können, die für einen Personenzusammenschluss handeln (also nicht in dem Personenzusammenschluss). Einschränkende Voraussetzung hierfür ist das zusätzliche Erfordernis einer nachdrücklichen Unterstützung.

Abs. 2 übernimmt unverändert die Definition des Begriffs der OK aus § 2 Abs. 3 Buchst. d des bisherigen Gesetzes.

Zum Zweiten Teil (Befugnisse des Landesamts)

Zu § 4 (Informationserhebung)

Die Norm bündelt die Befugnisse des Landesamts zur Informationserhebung ohne den Einsatz nachrichtendienstlicher Mittel. Die zuvor auf die §§ 3 und 4 aufgeteilten Befugnisse werden inhaltlich nicht erweitert, sondern strukturell in einer Norm zusammengefasst und nach Art der Erhebung differenziert aufgeführt. Dies erleichtert zum einen die Anwendbarkeit der Norm, schafft zum anderen zusätzliche Transparenz für die Bürgerinnen und Bürger. Die notwendige Sorgfalt beim Umgang mit den beim Landesamt vorhandenen Daten, insbesondere die Art der Aktenführung, der Informationsverwaltung und der Löschung ist durch eine detaillierte Dienstvorschrift zu regeln. Neben datenschutzrechtlichen Aspekten dient dies dem Wissensmanagement in der Behörde und sichert die Verfügbarkeit der Informationen zu dem Zeitpunkt, in welchem sie gebraucht werden.

Abs. 5 bestimmt als allgemeine Vorschrift, dass das Landesamt bei der Beantwortung von Übermittlungsersuchen maßgeblich auf der Basis seiner im Zeitpunkt des Ersuchens bereits vorhandenen Informationen arbeitet. Unberührt davon bleiben spezialgesetzliche, z.B. im Hessischen Sicherheitsüberprüfungsgesetz geregelte Befugnisse zur Datenerhebung in Mitwirkungsangelegenheiten. Ferner darf das Landesamt, wie Abs. 5 Satz 2 klarstellt, zur Beantwortung von Übermittlungsersuchen Daten aus öffentlich zugänglichen Quellen erheben bzw. unter den genannten Voraussetzungen Auskünfte bei öffentlichen Stellen oder Dritten einholen. Aus der Systematik von § 4 Abs. 3 und 5 folgt demnach, dass das Landesamt zur Beantwortung von Übermittlungsersuchen keine Daten mit nachrichtendienstlichen Mitteln erheben darf.

Zu § 5 (Informationserhebung mit nachrichtendienstlichen Mitteln)

§ 5 regelt die Informationserhebung mit nachrichtendienstlichen Mitteln sowie die allgemeinen Grenzen des Einsatzes. Der Einsatz nachrichtendienstlicher Mittel wurde im Rahmen der Aufarbeitung der NSU-Taten eingehend erörtert. Ein vollständig einvernehmliches Ergebnis konnte hierbei im Bundestagsuntersuchungsausschuss „Rechtsterrorismus“ (NSU I) nicht erzielt werden. Die Verantwortung für die Bekämpfung jeder Form von Extremismus ist groß. Der Schutz der Bürgerinnen und Bürger und die Sicherung der Grundrechte unserer Demokratie sind hierbei oberstes Gebot. Es bedarf eines starken zivilgesellschaftlichen Bewusstseins, Engagements aber auch staatlichen Handelns. Eine wehrhafte Demokratie muss den Feinden der Verfassung unter Einsatz aller rechtsstaatlichen Mittel entgegentreten. Dazu gehören auch nachrichtendienstliche Mittel. Kon-

spirativ agierende Gruppen hätten sonst leichtes Spiel, im Vorfeld polizeilicher Handlungsmöglichkeiten planen zu können. Zu diesem Ergebnis gelangte auch die Bund-Länder-Kommission Rechtsterrorismus. Konsens in diesem Zusammenhang ist es allerdings auch, dass der Einsatz nachrichtendienstlicher Mittel normenklar geregelt und kontrollierbar sein muss.

Der Gesetzentwurf enthält daher neben einer neu eingeführten Legaldefinition eine abschließende Aufzählung der nachrichtendienstlichen Mittel, deren konkrete Voraussetzungen in den Folgeparagraphen aufgeführt sind. Durch die ausdrückliche, ausdifferenzierte gesetzliche Regelung wird der grundrechtlichen Relevanz nachrichtendienstlicher Mittel noch deutlicher als bisher Rechnung getragen. Zudem wird die Arbeit des Verfassungsschutzes erkennbar transparenter.

Zu § 6 (Überwachung des Brief-, Post- und Fernmeldeverkehrs und der Telekommunikation)

Zu Abs. 1:

Die Vorschrift hat ausschließlich klarstellenden Charakter. Die Überwachung des Brief-, Post- und Fernmeldeverkehrs richtet sich aufgrund der erheblichen Grundrechtsrelevanz ausschließlich nach den Vorschriften des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz).

Im Einzelfall kann es im Rahmen möglicher Beschränkungen des Art. 10 des Grundgesetzes auch zulässig sein, einen sog. Command & Control-Server (C&C-Server genannt oder auch C2-Server) mit einer G-10-Beschränkungsmaßnahme zu belegen.

Ein C&C-Server wird bei einem Cyberangriff von den Angreifern genutzt, um den eigentlichen Urheber zu verschleiern. Die von einem Opfer entwendeten Daten werden an einen solchen C&C-Server ausgeleitet. Über C&C-Server werden Kommandos und weitere Schadprogramme an infizierte Systeme geschickt. Die Angreifer kommunizieren in der Regel über weitere zwischengeschaltete C&C Server und nicht direkt mit den infizierten Systemen.

Ein entsprechender Überwachungsbedarf ergibt sich aus der fortschreitenden Vernetzung bei gleichzeitiger Zunahme der Zahl elektronischer Angriffe. In diesem Zusammenhang spielen C&C-Server eine bedeutende Rolle. Soweit nämlich ein Server als C&C-Server identifiziert worden ist, können mittels einer Überwachung des Servers ggf. andere potentielle Opfer frühzeitig identifiziert und gewarnt werden. Zudem können weitere genutzte IT-Infrastrukturen aufgeklärt werden. Hessen ist ein wichtiger Server-Standort und Knotenpunkt für IP-Adressen. Insofern ist ein solches Mittel auch mit Blick auf die tatsächliche Zuständigkeit des Landesamts von zentraler Bedeutung.

Dies verdeutlicht, dass die an den Verfassungsschutz gestellte Aufgabe der Internetaufklärung mit fortschreitender IT-Technik immer komplexer wird. Weitergehende Befugnisse werden in Abs. 1 nicht geschaffen.

Zu Abs. 2:

Neu eingeführt wird in § 6 Abs. 2 die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Hierbei handelt es sich um einen besonderen Fall der Telekommunikationsüberwachung, bei der in der Regel auf dem Zielsystem (Mobilfunkgerät oder Computer) ein Programm installiert wird, das die Kommunikation vor der Verschlüsselung mitschneidet und an die Ermittlungsbehörde ausleitet. Allerdings hat die Vorschrift lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und – ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems – eine laufende Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der herkömmlichen Überwachungstechnik nicht mehr möglich ist. Inhaltlich ist Abs. 2 an die Vorschrift des § 20l Abs. 2 BKAG (Überwachung der Telekommunikation) angelehnt, der vom Bundesverfassungsgericht für verfassungskonform erklärt wurde (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 228ff.).

Vor allem Täter des internationalen Terrorismus sind aufgrund ihrer häufig länderübergreifenden Vernetzung und ihres konspirativen Vorgehens darauf angewiesen, über Mobilfunkgeräte oder andere Kommunikationsmittel und -wege wie etwa das Internet zu kommunizieren. Dem Landesamt muss daher zur Erfüllung seiner Aufgaben nach § 2 die Möglichkeit eröffnet werden, die Telekommunikation einer betroffenen Person überwachen und aufzeichnen zu können, um anhand der damit gewonnen Erkenntnisse gegebenenfalls weitere Maßnahmen zu ergreifen (zu den Einzelheiten vgl. BT-Drs. 16/10121, S. 31f.). Für den Verfassungsschutz ist die Quellen-TKÜ gerade deshalb von großer Relevanz, weil diese eine Überwachung der immer häufiger verschlüsselt erfolgenden digitalen Kommunikation ermöglicht. Denn häufig läuft die Überwachung des Fernmeldeverkehrs deshalb „ins Leere“, weil die überwachten Nutzer gezielt verschlüsselte Kommunikationswege nutzen. Die Möglichkeit des Zugriffs auf informationstechnische Systeme schließt insoweit eine technisch-sicherheitskritische Lücke.

Zudem beinhalten Informationen, die über technische Mittel gewonnen werden, nicht die Problematik einer Mitarbeiter- bzw. Quellengefährdung.

Durch die Regelung der Quellen-TKÜ in § 6 Abs. 2 Satz 1 wird die Bestimmtheit der gesetzlichen Befugnisse erhöht und die Rechtssicherheit verbessert. Da die Befugnisnorm darauf abzielt, die technischen Voraussetzungen für die eigentliche Tele-

kommunikationsüberwachung zu schaffen, stehen die bundesgesetzlichen Regelungen des Artikel 10-Gesetzes einer landesgesetzlichen Regelung nicht entgegen.

Zu Abs. 3:

Satz 1 erklärt die in § 8 Abs. 2 für die Online-Datenerhebung geregelten technischen Sicherungspflichten sowie das G 10-Verfahren für entsprechend anwendbar. Durch letztes wird auch der Schutz des Kernbereichs privater Lebensführung (vgl. hierzu BVerfG, Urt. vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 236ff.) und von Berufsgeheimnisträgern sichergestellt.

Die Maßgabe in Satz 2 für § 3a Satz 12 des Artikel 10-Gesetzes orientiert sich an den Vorgaben des Bundesverfassungsgerichts (aaO., Rn. 246, 127ff.) und stellt sicher, dass eine Löschung der Dokumentation erst nach einer wirksamen Kontrolle erfolgt.

Die Maßgabe in Satz 3 für § 4 Abs. 1 Satz 5 des Artikel 10-Gesetzes berücksichtigt die Vorgabe des Bundesverfassungsgerichts, wonach die Frist der Aufbewahrung der Löschungsprotokolle so bemessen sein muss, dass sie auch im Rahmen der nächsten aufsichtlichen Kontrolle noch vorliegen (aaO., Rn. 272).

Zu Abs. 4:

Abs. 4 sieht eine umfassende Protokollierungspflicht vor und lehnt sich damit an die Vorgaben des Bundesverfassungsgerichts an (aaO., Rn. 267) an. Er ermöglicht, sachhaltig zu prüfen, wie und ob von der Erlaubnis zur Durchführung der Maßnahme Gebrauch gemacht wurde. Die Protokollierung soll vor allem nachweisen, dass die Daten tatsächlich vom betroffenen informationstechnischen System stammen und weder absichtlich noch unabsichtlich verändert worden sind.

Nach Satz 1 Nr. 1 ist das zur Datenerhebung eingesetzte technische Mittel zu protokollieren, nach Satz 1 Nr. 2 der Zeitpunkt seines Einsatzes. Erforderlich sind lediglich allgemein verständliche Angaben zum Funktionsumfang des Mittels.

Nach Satz 1 Nr. 3 sind die Angaben zu protokollieren, die die Feststellung der erhobenen Daten ermöglichen. Damit sind Metadaten gemeint, die zuverlässige Rückschlüsse auf die erhobenen Daten erlauben.

Die Protokollierung der Beteiligten der überwachten Telekommunikation nach Satz 1 Nr. 4 trägt dem Umstand Rechnung, dass ein Eingriff in Artikel 10 GG vorliegt und diesen Personen daher nach Abs. 3 Satz 1 in Verbindung mit § 12 des Artikel 10-Gesetzes regelmäßig die Maßnahme nach ihrer Einstellung mitzuteilen ist.

Satz 1 Nr. 5 enthält die Pflicht zur Protokollierung der Angaben zur Identifizierung des informationstechnischen Systems und der daran vorgenommenen nicht nur flüchtigen Veränderungen. Informationstechnische Systeme sind nicht durch ein einzelnes Merkmal zu identifizieren. Daher sind die Informationen über die Hard- und Software zu dokumentieren, die das betroffene System so exakt beschreiben, dass es keine ernstzunehmenden Zweifel daran geben kann, dass Gegenstand der Maßnahme tatsächlich das in der Anordnung (Abs. 3 Satz 1 in Verbindung mit § 10 Abs. 2 des Artikel 10-Gesetzes) bezeichnete System war. Flüchtige Veränderungen müssen dagegen nicht protokolliert werden, da jede aktive Software kontinuierlich diverse vorübergehende Veränderungen des informationstechnischen Systems vornimmt, die für die Revisionssicherheit irrelevant sind und häufig bereits nach kurzer Zeit automatisiert gelöscht werden.

Satz 2 begründet eine Protokollierungspflicht für die Gründe der Zurückstellung der Mitteilung nach § 12 Abs. 1 Satz 2 des Artikel 10-Gesetzes (vgl. aaO., Rn. 267).

Satz 3 normiert, dass eine Übermittlung der erhobenen Daten zu protokollieren ist. Auch damit wird die Rechtsprechung des Bundesverfassungsgerichts umgesetzt (vgl. BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 114; BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 322, 140 f.).

Satz 4 legt eine Zweckbindung der Protokolldaten nach Satz 1 bis 3 fest. Die Daten dürfen neben der Mitteilung nach § 12 des Artikel 10-Gesetzes nur verwendet werden, um der G 10-Kommission oder der betroffenen Person im Rahmen ihres Auskunftsanspruchs die Prüfung der rechtmäßigen Durchführung der Maßnahme zu ermöglichen. Die Regelung normiert kein neues Prüfungsrecht der betroffenen Person. Es bleibt bei den bisherigen Möglichkeiten des Rechtsschutzes.

Satz 5 verweist bezüglich der Löschungsfristen für die Protokolldaten nach Satz 1 bis 3 auf Abs. 3 Satz 3 in Verbindung mit § 4 Abs. 1 Satz 5 des Artikel 10-Gesetzes sowie auf § 4 Abs. 1 Satz 7 des Artikel 10-Gesetzes, da die Protokolldaten jeweils vergleichbaren Zwecken dienen.

Zu § 7 (Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung)

§ 7 überführt die bisher in § 5a enthaltene Befugnis zum Einsatz verdeckter technischer Mittel in Wohnungen in die neue Gesetzessystematik und folgt der Aufzählung der einzelnen Befugnisse zum Einsatz nachrichtendienstlicher Mittel in § 5 Abs. 2 Satz 2.

In Satz 1 werden die bisherigen Rechtfertigungstatbestände (u.a. Planung und Begehung von Katalogstraftaten) durch eine Aufzählung überragend wichtiger Rechtsgüter ersetzt, für deren dringende Gefährdung tatsächliche Anhaltspunkte vorliegen müssen, um eine verdeckte Wohnraumüberwachung durch technische Mittel zu rechtfertigen. Die Aufzählung der Rechtsgüter entspricht dem § 20h Abs. 1 BKAG, der vom Bundesverfassungsgericht im BKAG-Urteil für verfassungskonform erachtet wurde (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 182f.).

Die Regelungstechnik, im Rahmen einer präventiven Befugnisnorm auf einen Straftatenkatalog Bezug zu nehmen, erscheint im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts problematisch. Der Charakter der Gefahrenabwehr sei entscheidend durch den Rechtsgüterschutz geprägt, die Eingriffsschwelle sei vom Grad der Rechtsgütergefährdung abhängig zu machen (BVerfGE 125, 260 Rn. 230). Daher werden in Satz 1 die bisherigen Straftatenkataloge durch eine Aufzählung überragend wichtiger Rechtsgüter ersetzt.

Der Begriff der dringenden Gefahr entstammt Art. 13 Abs. 4 Satz 1 des Grundgesetzes. Nach der Rechtsprechung des Bundesverfassungsgerichts nimmt der Begriff der dringenden Gefahr nicht nur im Sinne des qualifizierten Rechtsgüterschutzes auf das Ausmaß, sondern auch auf die Wahrscheinlichkeit eines Schadens Bezug. Der Gesetzgeber ist von Verfassungs wegen aber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er – insbesondere im Kontext der Terrorismusbekämpfung – die Grenzen für bestimmte Bereiche mit dem Ziel der Straftatenverhütung auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 112, 184; BVerfGE 130, 1, 32; jeweils m.w.N.).

Vor dem Hintergrund dieses vom Bundesverfassungsgericht fortentwickelten sicherheitsrechtlichen Gefahrenabwehrmodells schafft § 7 Satz 1 die verfassungsrechtlich ausgewogene, zugleich aber auch hinreichend praktikable Rechtsgrundlage für jene Lebenssachverhalte, in denen sich ein zum Schaden führender Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Mit den flankierenden Verfahrensregelungen des § 9 schafft die Vorschrift nunmehr diejenige Eingriffsgrundlage, mit der einem schweren Missbrauch des Wohnungsgrundrechts für extremistisch-terroristische Bestrebungen und Aktivitäten adäquat begegnet werden kann. Eine Wohnraumüberwachung kann als ultima ratio etwa dann in Betracht kommen, wenn Privaträume für Missionierungs- bzw. Radikalisierungszwecke genutzt werden. Es entspricht dabei nachrichtendienstlichem Erfahrungswissen, dass entsprechende extremistische Bestrebungen insbesondere dann in den nicht-öffentlichen Raum wie etwa Privaträume und angemietete Hallen verlagert werden, wenn der sicherheitsbehördliche Verfolgungsdruck steigt. Ebenso kann eine Wohnraumüberwachung dann erforderlich werden, wenn vom Wohnungsgrundrecht des Art. 13 des Grundgesetzes geschützte Fahrzeuginnenräume als Vorbereitungssphäre für mögliche Terroranschläge bzw. als Aufbewahrungs- und Transportmedium für Tatmaterial genutzt werden.

Satz 2 erklärt u.a. die Kernbereichs- und Drittschutzbestimmungen des Artikel 10-Gesetzes für anwendbar, erhöht jedoch den Grundrechtsschutz dergestalt weiter, dass bei Zweifeln über die Verwertbarkeit gewonnener Erkenntnisse die richterliche Entscheidung einzuholen ist. § 3a des Artikel 10-Gesetzes ist mit der Maßgabe nach § 6 Abs. 3 Satz 2 anzuwenden (berücksichtigt BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a. Rn. 246, 127ff.).

Zu § 8 (Verdeckter Zugriff auf informationstechnische Systeme)

§ 8 ermächtigt das Landesamt zur sogenannten verdeckten Online-Datenerhebung. In Anbetracht der modernen Kommunikationswege einer weltweit vernetzten Informationsgesellschaft können entsprechende Eingriffe im Einzelfall notwendig werden, um durch verdeckten Zugriff auf informationstechnische Systeme schwerwiegende Gefahren für Rechtsgüter von Verfassungsrang abzuwehren. Im Sinne der Transparenz und zur Verdeutlichung der besonderen Eingriffstiefe findet sich die Regelung – wie auch die Wohnraumüberwachung – in einer gesonderten Befugnisnorm.

Das Bundesverfassungsgericht hat in seinem zu dieser Thematik ergangenen Urteil vom 27. Februar 2008 (BVerfGE 120, 274ff.) aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes) ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt, für das ähnlich hohe Eingriffsschwellen wie für die technische Wohnraumüberwachung gelten (vgl. auch BVerfGE 133, 277 Rn. 226). Demnach ist die verdeckte Überwachung der Nutzung eines informationstechnischen Systems verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen (BVerfGE 120, 274, 328ff.).

Wesentlicher Zweck der in § 8 geschaffenen zusätzlichen Befugnis ist die Abwehr von Gefahren des internationalen Terrorismus. Nach der Rechtsprechung des Bundesverfassungsgerichts manifestiert sich darin ein legitimes Ziel staatlicher Überwachungsmaßnahmen: „Straftaten mit dem Gepräge des Terrorismus in diesem Sinne zielen auf eine Destabilisierung des Ge-

meinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung von wirksamen Aufklärungsmitteln zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht“ (Urt. v. 20. April 2016 - 1 BvR 966/09).

In Anbetracht des mit § 8 nunmehr ermöglichten, mitunter tief in die Privatsphäre reichenden Eingriffs handelt es sich um eine Norm, die das Landesamt ausnahmsweise und einzelfallbezogen in den Stand setzen soll, schwerwiegende Gefahren für Rechtsgüter von Verfassungsrang abzuwehren und Straftaten von großem Gewicht zu verhindern. Diesen hohen verfassungsrechtlichen Anforderungen trägt das in § 8 und § 9 diesbezüglich geregelte Verfahren Rechnung.

Zunächst muss das Gesetz, das zu einem solchen Eingriff ermächtigt, den Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung stellen (BVerfGE 120, 274, 331ff.). Es hat weiterhin Vorkehrungen zu treffen, um den Kernbereich privater Lebensgestaltung zu schützen (BVerfGE 120, 274, 335ff.). Es bietet sich daher an, die Eingriffsvoraussetzungen für die Online-Datenerhebung parallel zur Wohnraumüberwachung auszugestalten. Daher enthält Abs. 1 eine Rechtsgrundverweisung auf die Befugnisnorm zum verdeckten Einsatz technischer Mittel im Schutzbereich des Wohnungsgrundrechts (§ 7). In Bezug genommen sind beide Sätze des § 7, so dass auch auf die verdeckte Online-Datenerhebung § 3 Abs. 2 und die §§ 3a und 3b des Artikel 10-Gesetzes mit der Maßgabe einer richterlichen Entscheidung in Zweifelsfällen entsprechende Anwendung finden.

Bezüglich dieser Parallelität der Eingriffsvoraussetzungen hat das Bundesverfassungsgericht im BKAG-Urteil darauf hingewiesen, dass der Gesetzgeber nicht gehindert sei, die maßgebliche Schwelle für den Rechtsgüterschutz von Wohnraumüberwachung und Online-Durchsuchung einheitlich zu bestimmen (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 108). Es hat demgemäß auch die weitestgehend inhaltsgleiche Aufzählung der Rechtsgüter in § 20k Abs. 1 Satz 1 BKAG als Rechtfertigung für Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für ausreichend erachtet (BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 212). Gegen den in § 9 neu vorgesehenen Gleichlauf von Wohnraum- und Online-Überwachung bestehen somit keine Bedenken.

Zu beachten ist, dass § 8 wie jede Befugnis zur Datenerhebung mit nachrichtendienstlichen Mitteln nicht nur tatsächliche Anhaltspunkte für eine dringende Gefährdung der genannten Rechtsgüter verlangt. Im Falle der Erhebung personenbezogener Daten müssen vielmehr stets auch die Voraussetzungen des § 5 Abs. 1 erfüllt sein.

Nr. 2 normiert die Befugnis zum Einsatz technischer Mittel zur Identifikation und Lokalisation von informationstechnischen Systemen. Diese Regelung ist angesichts der technischen Entwicklungen 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. Die Spezifizierung der informationstechnischen Systeme ist aber im Regelfall Voraussetzung für die Durchführung einer Maßnahme nach Satz 1. Aus dem Verhältnismäßigkeitsgrundsatz (§ 15) folgt im Übrigen, dass personenbezogene Daten Dritter bei Maßnahmen nach § 8 nur erhoben werden dürfen, soweit dies aus technischen Gründen unvermeidbar ist.

Abs. 2 enthält dem § 20k Abs. 2 BKAG entsprechende technische Sicherungspflichten zur Minimierung unbeabsichtigter Folgeschäden eines verdeckten Zugriffs auf ein informationstechnisches System (vgl. hierzu BVerfG, Urt. vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 215).

Nach Abs. 3 gelten die in § 6 Abs. 4 geregelten Protokollierungs- und Löschpflichten für die Online-Durchsuchung entsprechend.

Zu § 9 (Verfahren bei Maßnahmen nach den §§ 7 und 8)

Für die verdeckte Online-Datenerhebung gelten die Verfahrensvorschriften für die Wohnraumüberwachung. Ebenso wie die materiellen Voraussetzungen wird auch das Verfahren vollumfänglich parallel ausgestaltet.

Zu Abs. 1: Maßnahmen, die in den Schutzbereich des Wohnungsgrundrechts eingreifen, stehen ebenso wie Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme unter Richtervorbehalt. Dies wird in Satz 1 geregelt.

Der Richtervorbehalt nach Satz 1 gilt nach den § 21 Abs. 3 Satz 1, § 22 Abs. 3 Satz 1 und § 23 Abs. 2 Satz 1 auch für die Übermittlung der aus Maßnahmen nach den §§ 7 und 8 gewonnenen Informationen („doppelter Richtervorbehalt“).

Satz 2 übernimmt die nach Art. 13 Abs. 4 Satz 2 des Grundgesetzes zulässige Eilzuständigkeit der Behördenleitung (Präsidentin oder Präsident) und ihrer Vertretung bei Gefahr im Verzug.

Zu Abs. 2:

Satz 1 schreibt eine Befristung der Anordnung auf höchstens einen Monat vor. Zwar sind nach dem Wortlaut des Art. 13 Abs. 3 Satz 2 des Grundgesetzes nur repressive Maßnahmen der verdeckten akustischen Wohnraumüberwachung zu befristen (vgl. hierzu BVerfGE 109, 279/316). Eine entsprechende verfahrensrechtliche Beschränkung ist aber im Hinblick auf die hohe Schutzwürdigkeit der betroffenen Grundrechte und die Intensität des Eingriffs auch für die präventive technische Wohnraumüberwachung und die Online-Datenerhebung geboten.

Satz 2 erlaubt Verlängerungen um jeweils bis zu einem Monat, solange die Anordnungsvoraussetzungen fortbestehen.

Satz 3 verweist hinsichtlich der Prüf-, Kennzeichnungs- und Löschpflichten sowie des Verfahrens auf Vorschriften des Artikel 10-Gesetzes, die inhaltlich im Wesentlichen mit den Vorschriften des Gesetzes übereinstimmen. Im Einzelnen:

Nach § 4 Abs. 1 Satz 1 des Artikel 10-Gesetzes muss unverzüglich und sodann im Abstand von höchstens sechs Monaten die Erforderlichkeit der weiteren Speicherung erhobener personenbezogener Daten geprüft werden. Nicht mehr erforderliche Daten, die auch nicht mehr für eine Mitteilung an Betroffene oder für die gerichtliche Rechtmäßigkeitskontrolle benötigt werden, sind nach § 4 Abs. 1 Satz 2 bis 7 des Artikel 10-Gesetzes unter Aufsicht einer Juristin oder eines Juristen zu löschen; die Löschung ist zu protokollieren.§ 4 Abs. 1 Satz 5 des Artikel 10-Gesetzes ist nur nach Maßgabe des § 6 Abs. 3 Satz 3 anzuwenden.

§ 4 Abs. 2 des Artikel 10-Gesetzes enthält die Pflicht zur Kennzeichnung der verbleibenden Daten. Auf die Kennzeichnung darf nach § 4 Abs. 3 des Artikel 10-Gesetzes bei der Übermittlung der Daten ausnahmsweise verzichtet werden, wenn dies unerlässlich ist, um die Geheimhaltung einer Maßnahme nicht zu gefährden und die nach Landesrecht zuständige Stelle zugestimmt hat. Der Halbsatz 2 des Satzes 1 bestimmt für Daten aus Maßnahmen nach den §§ 7 und 8 die Richterin oder den Richter als für die Zustimmung zuständige Stelle, nachdem die durch die Maßnahmen betroffenen Grundrechte unter Richtervorbehalt stehen. Bei Gefahr im Verzug kann die Zustimmung nach Abs. 1 auch zunächst durch die Behördenleitung oder ihre Vertretung erfolgen; die richterliche Zustimmung muss unverzüglich nachgeholt werden. Die Möglichkeit einer derartigen Verfahrensweise wird von § 4 Abs. 3 Satz 2 und 3 des Artikel 10-Gesetzes eingeräumt.

In § 10 Abs. 2 und 3 des Artikel 10-Gesetzes wird für die Anordnung einer Maßnahme die Schriftform und der notwendige Inhalt (Anordnungsgrund, berechtigte Stelle, Art, Umfang, Dauer, Adressat und ggf. Kennung des Anschlusses bzw. Endgeräts) bestimmt. Der Kennung des Endgeräts entspricht bei der Online-Datenerhebung die Bezeichnung des informationstechnischen Systems, auf das zugegriffen werden soll.

§ 11 Abs. 1 des Artikel 10-Gesetzes schreibt für die Durchführung der Maßnahme vor, dass diese unter Verantwortung der Behörde, die deren Anordnung beantragt hat, unter Aufsicht eines Juristen zu erfolgen hat. In § 11 Abs. 2 des Artikel 10-Gesetzes wird die vorzeitige Beendigung von Maßnahmen angeordnet, wenn sie nicht mehr erforderlich sind oder ihre Anordnungsvoraussetzungen nicht mehr vorliegen. Die Beendigung ist der anordnenden Stelle (bei den §§ 7 und 8 also der Richterin oder dem Richter) anzuzeigen. Der weiter in § 11 Abs. 2 Satz 2 des Artikel 10-Gesetzes genannte Verpflichtete spielt bei Maßnahmen nach den §§ 7 und 8 keine Rolle. Schließlich enthält § 12 des Artikel 10-Gesetzes die Pflicht, den betroffenen Personen die durchgeführten Maßnahmen nach deren Einstellung mitzuteilen. In Bezug genommen werden nur die Abs. 1 und 3 des § 12 des Artikel 10-Gesetzes, da sich Abs. 2 auf strategische Beschränkungen des Bundesnachrichtendienstes bezieht und daher nicht auf Maßnahmen einer Landesverfassungsschutzbehörde anwendbar ist.

Nach § 12 Abs. 1 Satz 1 des Artikel 10-Gesetzes besteht die Benachrichtigungspflicht gegenüber dem „Betroffenen“. Bei Maßnahmen im Schutzbereich des Wohnungsgrundrechts (§ 7) ist als betroffene Person nicht nur der diejenige anzusehen, gegen die sich die Überwachungsmaßnahme richtet. Nach der Rechtsprechung des Bundesverfassungsgerichts sind daneben auch die Inhaberin oder der Inhaber und die Bewohner der Wohnung sowie solche Personen, die sich als Gast oder sonst zufällig in der überwachten Wohnung aufgehalten haben, in ihrem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes geschützten Recht am gesprochenen Wort und in ihrem informationellen Selbstbestimmungsrecht derart „betroffen“, dass ihnen gegenüber grundsätzlich eine Benachrichtigungspflicht besteht (BVerfGE 109, 279, 365).

Bei Maßnahmen nach § 8 sind „Betroffene“ die Besitzerin oder der Besitzer des überwachten informationstechnischen Systems und die Personen, deren Daten auf dem System gespeichert sind. Nach § 12 Abs. 1 Satz 2 des Artikel 10-Gesetzes unterbleibt die Mitteilung, solange eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann oder solange der Eintritt übergreifende Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

Zur Gewährleistung eines effektiven Grundrechtsschutzes müssen Entscheidungen über ein längeres Zurückstellen der Benachrichtigung an Betroffene von einer unabhängigen Stelle kontrolliert werden. § 12 Abs. 1 Satz 3 des Artikel 10-Gesetzes fordert dementsprechend für ein über zwölf Monate hinausgehendes Zurückstellen die Zustimmung der G 10-Kommision. Aufgrund des Richtervorbehalts der betroffenen Grundrechte ordnet der Halbsatz 2 des Satz 3 für Maßnahmen nach den §§ 7 und 8 die Zuständigkeit der Richterin oder des Richters an. Da die Maßnahmen nach den §§ 7 und 8 schon bei ihrer Anordnung einer richterlichen Prüfung unterliegen und die Gründe für ein Zurückstellen der Auskunft in der Regel langfristiger Natur sind, muss das Zurückstellen der Auskunft nicht schon nach kurzer Zeit richterlich überprüft werden.

Die Maßnahme selbst ist bereits beendet, so dass die Auskunft lediglich dazu dient, die nachträgliche gerichtliche Überprüfung der bereits richterlich – bei längeren Maßnahmen sogar mehrfach – geprüften Maßnahme zu ermöglichen. Zum effektiven Schutz der Grundrechte der betroffenen Person erscheint daher die für G 10-Maßnahmen geltende zwölfmonatige Frist angemessen.

Um sicherzustellen, dass das Zurückstellen auch im weiteren Verlauf auf das unbedingt Erforderliche begrenzt bleibt, bedarf es in Zeitabständen einer erneuten gerichtlichen Überprüfung (vgl. BVerfGE 109, 279/367). Daher hat die Richterin oder der Richter die Dauer des weiteren Zurückstellens zu bestimmen (§ 12 Abs. 1 Satz 4 des Artikel 10-Gesetzes i.V.m. § 9 Abs. 2 Satz 3 Halbsatz 2). Ausnahmsweise kann die Richterin oder der Richter schließlich auch das dauerhafte Unterbleiben der Mitteilung anordnen, wenn hierfür hinreichend gewichtige Gründe vorliegen (vgl. BVerfGE 109, 297, 365). Solche Gründe ergeben sich aus § 12 Abs. 1 Satz 5 des Artikel 10-Gesetzes.

Nach Satz 4 kann die Mitteilung 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 sein wird. Dadurch werden rein formale Prüfungen durch die Gerichte ohne Aussicht auf eine positive Entscheidung vermieden;

- der Grundrechtseingriff bei der Zielperson oder bei dem zu benachrichtigenden Beteiligten vertieft würde oder

- die Identitätsfeststellung bzw. die Ermittlung des Aufenthaltsortes nur unter unverhältnismäßigem Aufwand möglich ist.

Da die Gründe nach Satz 4 zu einem dauerhaften Unterbleiben der Mitteilung führen, muss über ihr Vorliegen nach Satz 3 Halbsatz 2 i.V.m. Abs. 1 grundsätzlich die Richterin oder der Richter befinden.

Zu Abs. 3:

Nach der Rechtsprechung des Bundesverfassungsgerichts unterliegen die von staatlichen Stellen erhobenen Daten einer Zweckbindung, die ihre weitere Verwendung begrenzt (vgl. BVerfGE 109, 279, 375ff.; 133, 277 Rn. 113f. m.w.N.). Zweckänderungen durch den Gesetzgeber sind zulässig, wenn diese durch Gemeinwohlbelange gerechtfertigt sind, die die grundrechtlich geschützten Interessen überwiegen. Dies hat insbesondere für die Übermittlung der Daten an andere öffentliche Stellen Bedeutung. Ausgeschlossen ist eine Zweckänderung dann, wenn mit ihr grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Ermittlungsmethoden umgangen werden, also die Informationen für den geänderten Zweck selbst auf entsprechender gesetzlicher Grundlage nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen. Abs. 3 trägt diesen verfassungsgerichtlichen Vorgaben Rechnung und gewährleistet die Zweckbindung der erhobenen Daten bei ihrer weiteren Verwendung.

In Nr. 1 bis 3 werden die materiellen Voraussetzungen für die Datenverwendung geregelt.

Nr. 1 beschränkt die weitere Verwendung der Daten zu Präventionszwecken auf die Abwehr von Gefahren im Sinne des § 7 Satz 1. Daten, die zur Abwehr einer Gefahr im Sinne des § 7 Satz 1 erhoben wurden, dürfen somit nur zur Abwehr von anderen Gefahren in diesem Sinne verwendet werden. In diesem Rahmen ist auch die Verwendung durch die Polizei zulässig.

Nr. 2 begrenzt die Datenverwendung im Übrigen. Da im neuen § 7 Satz 1 kein Straftatenkatalog mehr wie im bisherigen § 5a enthalten ist, wird auf den Katalog besonders schwerer Straftaten in § 100b Abs. 2 der Strafprozessordnung Bezug genommen.

Nr. 3 greift den vom Bundesverfassungsgericht im ATDG-Urteil postulierten Grundsatz der Vergleichbarkeit der Informationszusammenhänge (BVerfGE 133, 277, Rn. 114) auf und erlaubt eine Übermittlung der nach den §§ 7 und 8 erhobenen Daten zu repressiven Zwecken, wenn die Daten sowohl zum Zeitpunkt ihrer Erhebung als auch bei der Übermittlung nach den Vorschriften der Strafprozessordnung hätten erhoben werden dürfen.

Zu Abs. 4:

Nach Art. 13 Abs. 5 des Grundgesetzes gelten für eine Wohnraumüberwachung, die ausschließlich dem Schutz der bei einem Einsatz in Wohnungen tätigen Personen dient, abgeschwächte Voraussetzungen, da diese Personen selbst von den Vorgängen in der Wohnung Kenntnis erlangen. Eine entsprechende Regelung wird in Abs. 4 aufgenommen und im Hinblick auf die parallele Ausgestaltung der Eingriffsbefugnisse auch auf Maßnahmen nach § 8 erstreckt.

Satz 1 überträgt die Zuständigkeit für die Anordnung der Maßnahme auf die Behördenleitung und ihre Vertretung.

Satz 2 regelt die Zweckänderung von Daten, die aus Maßnahmen zum Mitarbeiterschutz gemäß Satz 1 gewonnen wurden. Eine nachträgliche Verwendung der Daten zu anderen Zwecken bedarf der richterlichen Genehmigung, bei der die Rechtmäßigkeit der ursprünglichen Maßnahmen ebenso geprüft wird wie der beabsichtigte Verwendungszweck der Daten. Bei Gefahr

im Verzug kann nach Halbsatz 2 die Zweckänderung ebenso wie die Maßnahme selbst zunächst durch die Behördenleitung oder ihre Vertretung erfolgen.

Satz 3 ordnet grundsätzlich die unverzügliche Löschung der nach Satz 1 gewonnenen Daten an, sofern nicht ausnahmsweise eine Zweckänderung nach Satz 2 erfolgt.

Zu Abs. 5:

Die präventive Wohnraumüberwachung nach Art. 13 Abs. 4 des Grundgesetzes steht im Gegensatz zur repressiven akustischen Überwachung (Art. 13 Abs. 3 Satz 3 des Grundgesetzes) nicht unter einem qualifizierten Richtervorbehalt (vgl. Papier in Maunz/Dürig, GG, 74. EL Mai 2015, Art. 13 Rn. 96). Aus der Rechtsprechung des Bundesverfassungsgerichts ergibt sich insoweit nichts anderes (BVerfGE 109, 279, 357f.).

Satz 1 weist dementsprechend Entscheidungen über die Anordnung und Verwertbarkeit von Daten, die aus Maßnahmen nach den §§ 7 oder 8 gewonnen wurden, der Einzelrichterin oder dem Einzelrichter am Amtsgericht zu (ebenso § 9 Abs. 2 Satz 3 bis 5 des Bundesverfassungsschutzgesetzes). Im Hinblick auf den im Gesetzentwurf angelegten Gleichlauf der Maßnahmen nach den §§ 7 und 8 soll künftig in beiden Fällen das Amtsgericht entscheiden.

Örtlich zuständig ist das Amtsgericht am Sitz des Landesamts. Nach Halbsatz 2 wird über Beschwerden von einem nicht mit der Hauptsache im Strafverfahren befassten Senat des Oberlandesgerichts (§ 120 Abs. 4 Satz 2 GVG) entschieden.

Satz 2 bestimmt wie § 9 Abs. 2 Satz 6 des Bundesverfassungsschutzgesetzes im Wege einer dynamischen Rechtsgrundverweisung das Gesetz über das Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) als maßgebliche Verfahrensordnung für richterliche Entscheidungen nach Satz 1. Danach ergeht die richterliche Anordnung schriftlich und ist zu unterschreiben (§ 51 Abs. 2 Satz 1 FamFG i.V.m. § 38 FamFG). Sie enthält die Angabe der betroffenen Person, gegen die sich die Maßnahme richtet (die Bezeichnung der Beteiligten, ihre gesetzlichen Vertreter und der Bevollmächtigten). Art, Umfang und Dauer der Maßnahme sind in § 9 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1 geregelt und Gegenstand der Anordnungsformel. Die Anordnung ist zu begründen.

Satz 2, 2. Halbsatz schließt im Interesse der Verfahrensbeschleunigung die Rechtsbeschwerde (§ 70 FamFG) aus.

Zu § 10 (Ortung von Mobilfunkendgeräten)

§ 10 (früher § 5 Abs. 2) regelt die Verwendung des sogenannten „IMSI-Catchers“. Dieser wird zur Ermittlung des Standorts von Mobilfunkgeräten oder zur Ermittlung der Geräte- und Kartennummern eingesetzt. Ein solcher IMSI-Catcher ermöglicht es, die auf der Chipkarte eines Mobilfunkgerätes gespeicherte Internationale Mobilfunk-Teilnehmerkennung (International Mobile Subscriber Identity, kurz IMSI) auszulesen und den Standort des aktiv geschalteten Mobilfunktelefons innerhalb einer Funkzelle näher zu bestimmen.

Wie das Bundesverfassungsgericht klargestellt hat, greift der Einsatz eines IMSI-Catchers nicht in das von Art. 10 des Grundgesetzes geschützte Telekommunikationsgeheimnis ein, weil mit Hilfe des IMSI-Catchers der Inhalt der Kommunikation nicht abgehört werden kann und sein Einsatz auch nicht im Zusammenhang mit einem Kommunikationsvorgang steht (BVerfG NJW 2007, 351, 353). Vielmehr dient der Einsatz des IMSI-Catchers neben der ungefähren Ortung erst der Vorbereitung von späteren G 10-Maßnahmen oder von Verkehrsdatenauskünften. Da Art. 10 des Grundgesetzes nicht eingreift, fallen die durch den IMSI-Catcher erhobenen technischen Kommunikationsdaten in den Schutzbereich des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes. Dementsprechend wird der Einsatz des IMSI-Catchers in einer gesonderten Befugnisnorm getrennt von Maßnahmen im Schutzbereich des Art. 10 des Grundgesetzes geregelt. Dessen Einsatz ist in Abs. 1 an hohe Voraussetzungen geknüpft und im Übrigen durch den Verhältnismäßigkeitsgrundsatz beschränkt.

Zu § 11 (Besondere Auskunftsersuchen)

§ 11 überführt die bisher in § 4a enthaltene Befugnis für besondere Auskunftsersuchen in die neue Gesetzessystematik und folgt der Aufzählung der einzelnen Befugnisse zum Einsatz nachrichtendienstlicher Mittel in § 5 Abs. 2.

Neu geschaffen wurde in Abs. 2 Satz 1 Nr. 1 die – beim Bundesamt für Verfassungsschutz ebenfalls bestehende – Befugnis, nun auch bei Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge Auskünfte zu Namen, Anschriften und zur Inanspruchnahme von Transportdienstleistungen und sonstigen Umständen des Luftverkehrs einzuholen. Zur Erfüllung des Normziels des § 11 Abs. 2 Satz 1 Nr. 1, durch frühzeitige und umfassend verfügbare Informationen über Reisewege, Ruhe- und Vorbereitungsräume, aber auch Zielgebiete internationaler terroristischer Gruppen oder andere Personen im Beobachtungsbereich des Verfassungsschutzes zu erschließen, besteht die Notwendigkeit, Auskunft auch bei Computerreservierungssystemen und den mit ihnen sehr eng verwandten Globalen Distributionssystemen einholen zu dürfen. Die in den Fachbereichen der Nachrichtendienste anfallenden Informationen zu Reisebewegungen sind nämlich in aller Regel lediglich fragmentarisch, so dass sich aus ihnen meist keine Rückschlüsse auf die benutzte Fluggesellschaft ergeben. Denn nur

wenn zu einer betroffenen Person weitergehende Hintergrundinformationen vorliegen, die eine Konkretisierung des Luftfahrtunternehmens zulassen, kann bislang ein Auskunftsersuchen an nur eine Fluggesellschaft gestellt werden.

Ein solcher Fall wäre denkbar, wenn z.B. der Wohnort oder die Aufenthaltsregion der betroffenen Person und die Tatsache, dass sie oder er über einen bestimmten Flughafen reisen wird, bekannt sind. Sollten darüber hinaus noch Hinweise auf das Reiseziel vorliegen, ließe sich z.B. auch der Kreis der für ein Auskunftsersuchen in Frage kommenden Fluggesellschaften einschränken, auch wenn hierzu vorab keine konkreteren Daten bekannt sind. Dies ist hingegen regelmäßig nicht der Fall. Während über Computerreservierungssysteme Reservierungen bearbeitet werden, sind Globale Distributionssysteme Datenbanken, in denen die entsprechenden Reservierungsdaten dann gespeichert werden. Der Zugriff auf ein Globales Distributionssystem erfordert regelmäßig den Zugang über ein Computerreservierungssystem. Bei den bedeutsamen Systemen werden beide Leistungen zugleich erbracht. Praktisch sämtliche Reisebüros, auch solche, die Buchungsmöglichkeiten im Internet anbieten, sind an eines der vier großen Systeme angeschlossen. Praktisch alle Fluggesellschaften, die Linienflüge anbieten und nicht nur im Low-Cost-Segment tätig sind, ermöglichen Buchungen über sämtliche bedeutsamen Computerreservierungssysteme, die für sie wichtige Vertriebskanäle darstellen. In den entsprechenden Systemen werden bei einer Buchung Datensätze vorgehalten, die ebenso wie die Datenbanken der Fluggesellschaften die Einzelheiten der Buchung enthalten. Durch automatische Synchronisationsverfahren wird sichergestellt, dass die Daten bei der Fluggesellschaft und beim jeweiligen Reservierungs- bzw. Distributionssystem auch bei Änderungen aktuell bleiben.

Der in Abs. 2 Nr. 1 ausdrücklich weit gefasste Begriff der Verkehrsunternehmen trägt den volatilen Bedingungen eines globalisierten Fernreisemarkts Rechnung, wonach sich binnen kurzer Zeiträume nicht nur Reisewege und Reisemittel, sondern auch die seitens der Reisedienstleister verwendeten Abwicklungsmethoden ändern können. Durch die Neuregelung erhält das Landesamt die Befugnis, künftig u.a. auch bei Fernbus- und Eisenbahntransportunternehmen Auskünfte einzuholen. Im Falle von Bestrebungen nach § 2 Abs. 2 Nr. 1 enthält § 11 Abs. 2 Satz die dahingehende Beschränkung, dass von diesen die in § 11 Abs. 2 Satz 2 Nr. 1 und 2 genannten schwerwiegenden Zweckrichtungen und Wirkungsweisen ausgehen müssen.

Die in Abs. 2 Nr. 2 genannte Befugnis zum Einholen von Auskünften gilt auch für Anfragen im Bereich der virtuellen Währungen (z. B. Bitcoin) sowie FinTech-Anbieter.

Die in § 4a Abs. 8 des bisherigen Gesetzes geregelte Berichtspflicht des für den Verfassungsschutz zuständigen Ministeriums wurde in den Entwurf eines neuen Gesetzes zur parlamentarischen Kontrolle des Verfassungsschutzes in Hessen überführt.

Abs. 8 erklärt für die Erteilung von Auskünften der Telemediendiensteanbieter, Verkehrsunternehmen, Kreditinstitute u.ä. die Nachrichtendienste-Übermittlungsverordnung (NDÜV) des Bundes für anwendbar.

Abs. 9 enthält ein Benachteiligungsverbot. Ein Auskunftsersuchen des Landesamts darf der betroffenen Person nicht zum Nachteil gereichen.

Zu § 12 (Ton- und Bildaufzeichnungen außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes)

Die Norm regelt – in Ergänzung zu § 6 – Ton- und Bildaufzeichnungen außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes. Die Befugnis war bisher in § 3 Abs. 2 geregelt und erfährt nun in ihren Tatbestandvoraussetzungen eine deutliche Ausgestaltung. Dies erleichtert die Normanwendung und unterstreicht den Grundrechtsschutz der Bürger.

Zu § 13 (Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter)

In enger Anlehnung an das Bundesverfassungsschutzgesetz (§§ 9a und 9b) wird der Einsatz von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern (§ 13) sowie Vertrauensleuten (§ 14) geregelt. Der Gesamtkontext der verdeckt eingesetzten Personen war auf gesetzlicher Ebene bislang nur abstrakt und unvollständig in § 3 Abs. 2 des bisherigen Gesetzes geregelt. Hier hat die Expertenkommission signifikanten Regelungsbedarf aufgezeigt, dies insbesondere im Hinblick auf die sog. Vertrauensleute („Quellen“). In Umsetzung der entsprechenden Handlungsempfehlungen (44-46.01, Abschlussbericht der Expertenkommission, S. 209, Rn. 469ff.) erfolgt nunmehr mit den §§ 13 und 14 erstmals eine differenzierte, eng an das Bundesverfassungsschutzgesetz angelehnte Regelung.

Zu Abs. 1:

Unter Vornahme einer Legaldefinition regelt Abs. 1 die Befugnis des Landesamts zum Einsatz eigener Mitarbeiterinnen und Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende. Die Rahmenbedingungen für deren Einsatz werden umfänglich gesetzlich geregelt. Abs. 1 übernimmt dabei weitestgehend den Wortlaut des § 9a Abs. 1 Satz 1 des Bundesverfassungsschutzgesetzes.

Im Unterschied zu dieser Bundesregelung stellt Abs. 1 jedoch nicht auf den Zweck der „Aufklärung von Bestrebungen“ ab, so dass auch Tätigkeiten i.S.v. § 2 mit Hilfe von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern beobachtet werden können. Damit können in Hessen Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter auch zur Aufklärung sicherheitsgefährdender und geheimdienstlicher Tätigkeiten i.S.v. § 2 Abs. 2 Nr. 2 eingesetzt werden.

Die Beschränkung des § 9a Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes wird auf Bundesebene mit einer stärkeren Fokussierung des Aufgabenbereichs auf gewaltbereite Bestrebungen und einer effizienten Ressourcensteuerung begründet (vgl. BT-Drs. 18/4654, S. 26). Im Rahmen der arbeitsteiligen Zusammenarbeit der Verfassungsschutzbehörden von Bund und Ländern hat dies zwangsläufig einen erweiterten Beobachtungsauftrag auf Seiten der Landesverfassungsschutzbehörden zur Folge, der auch nicht-gewaltorientierte Bestrebungen einbezieht. Nur so kann sichergestellt werden, dass verfassungsfeindliche Bestrebungen, die sich nicht auf die Ausübung von Gewalt und Terror, sondern auf das Ausnutzen demokratischer Strukturen stützen, indem sie z.B. unter dem Deckmantel einer nach Art. 21 des Grundgesetzes geschützten Partei agieren, frühzeitig erkannt und mit rechtsstaatlichen Mitteln bekämpft werden können. Auch Bestrebungen und Tätigkeiten der OK (§ 2 Abs. 2 Nr. 5) lassen sich – wie sich aus der Definition des § 3 Abs. 2 unmittelbar ergibt – keineswegs allein durch die Anwendung von Gewalt kennzeichnen.

Zu Abs. 2:

Die Befugnis zum Einsatz Verdeckter Mitarbeiterinnen und Verdeckter Mitarbeiter als nachrichtendienstliches Mittel wird durch Abs. 2 gesetzlichen Schranken unterworfen. Insoweit übernimmt der Gesetzentwurf die neu geschaffenen Vorschriften des Bundesverfassungsschutzgesetzes inhaltlich ohne Einschränkung.

Satz 1 verbietet eine steuernde Einflussnahme auf Bestrebungen i.S.v. § 2 Abs. 2. Dies gilt selbst dann, wenn die Einflussnahme mit dem Ziel erfolgt, die Bestrebungen abzuschwächen (vgl. BT-Drs. 18/4654, S. 26). Erst recht dürfen vom Landesamt solche Bestrebungen nicht initiiert werden, auch nicht zum Zwecke der Informationsgewinnung.

Satz 2 erlaubt daher inhaltlich übereinstimmend mit § 9a Abs. 2 Satz 2 des Bundesverfassungsschutzgesetzes – mit zur Verbesserung der Normklarheit geringfügig abgeändertem Wortlaut – nur den Einsatz von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern in bereits existenten Bestrebungen, die dem Beobachtungsauftrag unterfallen. Auch wenn die Bestrebung einem Vereinigungsverbot unterfällt, steht dies der Aufklärung der Vereinigung von Innen, durch Insider, nicht entgegen. Satz 2 regelt demnach einen strafrechtlichen Rechtfertigungsgrund für durch die Mitwirkung in oder Tätigkeit für eine solche Vereinigung verwirklichte Straftatbestände (insbesondere die §§ 84, 85, 129, 129a, 129b StGB und § 20 VereinsG).

Satz 3 enthält einen strafrechtlichen Rechtfertigungsgrund für bestimmte im Einsatz verwirklichte Straftaten. Durch den gegenüber § 9a Abs. 2 Satz 3 des Bundesverfassungsschutzgesetzes geringfügig anderen Wortlaut soll verdeutlicht werden, dass in Satz 2 nicht die Beteiligung an den Bestrebungen als solche gemeint ist. Vielmehr geht es um Handlungen, die eine Verdeckte Mitarbeiterin oder ein Verdeckter Mitarbeiter begeht, um hinreichendes Vertrauen zu gewinnen und um nicht enttarnt zu werden, was wiederum die Voraussetzung für den Zugang zu konspirativ ausgetauschten Informationen ist. In Satz 3 wird die Begehung strafbarer Handlungen daher in sehr engen Grenzen zugelassen.

Eine generalklauselartige Befugnis zu Begleiteingriffen in andere Grundrechte ergibt sich daraus nicht. Solche Begleiteingriffe gehören nicht zum planmäßigen Vorgehen des Landesamts bei der Durchführung von verdeckten Ermittlungen. Sonstige bestehende Befugnisse, insbesondere zur Datenerhebung mit anderen nachrichtendienstlichen Mitteln, bleiben unberührt.

Nr. 1 verbietet zunächst den Eingriff in Individualrechte. Mithin dürfen nur solche Straftatbestände verwirklicht werden, die ausschließlich Kollektivrechte bzw. öffentliche Interessen berühren (z.B. das Verwenden von Symbolen verfassungswidriger Organisationen gemäß § 86a StGB oder ein Verstoß gegen das versammlungsrechtliche Vermummungsverbot).

Nr. 2 beschränkt die Zulässigkeit der Handlungen weiter auf solche, die für die Durchführung des Aufklärungsauftrags erforderlich sind. Zulässig ist nur, was für die Akzeptanz im aufzuklärenden Umfeld unerlässlich ist. Derartige zugehörigkeitsstiftenden Verhaltensmuster sind subkulturell in den verschiedenen Phänomenbereichen sehr unterschiedlich ausgeprägt und entwicklungsoffen, so dass eine nähere Umschreibung oder katalogmäßige Auflistung durch den Gesetzgeber weder möglich noch sinnvoll ist. Stattdessen können nähere Festlegungen untergesetzlich in Dienstvorschriften getroffen werden. Da diese als Verschlusssachen eingestuft sind, besteht auch keine Gefahr, dass sie von Szeneangehörigen als Richtschnur verwendet werden, um einen vermuteten Einsatz einer Verdeckten Mitarbeiterin oder eines Verdeckten Mitarbeiters zu enttarnen (vgl. BT-Drs. 18/4654, S. 26).

Nr. 3 begrenzt die Erlaubnis zur Verwirklichung von szenetypischen Straftatbeständen ohne Schädigung Einzelner weiter durch den Verhältnismäßigkeitsgrundsatz. Die Handlungen dürfen nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen. Damit sind solche tatbestandsmäßigen Handlungen zulässig, die die Enttarnung der Verdeckten Mitarbeiterin oder des Verdeckten Mitarbeiters verhindern, da eine Aufdeckung seiner Tarnidentität die weitere Aufklärung und Informationsübermittlung vereiteln würde. Sollte die Enttarnung mit einer akuten Gefahr für Leib und Leben der Mitarbeiterin oder des Mitarbeiters verbunden sein, ist er allerdings nicht auf den von Satz 3 vorgegebenen Rahmen beschränkt, sondern kann wie jedermann von seinen durch das Strafrecht eingeräumten Rechten zu Notwehr- und Notstandshandlungen (§§ 32ff. StGB) Gebrauch machen. Der Verhältnismäßigkeitsgrundsatz beschränkt das Handlungsspektrum aber nicht auf Maßnahmen der Eigensicherung. Bezugspunkt der Verhältnismäßigkeitsprüfung ist die Bedeutung der aufzuklärenden Sache. Soll daher ein bedeutender Sachverhalt, etwa ein geplanter terroristischer Anschlag, aufgedeckt werden, dürfen Straftatbestände auch verwirklicht werden, um das Vertrauen der maßgeblichen Akteure und so Informationen zu den Details der Planung zu gewinnen.

Umgekehrt sind Handlungen, die weder dem Eigenschutz dienen noch der Aufklärung eines bedeutenden Sachverhalts, unverhältnismäßig und damit unzulässig.

Satz 4 enthält in Übereinstimmung mit dem Bundesrecht Ausnahmen von der Einsatzbeendigung und der Erstattung von Strafanzeigen. Bei Straftaten von erheblicher Bedeutung ist der Einsatz grundsätzlich abzubrechen (vgl. BT-Drs. 18/5415, S. 9f.). Der Wortlaut ist insoweit im Vergleich zur bundesgesetzlichen Regelung (dort „soll“) noch deutlicher formuliert.

Die Pflicht zum Abbruch des Einsatzes gilt nicht nur bei einem Einsatzverhalten, das die in Abs. 2 gezogenen Grenzen übersteigt, sondern für jedwedes Verhalten, auch wenn es nicht im Zusammenhang mit dem Einsatz steht (vgl. BT-Drs. 18/4654, S. 27).

Für die insoweit zu treffende Ermessensentscheidung liegt nach Satz 5 die Zuständigkeit bei der Behördenleitung oder ihrer Vertretung. Das Regel-/Ausnahme-Verhältnis zwischen Satz 4 und 5 gibt eindeutig zu erkennen, dass das in Satz 5 eingeräumte Ermessen bei der Entscheidung über die Fortsetzung des Einsatzes trotz einer Straftat von erheblicher Bedeutung und über Ausnahmen von der Unterrichtung der Strafverfolgungsbehörde bei Anzeigehindernissen restriktiv zu handhaben ist. Eine Ausnahme von der Information der Strafverfolgungsbehörde scheidet jedenfalls in den Fällen des § 21 Abs. 2 Satz 2 dieses Gesetzes aus, der auf § 20 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes Bezug nimmt und Staatsschutzdelikte im Zusammenhang mit der aufzuklärenden Bestrebung betrifft. Die Übermittlungsverbote nach § 24 sind angesichts der rechtsstaatlichen Sensitivität des Vorgangs restriktiv anzuwenden (vgl. auch BT-Drs. 18/4654, S. 27; 18/5415, S. 9f.).

Die Staatsanwaltschaft kann nach § 9a Abs. 3 des Bundesverfassungsschutzgesetzes, der nach seinem Satz 5 auch für die Landesbehörden für Verfassungsschutz gilt, unter den in § 9a Abs. 3 Satz 1 bis 4 des Bundesverfassungsschutzgesetzes näher geregelten Voraussetzungen von der Verfolgung von im Einsatz begangenen Vergehen absehen oder eine bereits erhobene Klage in jeder Lage des Verfahrens zurücknehmen und das Verfahren einstellen. § 9a Abs. 3 des Bundesverfassungsschutzgesetzes enthält somit eine bereichsspezifische Regelung einer Einstellungsbefugnis. Als Beispiel führt die Gesetzesbegründung den Fall von Sachbeschädigungen im Anschluss an Demonstrationen mit militantem Verlauf an, wenn sich die Quelle unter einem dynamischen Gruppendruck dem nicht entziehen kann (BT-Drs. 18/4654, S. 27). Die Einstellungstatbestände der §§ 153ff. der Strafprozessordnung bleiben unberührt.

Zu Abs. 3:

Die Einstellungsmöglichkeit nach § 9a Abs. 3 Satz 1 Nr. 1 des Bundesverfassungsschutzgesetzes besteht nur, wenn der Einsatz zur Aufklärung von Bestrebungen erfolgte, die auf Begehung einer Katalogstraftat gemäß § 3 Abs. 1 des Artikel 10-Gesetzes gerichtet sind.

Zu Abs. 4:

Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter sind nach der Legaldefinition des Abs. 1 dadurch gekennzeichnet, dass sie unter einer auf Dauer angelegten Legende eingesetzt werden. Daher können Mitarbeiterinnen und Mitarbeiter, die unter einer Tarnidentität im Internet tätig werden, nicht ohne Weiteres immer unter diesen Begriff subsumiert werden, da die Dauer einer solchen Tarnidentität sich nicht durch die gleiche Langfristigkeit auszeichnet wie bei Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern, die in der „realen“ Welt eingesetzt werden.

Der Bundesgesetzgeber ist bei der Regelung des § 9a des Bundesverfassungsschutzgesetzes davon ausgegangen, dass Mitarbeiter des Bundesamts für Verfassungsschutz, die zwar nicht offen, aber auch nicht unter einer Legende operieren, wie z.B. bei der Teilnahme an sozialen Netzwerken oder Internetforen mit „nickname“, nicht den Vorschriften über Verdeckte Mitarbeiter unterfallen, sondern nach den allgemeinen Regelungen nach § 8 Abs. 2 und § 9 Abs. 1 des Bundesverfassungsschutzgesetzes zum Einsatz kommen (BT-Drs. 18/4654, S. 26). Um für die zunehmend bedeutsame verdeckte Datenerhebung im Internet rechtliche Zweifel auszuschließen, werden – insbesondere im Interesse der als Internetauswerter tätigen Mitarbeiterinnen und Mitarbeiter – durch Abs. 4 Internetauswerter den Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern insoweit gleichgestellt, als die für Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter geltenden Vorschriften über den rechtlichen Befugnisrahmen nach Abs. 2 und die strafprozessualen Konsequenzen seiner Überschreitung nach § 9a Abs. 3 des Bundesverfassungsschutzgesetzes und Abs. 3 auf Internetauswerter entsprechende Anwendung finden, auch wenn ihre Legende nicht auf Dauer angelegt ist. Eine solche Gleichbehandlung ist sachlich durch die diesbezüglich vergleichbare Interessenlage gerechtfertigt. Auch Internetauswerter müssen, wenn sie in sozialen Netzwerken und einschlägigen Foren tätig werden, die dort üblichen szenetypischen Verhaltensweisen an den Tag legen, um nicht aufzufallen und das notwendige Vertrauen der übrigen Teilnehmer zu gewinnen.

Die vom Bundesgesetzgeber in § 9a Abs. 1 des Bundesverfassungsschutzgesetzes getroffene Legaldefinition steht einer solchen Regelung durch den Landesgesetzgeber nicht entgegen. Denn der Bundesgesetzgeber ging bei der Normierung des § 9a des Bundesverfassungsschutzgesetzes davon aus, dass es sich um eine beschränkende Regelung handelt, die nur für den auf Dauer angelegten Einsatz notwendig sei, nicht aber für eine vorübergehende verdeckte Informationsbeschaffung. Der Bundesgesetzgeber hat also Internetauswertern weitergehende Befugnisse zugestanden als Verdeckten Mitarbeiterinnen und Verdeck-

ten Mitarbeitern. Engere Vorgaben durch den Landesgesetzgeber sind daher möglich, ohne den bundesgesetzlich vorgegebenen Rahmen zu überschreiten.

Aufgrund der Vergleichbarkeit kommen für Internetauswerter die Rechtfertigungsgründe des Abs. 2 Satz 2 und 3 entsprechend zur Anwendung. Zugleich sind die bundesrechtlichen Regelungen zur Ermessenseinstellung im Strafverfahren nach § 9a Abs. 3 des Bundesverfassungsschutzgesetzes und Abs. 3 entsprechend anwendbar. Der Bundesgesetzgeber hat sich bewusst auf die Normierung des rechtlichen Rahmens für den Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten beschränkt, ohne damit eine abschließende Regelung der Informationsbeschaffung durch „menschliche Quellen“ zu erlassen. Insbesondere hat der Bundesgesetzgeber keine nähere Festlegung zu Internetauswertern getroffen. Er hat vielmehr über § 9a Abs. 3 Satz 5 des Bundesverfassungsschutzgesetzes die jeweils landesrechtlich vorgefundenen Begriffsabgrenzungen der „Verdeckten Mitarbeiter“ ausdrücklich anerkannt, weil „insoweit die gleichen Sachgründe für eine solche Regelung“ sprechen (BT-Drs. 18/4654, S. 27), und sich damit nicht nur offen für landesrechtliche Festlegungen gezeigt, sondern auch seinerseits analogienah argumentiert. Das aus Art. 103 Abs. 2 des Grundgesetzes abgeleitete strafrechtliche Analogieverbot gilt hinsichtlich strafprozessualer Einstellungen nicht. Die Interessenlage von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern und Internetauswertern ist insoweit vergleichbar.

Zu § 14 (Vertrauensleute)

Um interne Informationen über extremistische Bestrebungen, die ihrerseits ihre Ziele meist verdeckt verfolgen und deren Angehörige sich oftmals sehr konspirativ verhalten, zu erlangen, bleibt der planmäßige und systematische Einsatz von Vertrauensleuten ein unverzichtbares Mittel. In § 14 wird nun der Einsatzrahmen unter Übernahme der entsprechenden Vorschrift in § 9b des Bundesverfassungsschutzgesetzes gesetzlich festgelegt und damit eine weitere Empfehlung der Expertenkommission der Hessischen Landesregierung umgesetzt (Empfehlung 44-46-01, S. 210). Diese Transparenz soll die Akzeptanz des in der Öffentlichkeit kontrovers diskutierten Mittels der Informationsbeschaffung stärken. Die Informationsgewinnung durch Vertrauensleute richtet sich nach § 4 Abs. 1 Satz 1 i.V.m. § 5 Abs. 1.

Zu Abs. 1:

In Abs. 1 ist die grundsätzliche Befugnis des Landesamts zum Einsatz von Vertrauensleuten geregelt. Der Begriff wird gesetzlich definiert. Bei Vertrauensleuten handelt es sich in der Regel um Szeneangehörige, die sich aus unterschiedlichen Motiven zur Informationssammlung und Weitergabe an das Landesamt bereit erklären. Wesentliches Begriffsmerkmal ist die Auftragssteuerung durch das Landesamt und zwar hinsichtlich der Informationsbeschaffung. Nicht als Vertrauensleute zu qualifizieren sind daher Personen, die

- ohne Auftrag bzw. Einsatzführung lediglich in Einzelfällen oder gelegentlich Hinweise liefern (Informanten),

- das Landesamt anderweitig, etwa logistisch, unterstützen (Gewährspersonen) oder

- zur Spionageabwehr eingesetzt werden, einschließlich überworbene oder geworbene Mitarbeiter gegnerischer Nachrichtendienste (Countermen, Doppelagenten).

Hinsichtlich des Befugnisrahmens bei der Auftragssteuerung verweist Abs. 1 auf die für Verdeckte Mitarbeiter geltenden Regelungen in § 13. Somit ist die Führung von Vertrauensleuten nur in den Grenzen des § 13 Abs. 2 rechtmäßig. Umgekehrt wird ein Verhalten von Vertrauensleuten außerhalb des Auftragsrahmens von vornherein nicht von der Regelung gedeckt (vgl. BT-Drs. 18/4654, S. 28 zur entsprechenden Vorschrift in § 9b des Bundesverfassungsschutzgesetzes).

Zu Abs. 2:

Satz 1 behält die Entscheidung über die Verpflichtung von Vertrauensleuten der Behördenleitung und ihrer Vertretung vor. Dadurch wird verfahrensmäßig eine besondere Prüfung und zugleich auch ein einheitlich strenger Maßstab bei der Würdigung von Ausnahmesachverhalten gewährleistet.

Satz 4 enthält eine gesetzliche Regelung der Anforderungen an die Auswahl von Vertrauensleuten. Eine solche ist geboten, da es sich bei Vertrauensleuten im Unterschied zu Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern nicht um Beschäftigte handelt. Entsprechend den von der IMK in der Sitzung vom 22. bis 24. Mai 2013 beschlossenen gemeinsamen Standards und in Übereinstimmung mit § 9b Abs. 2 des Bundesverfassungsschutzgesetzes werden die in innerdienstlichen Vorschriften bereits umgesetzten persönlichen Ausschlusskriterien gesetzlich fixiert. Gründe für einen Ausschluss können sich aus entgegenstehenden Interessen und aus grundlegenden Risiken für die Verlässlichkeit der Informationsgewinnung ergeben.

Nr. 1 verbietet den Einsatz von Minderjährigen. Vertrauensleute müssen daher mindestens 18 Jahre alt sein und dürfen in ihrer Geschäftsfähigkeit keinen Einschränkungen unterliegen.

Nr. 2 soll verhindern, dass sich eine finanzielle Abhängigkeit nachteilig auf die Nachrichtenbeschaffung auswirkt. Die Vorschrift dient also der Verlässlichkeit der Informationsbeschaffung. Der persönliche Ausschlussgrund ist nicht einschlägig,

wenn im besonders begründeten Sonderfall Vertrauensleute legendengerecht eingesetzt werden und keine Aufklärungsalternative besteht. Hier ist der Sachverhalt nicht in der Person, sondern in der Legende angelegt (vgl. BT-Drs. 18/4654, S. 28).

Im Übrigen muss das Landesamt darauf bedacht sein, dass ausgezahlte Prämien möglichst nicht der aufzuklärenden Organisation zufließen. Wenn allerdings Beiträge, die von jedem Mitglied erwartet werden, aus solchen Zahlungen bestritten werden, erscheint dies hinnehmbar, solange die Vertrauensperson nicht von den Prämien des Landesamts abhängig ist.

Nr. 3 schließt ein Anwerben von Teilnehmern eines Aussteigerprogramms aus. Insoweit steht das vorrangige Interesse entgegen, die Teilnahmeschwelle niedrig zu halten und die Ausstiegsbereitschaft nicht zu gefährden.

Nr. 4 schützt die Unabhängigkeit von Parlamentsabgeordneten. Erfasst werden nicht nur Abgeordnete des Bundes oder eines Landes, sondern auch solche, die auf Ebene der Europäischen Union gewählt wurden. Der Schutz erstreckt sich auch auf die Mitarbeiter der Abgeordneten.

Nr. 5 enthält einen Ausschlussgrund wegen vorausgegangener Straftaten, die im Bundeszentralregister eingetragen sind. Die rechtskräftige Verurteilung wegen eines Verbrechens oder eine Verurteilung zu einer nicht zur Bewährung ausgesetzten Freiheitsstrafe lassen auf die mangelnde Eignung der betreffenden Person schließen. Laufende Strafverfahren sind hingegen nicht generell verpflichtungsschädlich. Vielmehr kommt es auf die Eignungsprüfung im Einzelfall an. Hierbei ist auch die Wertung des Satz 3 einzubeziehen. Je nach Verdachtsgrad und Tatschwere ist daher von einer Anwerbung abzusehen (vgl. BT-Drs. 18/4654, S. 28).

Satz 5 erlaubt in gewissen Grenzen Ausnahmen vom Ausschlussgrund nach Satz 4 Nr. 5. Die Vorschrift orientiert sich an den Wertungen des Strafprozessrechts. Die Strafprozessordnung lässt es selbstverständlich zu, dass auch Straftäter als Zeugen gehört werden. Es kann nicht generell davon ausgegangen werden, dass eine solche Person als Informationsquelle untauglich ist. Trägt eine Zeugin oder ein Zeuge mit ihrer oder seiner Aussage zur Aufklärung einer schweren Straftat i.S.v. § 100a Abs. 2 der Strafprozessordnung bei, kann dies nach § 46b StGB bei der Strafzumessung sogar zu ihren oder seinen Gunsten berücksichtigt werden. Ist eine solche Person darüber hinaus zu weiterer Informationsbeschaffung bereit, sollte die Zusammenarbeit daher nicht ausnahmslos gesetzlich untersagt werden (vgl. BT-Drs. 18/5415, S. 11).

In Anlehnung an den in § 46b StGB enthaltenen Verweis auf den Katalog schwerer Straftaten in § 100a der Strafprozessordnung enthält der Satz 5 für Ausnahmen vom Ausschlussgrund nach Satz 4 Nr. 5 eine qualifizierte Einsatzschwelle. Die Bestrebung, zu deren Aufklärung der Einsatz erfolgt, muss auf die Begehung von schweren Straftaten, die im Katalog des § 3 Abs. 1 des Artikel 10-Gesetzes enthalten sind, oder von besonders schweren Straftaten, die im Katalog des § 100b Abs. 2 der Strafprozessordnung genannt sind, gerichtet sein. Mit dem Verweis auf die in § 100b Abs. 2 der Strafprozessordnung genannten besonders schweren Straftaten geht der Satz 3 über die entsprechende Bundesregelung in § 9b Abs. 2 Satz 3 des Bundesverfassungsschutzgesetzes hinaus. Dies wird auch durch die dem Verfassungsschutz in Hessen obliegende Aufgabe gerechtfertigt, Bestrebungen und Tätigkeiten der OK zu beobachten (§ 2 Abs. 2 Nr. 5).

Auch wenn die Voraussetzung, dass der Einsatz der Aufklärung einer Katalogstraftat dienen muss, erfüllt ist, kommt es maßgeblich auf die konkreten Umstände an. In die Abwägung sind vor allem das Ausmaß der Bedrohung durch die zu beobachtende Bestrebung, der Stand der Resozialisierung und die Verfügbarkeit alternativer Informationszugänge einzubeziehen (vgl. BT-Drs. 18/4654 S. 28). Eine absolute Grenze gilt jedoch bei der Verurteilung als Täter eines Totschlags, Mordes oder einer anderen zwingend mit lebenslanger Freiheitsstrafe bedrohten Straftat. Solche durch die Rechtsordnung durch das Höchstmaß der Strafzumessung belegten Fälle schwerster Kriminalität (Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen nach § 6 Abs. 1, § 7 Abs. 1 Nr. 1 und 2 sowie § 8 Abs. 1 Nr. 1 Völkerstrafgesetzbuch) schließen in jeder denkbaren Fallkonstellation die Anwerbung als Vertrauensleute aus. Entsprechendes gilt für den Totschlag, der als Verbrechen gegen das Leben ein absolutes Tabu bricht. Das Anwerbeverbot gilt dabei sowohl während des Haftvollzugs als auch für die Zeit nach dem Freiheitsentzug (Aussetzung der Vollstreckung des Strafrests nach § 57a StGB bzw. im Falle des versuchten Delikts oder eines heranwachsenden Täters angesichts der Strafrahmenverschiebung nach § 23 Abs. 2 bzw. § 106 Abs. 1 des Jugendgerichtsgesetzes auch nach § 57 StGB, Jugendstrafe gemäß den §§ 18, 105 Abs. 3 des Jugendgerichtsgesetzes).

Als zusätzliche Verfahrensvorkehrung sieht Satz 5 die Entscheidung über Ausnahmen der Behördenleitung und ihrer Vertretung vor. Eine Delegation ist insoweit ausgeschlossen, zulässig bleibt aber die Abwesenheitsvertretung.

Satz 5 stellt klar, dass eine grundsätzlich nach Satz 4 Nr. 5 ausgeschlossene Anwerbung nur dann in Betracht kommt, wenn zu erwarten ist, dass die Informationen der Quelle von derartiger Qualität sind, dass das Aufklärungsinteresse das grundsätzliche Anwerbeverbot überwiegt. Neben die abstrakt-phänomenbezogene Bewertung („Bestrebungen, die auf die Begehung von in § 3 Abs. 1 des Artikel 10-Gesetzes oder § 100b der Strafprozessordnung bezeichneten Straftaten gerichtet sind“) muss dabei auch eine konkret quellenbezogene Einschätzung treten (vgl. BT-Drs. 18/5415, S. 11).

Als weitere verfahrenstechnische Sicherung schreibt Satz 6 vor, dass nach spätestens sechs Monaten die Ausnahmeentscheidung anhand des Werts der erlangten Informationen zu überprüfen ist. Wenn sich die Erwartung, die Vertrauensperson werde wichtige Information zur Aufklärung der Bestrebung liefern, nicht bestätigt, ist der Einsatz zu beenden.

Satz 7 stellt klar, dass unabhängig von der Prüffrist nach Satz 6 Wert und Wahrheitsgehalt der gelieferten Informationen fortlaufend zu prüfen sind. Dies entspricht den bereits derzeit gültigen, untergesetzlich fixierten Qualitätsstandards zur Führung von Vertrauensleuten und wird durch die gesetzliche Verankerung unterstrichen. So wird betont, dass gerade wegen der besonderen Sensibilität gravierender Vorstrafen eine laufende Überprüfung der Angemessenheit der Einsatzfortsetzung angezeigt ist (vgl. BT-Drs. 18/5415, S. 11).

Zu § 15 (Verhältnismäßigkeit)

§ 15 regelt den zuvor für die jeweiligen Arten der Informationserhebung getrennt formulierten Verhältnismäßigkeitsgrundsatz in nun einem eigenen Paragraphen. Dies erleichtert die Gesetzanwendung, verdeutlicht den Stellenwert verhältnismäßigen Handelns ausdrücklich auch beim Einsatz nachrichtendienstlicher Mittel durch den Verfassungsschutz und erhöht die Transparenz für die Bürgerinnen und Bürger.

Sämtliche Befugnisse des Landesamts sind durch den allgemeinen Verfassungsgrundsatz der Verhältnismäßigkeit begrenzt. Dieser wird bislang in § 5 Abs. 3 Satz 1 bis 3 allgemein geregelt und teilweise in den besonderen Befugnisnormen ohne eigenständigen Regelungsgehalt wiederholt. Die zentrale Bedeutung des Verhältnismäßigkeitsgrundsatzes soll dadurch betont werden, dass er parallel zur Regelung in § 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) als allgemeiner Grundsatz im Schlussparagraphen des Zweiten Teils zu den Befugnissen des Verfassungsschutzes normiert wird.

Die Verankerung als zentrale allgemeine Bestimmung bedeutet, dass der Verhältnismäßigkeitsgrundsatz bei allen Maßnahmen, seien sie allein auf die allgemeine Befugnis des § 4 oder in Verbindung mit den §§ 5ff. auch auf die besonderen Befugnisse gestützt, zu beachten ist. Dies erlaubt es im Gegenzug, auf Wiederholungen in diesen Vorschriften zu verzichten.

Zu Abs. 1:

Abs. 1 bringt den sogenannten Grundsatz der Erforderlichkeit zum Ausdruck. Danach verlangt der Grundsatz der Verhältnismäßigkeit zunächst, dass nur das Notwendige zum Schutz eines von der Verfassung anerkannten Rechtsgutes im Gesetz vorgesehen und im Einzelfall angeordnet werden darf (vgl. BVerfGE 7, 377, 397ff.; 30, 1, 20).

Zu Abs. 2:

Nach dem in Abs. 2 beschriebenen Grundsatz der Angemessenheit oder Verhältnismäßigkeit im engeren Sinne darf die Schwere des Eingriffs bei einer Gesamtabwägung auch nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen (vgl. BVerfGE 134, 141 Rn. 119 m.w.N.).

Zu Abs. 3:

Erweist sich schließlich, dass eine Maßnahme nicht mehr notwendig ist, gebietet es der Grundsatz der Erforderlichkeit in zeitlicher Hinsicht, die Beobachtung umgehend zu beenden (vgl. BVerfGE 113, 63, 84). Insoweit kann es der Verhältnismäßigkeitsgrundsatz im Einzelfall gebieten, Maßnahmen schon bei ihrer Anordnung aufgrund einer Prognose über die mutmaßliche Dauer ihrer Erforderlichkeit zu befristen, wobei die Befristung, sollte die Prognose sich im Nachhinein als unzutreffend erweisen, erforderlichenfalls verlängert werden kann.

Zum Dritten Teil (Speicherung, Sperrung, Löschung und Übermittlung personenbezogener Daten)

Zu § 16 (Geltung des Hessischen Datenschutzgesetzes)

Die Klarstellung der grundsätzlichen Geltung des Hessischen Datenschutzgesetzes zu Beginn des Dritten Teils (Speicherung, Sperrung, Löschung und Übermittlung personenbezogener Daten) unterstreicht die besondere Sorgfalt, mit der der Verfassungsschutz die erhobenen Daten behandeln muss.

Zu § 17 (Speicherung, Sperrung und Löschung)

Zu Abs. 1:

Abs. 1 harmonisiert die Vorschriften der Speichervoraussetzungen mit denen des Bundes (§ 10 Abs. 1 und 2 des Bundesverfassungsschutzgesetzes). Dies erleichtert die Zusammenarbeit und ermöglicht einen Gleichlauf der Speicherung von Daten in gemeinsamen Systemen und Dateien. In der bisherigen Fassung sind die gesetzlichen Regelungen im Bund und in Hessen unterschiedlich gefasst.

§ 6 Abs. 2 des Bundesverfassungsschutzgesetzes enthält die Rechtsgrundlage für die gemeinsame Datenbank der Verfassungsschutzbehörden („NADIS“). § 6 Abs. 2 Satz 2 verweist auf die §§ 10 und 11 des Bundesverfassungsschutzgesetzes. In § 10 Abs. 1 und 2 des Bundesverfassungsschutzgesetzes sind die Speichervoraussetzungen geregelt.

Zu Abs. 3:

Bisher war die Datenspeicherung über eine Person unter 14 Jahren nur in zu ihrer Person geführten Akten zulässig. Ein Mindestalter von 14 Jahren für die Speicherung in Dateien wird jedoch der Wirklichkeit kaum noch gerecht und erschwert den Austausch im NADIS-Verbundsystem. Dies hat beispielsweise der gescheiterte Terroranschlag eines Zwölfjährigen auf den Ludwigshafener Weihnachtsmarkt am 26. November 2016 gezeigt. Wenn tatsächliche Anhaltspunkte für eine der in Abs. 3 bezeichneten Straftaten bestehen, soll deshalb auch in Dateien eine Datenspeicherung von unter 14-Jährigen möglich sein.

Zu Abs. 6:

Die IMK hat bereits in ihren Herbstsitzungen 2011 und 2012 gefordert, die Speicherfristen für personenbezogene Daten gewaltbereiter extremistischer Bestrebungen auf fünfzehn Jahre zu erhöhen. Derzeit sind personenbezogene Daten über Bestrebungen nach § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, der Behördenleiter oder sein Vertreter trifft im Einzelfall ausnahmsweise eine andere Entscheidung. In Hessen gilt wie in einigen anderen Bundesländern die Zehn-Jahres-Löschfrist nur für personenbezogene Daten über Bestrebungen, die u.a. gegen die freiheitliche demokratische Grundordnung gerichtet sind (§ 2 Abs. 2 Nr. 1). Bei Bestrebungen, die durch Anwendung von Gewalt auswärtige Belange der Bundesrepublik gefährden (§ 2 Abs. 2 Nr. 3) und bei Bestrebungen und Tätigkeiten der OK (§ 2 Abs. 2 Nr. 5) gilt eine Fünfzehn-Jahres-Löschfrist. Diese Fünfzehn-Jahres-Löschfrist gilt wiederum nicht für Bestrebungen, die sich gegen den Gedanken der Völkerverständigung u.a. richten (§ 2 Abs. 2 Nr. 4). Ein sachlicher Grund für diese Differenzierung ist nicht ersichtlich, weshalb mit § 14 Abs. 6 jetzt eine einheitliche, späteste Löschverpflichtung nach 15 Jahren festgeschrieben wird. Gruppierungen (so die Erfahrung aus den Taten des NSU) können durchaus längere Zeit im Untergrund sein, weshalb die Erkenntnisse über Personen, die bestimmten Gruppierungen zugeordnet werden können, für die Arbeit der Sicherheitsbehörden länger benötigt werden. Die einheitliche Frist erleichtert zudem die Normanwendung durch die Sachbearbeiter im Landesamt. Dies und die normklare Zusammenführung von Lösch- und Sperrfristen aus den §§ 6 und 19 a.F. stellt den erforderlichen Ausgleich zwischen dem rechtsstaatlichen Grundsatz der Aktenklarheit und Aktenwahrheit einerseits, dem grundrechtlich gebotenen Datenschutz andererseits dar.

Zu Abs. 7:

Sperren bedeutet, gespeicherte personenbezogene Daten zu kennzeichnen, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

Zu Abs. 10:

Die Informationsbeschaffung durch das Landesamt erfolgt in erster Linie und vorrangig durch Auswertung offen zugänglicher Quellen. Daneben ist das Landesamt aber zwingend auf den Einsatz nachrichtendienstlicher Mittel und insbesondere von verdeckt eingesetzten Personen angewiesen. Nur so lassen sich in Zukunft und bei stark abgeschotteten Personenkreisen frühzeitig Erkenntnisse über extremistische Bestrebungen gewinnen. Werbung und Führung von verdeckt eingesetzten Personen werden in Hessen in einer Dienstvorschrift geregelt. Bei Einsätzen von verdeckt eingesetzten Personen des Bundesamts und anderer Länder sind mit Blick auf länderübergreifende oder bundesweit agierende und zu beobachtende Personenzusammenschlüsse und Einzelpersonen ein enger Informations- und Erkenntnisaustausch und eine Abstimmung notwendig. Die IMK hat bereits in ihrer Herbstsitzung 2012 beschlossen, im Bundesamt für Verfassungsschutz eine zentrale „V-Leute-Datei“ aufzubauen, damit dort Kenntnisse über Grund- und Strukturdaten und den Einsatzbereich der verdeckt eingesetzten Personen vorhanden sind. Die Landesbehörden sollen die notwendigen Daten verschlüsselt und nach bestimmten Kriterien berichten. § 14 Abs. 10 unterstreicht die Notwendigkeit einer solchen Datei durch eine landesseitige Ermächtigung und verpflichtet die Sicherheitsbehörden im Land zum koordinierten Vorgehen beim Einsatz nachrichtendienstlicher Mittel, auch um Doppeleinsätze von verdeckt eingesetzten Personen in von beiden Behörden beobachteten Organisationen zu vermeiden.

Zu § 18 (Zweckbindung)

§ 18 entspricht dem bisherigen § 7. Die Aufsichts- und Kontrollbefugnisse umfassen die Dienst-, Rechts- und Fachaufsicht des für den Verfassungsschutz zuständigen Ministeriums und die Kontrolle durch die Parlamentarische Kontrollkommission.

Inhaltlich gestrichen wurde die Verwendungsmöglichkeit personenbezogener Daten zu Ausbildungs- und Prüfungszwecken. Personenbezogene Daten, die durch das Landesamt erhoben wurden, unterliegen aufgrund der besonderen Aufgaben eines Nachrichtendiensts erhöhter Sensibilität.

Zu § 19 (Informationsübermittlung durch öffentliche Stellen an das Landesamt)

Die wesentliche Änderung von § 19 Abs. 1 besteht darin, dass die dort aufgezählten Behörden und sonstigen öffentlichen Stellen des Landes nunmehr generell zur Informations- und Datenübermittlung verpflichtet sind, wenn tatsächliche Anhaltpunkte dafür bestehen, dass die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist.

Bisher enthielt § 8 Abs. 1 eine sogenannte „Kann-Regelung“: Die angesprochenen Behörden durften Informationen übermitteln, sie mussten es aber nicht. Etwas Anderes galt bisher nach § 8 Abs. 2 Satz 3 nur für die Polizeibehörden und wiederum eingeschränkt die Staatsanwaltschaften mit einer Verpflichtung zur Übermittlung von Anklageschriften und Urteilen.

Für diese inhaltliche Beschränkung der Übermittlungspflichten gibt es keinen zwingenden Grund. Das zeigt auch der Bund-Länder-Vergleich: Art. 12 und 13 des Bayerischen Verfassungsschutzgesetzes und § 9 des Landesverfassungsschutzgesetzes Baden-Württemberg kennen zum Beispiel keine Unterscheidung von „Darf-“, „Kann-“ und „Muss-Regelungen“, die Übermittlung von verfassungsschutzrelevanten Daten ist für alle Stellen verbindlich. Im Bund und in einigen anderen Ländern ist die Rechtslage dagegen differenziert. Dort trifft alle Behörden eine Übermittlungspflicht bei Erkenntnissen über Bestrebungen, die durch Anwendung von Gewalt oder dahingehende Vorbereitungshandlungen gegen verfassungsschutzrelevante Schutzgüter gerichtet sind. Bei allen anderen, im Rahmen der eigenen Aufgabenerfüllung bekannt gewordenen Informationen gilt die Übermittlungspflicht nur für Staatsanwaltschaften und Polizeidienststellen, die übrigen Behörden können in diesen Fällen die Übermittlung vornehmen. Der bundesweite Vergleich der Übermittlungsvorschriften zeigt, dass Einschränkungen nicht nur zu Lasten der Verständlichkeit und Praktikabilität der Regelungen gehen, sondern der inzwischen als notwendig erkannten, möglichst weitgehenden und engeren Zusammenarbeit der Behörden im Sicherheitsbereich entgegenstehen.

Nach der Formulierung „auch ohne vorheriges Ersuchen“ bleibt es dem Landesamt unbenommen, um Übermittlung der entsprechenden Informationen zu ersuchen. Diese Befugnis ist notwendig, weil andere Behörden nicht immer die Bedeutung ihrer Informationen für den Verfassungsschutz erkennen können.

Ferner wird im neuen § 19 Abs. 1 die Aufzählung der übermittlungspflichtigen Stellen zusammengefasst. Staatsanwaltschaften und Polizeibehörden sind Behörden im Sinne von § 19 Abs. 1 Satz 1. Zu den Gerichten hinsichtlich ihrer Register zählen z. B. das Vereins-, Handels-, Genossenschafts-, Güterrechts- und Partnerschaftsregister.

Zu § 20 (Informationsübermittlung durch das Landesamt an übergeordnete Behörden)

Das Aufklären der Öffentlichkeit über verfassungsfeindliche Bestrebungen gehört zum Kernauftrag des Landesamts. § 20 Abs. 2 setzt unter Einbeziehung des Landesamts den für die Übermittlung von personenbezogenen Daten notwendigen datenschutzrechtlichen Rahmen.

Zu § 21 (Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs)

Unter ausdrücklichem Benennen des Informationswegs – vom Landesamt an die jeweilige inländische öffentliche Stelle – strukturiert § 21 die Übermittlungsbefugnisse und -pflichten des Landesamts neu. Während zuvor eine Aufteilung in zwei Vorschriften erfolgte (ex-§ 10 für Übermittlungen an die Strafverfolgungsbehörden in Staatsschutzangelegenheiten und ex-§ 11 für Übermittlungen innerhalb des öffentlichen Bereichs), wird nun die Übermittlung für den gesamten öffentlichen Sektor einheitlich geregelt. Die Neufassung des § 21 greift damit die Empfehlungen im Abschlussbericht der BLKR (dort insb. Rn. 798 f.) und die Handlungsempfehlungen der Expertenkommission der Hessischen Landesregierung auf (insbes. Empfehlung 4.03). Die BLKR wie auch die Expertenkommission hatten zur Verbesserung des Informationsaustauschs empfohlen, die Übermittlungsvorschriften in Bund und Ländern zu vereinheitlichen, so dass alle Sicherheitsbehörden auf Bundes- und Landesebene von einem einheitlichen Rechtsstandard ausgehen können.

Weiterhin werden in § 21 die Vorgaben, die sich aus dem ATDG-Urteil (BVerfGE 133, 277ff.) für eine Informationsübermittlung von Nachrichtendiensten an Sicherheits- und Strafverfolgungsbehörden ergeben, umgesetzt. Die Regelung orientiert sich an der Neufassung des § 19 des Bundesverfassungsschutzgesetzes und tritt an die Stelle der §§ 10 und 11 des bisherigen Gesetzes. Dass jeder Übermittlungsvorgang aktenkundig zu machen ist, ergibt sich bereits aus dem allgemeinen Grundsatz förmlicher Vorgangsbearbeitung und bedarf daher keiner fachgesetzlichen Spezialregelung.

Zu Abs. 1:

Als allgemeine Vorschrift verleiht Abs. 1 dem Landesamt die Befugnis, in den enumerativ aufgeführten Fällen Daten an inländische öffentliche Stellen zu übermitteln. Die Regelung gilt grundsätzlich auch, wenn die Informationen mit nachrichtendienstlichen Mitteln erhoben wurden. Nur für die Übermittlung solcher Informationen an Behörden, die polizeiliche Exekutivbefugnisse ausüben, gilt die Sondervorschrift des Abs. 2. Daraus folgt im Umkehrschluss, dass Informationen, die nicht mit nachrichtendienstlichen Mitteln erhoben wurden, auch an Polizei- und Strafverfolgungsbehörden unter den Voraussetzungen des Abs. 1 übermittelt werden dürfen.

Während Nr. 1 sowohl für Spontan- als auch für Ersuchensübermittlungen gilt, regelt Nr. 2 die Befugnisse und das Verfahren für die Beantwortung von Übermittlungsersuchen in Mitwirkungsangelegenheiten.

Nr. 1 übernimmt die Regelung aus § 10 Satz 1 Alt. 2 des bisherigen Gesetzes (entspricht im Wesentlichen § 19 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes). Danach sind Übermittlungen zum Zwecke der öffentlichen Sicherheit oder der Strafverfolgung zulässig. Das beispielhaft genannte Schutzgut der freiheitlichen demokratischen Grundordnung und die weiter angeführte Strafverfolgung, an der ein herausragendes öffentliches Interesse besteht, machen bereits deutlich, dass nur hinrei-

chend gewichtige Zwecke der öffentlichen Sicherheit eine Informationsübermittlung zulassen und Bagatellsachverhalte nicht ausreichen. Dies ergibt sich auch unmittelbar aus dem Grundsatz der Verhältnismäßigkeit (§ 15). Eine nochmalige gesetzliche Regelung ist daher nicht erforderlich.

Nr. 2 regelt die Übermittlungsbefugnis im Rahmen der sogenannten Mitwirkungsaufgaben. Diese sind bislang in § 2 Abs. 5 des bisherigen Gesetzes geregelt, werden nun aber systematisch richtig in den Kontext der Übermittlungsbefugnisse überführt. Dies ist maßgeblich dem Umstand geschuldet, dass es sich hierbei regelmäßig um eine Weitergabe von im Landesamt bereits vorhandener Daten handelt. Eine Befugnis zur weitergehenden Datenerhebung mit nachrichtendienstlichen Mitteln resultiert daraus nicht (vgl. oben die Einzelbegründung zu § 2 Abs. 3 und § 4 Abs. 3 und 5). Mitwirkungsaufgaben sind dadurch gekennzeichnet, dass der Empfänger Aufgaben wahrnimmt, die auch dem Schutz der freiheitlichen demokratischen Grundordnung, der öffentlichen Sicherheit oder auswärtiger Belange dienen und dabei auf eine Übermittlung des Verfassungsschutzes angewiesen ist.

Solche Übermittlungen können einzelfallabhängig aus umfangreichen Erkenntniszusammenstellungen, unbewerteten Informationen oder aus bloßen, ohne Begründung erfolgenden Empfehlungen bestehen.

In der Nr. 2 geht damit § 11 Abs. 1 Nr. 4 des bisherigen Gesetzes auf. § 21 Abs. 1 Nr. 2 Buchst. a bis m regelt die Mitwirkung des Landesamts an verschiedenen, im Einzelnen benannten Sicherheitsüberprüfungs- und Zuverlässigkeitsüberprüfungsverfahren. Hierbei ist zu betonen, dass eine Vielzahl bedeutsamer Aufgaben im Kontext staatlicher und nichtstaatlicher Veranstaltungen und Einrichtungen nur durch entsprechend überprüftes Personal zu bewältigen ist. Nicht nur der zurückliegende Zustrom von Flüchtlingen nach Deutschland und Hessen, sondern auch diverse Großveranstaltungen haben dies verdeutlicht. Daher kann es erforderlich sein, dass die hessischen Sicherheitsbehörden – mithin auch der Verfassungsschutz – solche Beschäftigte auf ihre Zuverlässigkeit überprüfen, die mit besonderen Aufgaben betraut werden sollen.

Das Landesamt soll künftig kraft der in § 2 Abs. 3 i.V.m. § 21 Abs. 1 Nr. 2 angelegten Konnex-Aufgabe bei derartigen Überprüfungen mitwirken und so unter anderem dazu beitragen, dass keine Extremisten im räumlichen bzw. fachlichen Zusammenhang mit Flüchtlingsheimen, Sicherheitsdiensten oder sonstigen sicherheitsrelevanten Stellen eingesetzt sind.

Buchst. a betrifft die Mitwirkung in Geheimschutzsachverhalten. Diese originär aus § 3 Abs. 2 Nr. 1 des Bundesverfassungsschutzgesetzes folgende und im bisherigen § 2 Abs. 5 Nr. 1 geregelte Aufgabe wird deklaratorisch auch von § 2 Abs. 3 genannt. Buchst. a enthält die zugehörige Übermittlungsbefugnis.

Buchst. b umfasst die Übermittlungsbefugnis bei der Mitwirkung im Kontext kritischer Infrastrukturen.

Buchst. c erlaubt die Auskunft im Rahmen der Einstellung in den öffentlichen Dienst. Die Zulässigkeit einer solchen Auskunft über Bewerber ist ausdrücklich von deren Einwilligung abhängig. Nach § 7 Abs. 1 Nr. 2 des Beamtenstatusgesetzes (BeamtStG) setzt die Berufung in das Beamtenverhältnis voraus, dass der Bewerber die Gewähr dafür bietet, jederzeit für die freiheitliche demokratische Grundordnung im Sinne des Grundgesetzes einzutreten.

Buchst. d betrifft das Einbürgerungsverfahren.

Buchst. e nimmt auf das allgemeine Ausländerrecht und darin geregelte Mitwirkungen Bezug.

Buchst. f verweist auf Mitwirkungen des Landesamts nach verschiedenen Fachgesetzen.

Buchst. g betrifft Zuverlässigkeitsüberprüfungen nach den bewachungs- und gewerberechtlichen Vorschriften und benennt insbesondere die Überprüfung solcher Beschäftigter als Mitwirkungsaufgabe, die in Flüchtlingsunterkünften oder im sicherheitssensiblen Bereich von Veranstaltungen (beispielsweise dem Hessentag) eingesetzt werden sollen.

Buchst. h betrifft die Zuverlässigkeitsüberprüfung von an der Hessischen Erstaufnahmeeinrichtung für Flüchtlinge und ihren Außenstellen beschäftigten Dolmetscherinnen und Dolmetschern, die nicht unter die bewachungs- und gewerberechtlichen Vorschriften nach Buchst. g fallen.

Buchst. i schafft einen originären Mitwirkungstatbestand im Rahmen der Präventionsaufgabe. Danach können u.a. in staatlichen Präventionsstellen und -gremien (z.B. dem Hessischen Informations- und Kompetenzzentrum gegen Extremismus – HKE) oder in Projekten und Partnervereinen (etwa dem Violence Prevention Network e.V.) tätige Personen auf der Basis der Einwilligung auf ihre Zuverlässigkeit überprüft werden.

Buchst. j betrifft die Mitwirkung im Kontext der Vollzugsgesetze.

Buchst. k benennt bestimmte Ordensverfahren als Mitwirkungsaufgabe des Landesamts.

Buchst. l regelt die Übermittlungsbefugnis des Landesamts nunmehr auch für die Fälle gesetzlich an anderer Stelle normierter Überprüfungen. Dies betrifft z.B. die für den Bereich der Polizei geltenden §§ 13a und 13b HSOG, wonach eine Zuverlässig-

keitsüberprüfung zum Schutz staatlicher Einrichtungen und Veranstaltungen sowie zum Schutz von Veranstaltungen außerhalb des öffentlichen Bereichs mit Einwilligung der betroffenen Person möglich ist. Empfänger nach § 21 Abs. 1 kann hierbei auch die ersuchende Stelle bzw. Behörde im Sinne des § 13a HSOG sein. Eine weitere Fallgestaltung sind Überprüfungen nach § 2 Abs. 2 Satz 1 Nr. 2 des Artikel 10-Gesetzes.

Buchst. m enthält einen originären Auffangtatbestand für sonstige Fälle, in denen ein besonderes öffentliches Interesse an einer Überprüfung der Verfassungstreue von Personen besteht. Soweit die Auskunftserteilung nicht bereits durch eine spezialgesetzliche Regelung ermöglicht wird (z.B. nach § 9 Abs. 2 Satz 2 und 3 BewachV), kann über Buchst. m mit Einwilligung der betroffenen Person eine Auskunft des Landesamts für Verfassungsschutz eingeholt werden.

Zu Abs. 2:

Nach Ansicht des Bundesverfassungsgerichts ist der Austausch von Daten zwischen Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden grundsätzlich nur zulässig, wenn der Datenaustausch einem herausragenden öffentlichen Interesse dient, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten im Unterschied zur Polizei zu Gebot stehen, rechtfertigt. Dies muss durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein; insbesondere die Eingriffsschwellen für das Erlangen der Daten dürfen hierbei nicht unterlaufen werden (BVerfGE 133, 277 Rn. 123).

Satz 1 zieht in Umsetzung des ATDG-Urteils der Übermittlung von Informationen des Landesamts für Verfassungsschutz, die mit nachrichtendienstlichen Mitteln gewonnen wurden, an die Staatsanwaltschaften, Polizeien sowie Finanz- und Zollbehörden engere Grenzen als das geltende Gesetz. Der in Satz 1 bezeichnete Empfängerkreis für Informationen des Landesamts für Verfassungsschutz, die mit nachrichtendienstlichen Mitteln gewonnen wurden, entspricht dem neu gefassten § 19 Abs. 1 Satz 1 des Bundesverfassungsschutzgesetzes und folgt daraus, dass das Bundesverfassungsgericht die beschränkenden Erwägungen an das Übermittlungsziel eines „operativen polizeilichen Tätigwerdens“ knüpft, also letztlich auf Zwangsmaßnahmen der Vollzugspolizei bezieht. Diese Erwägung ist jedoch nicht auf die Schutzpolizei beschränkt, sondern erstreckt sich konsequenterweise auch auf die Kriminalpolizei, die Staatsanwaltschaften sowie die bei Steuerstraftaten nach § 386 der Abgabenordnung (AO) ermittelnde Finanzbehörde und die nach § 404 AO zuständige Steuer- und Zollfahndung. Nach dem Vorbild des Bundesverfassungsschutzgesetzes wird im Interesse der Rechtssicherheit die Beschränkung der Übermittlung an diese Stellen unabhängig von einem womöglich intendierten Ziel irgendwelchen Tätigwerdens geregelt (vgl. BT-Drs. 18/4654, S. 33). Da die Aufgabe des Landesamts für Verfassungsschutz gemäß § 2 Abs. 2 Satz 1 i.V.m. § 3 Abs. 1 des Bundesverfassungsschutzgesetzes in der nachrichtendienstlichen Sammlung und Auswertung von Informationen besteht, werden im Rahmen der Informationsübermittlung keine Rohdaten, sondern Erkenntnisse der Auswertung weitergegeben. Der Nachrichtendienst fungiert also nicht als Vorfeldbeschaffer der Sicherheits- und Strafverfolgungsbehörden, sondern wird als analytischer Informationsdienstleister tätig.

Die aufgabengemäße, vorgelagerte Informationsfilterung bewirkt, dass der in der Übermittlung einer punktuellen, gefahrenrelevanten Information liegende Grundrechtseingriff regelmäßig geringer wiegt als der vorausgegangene, gefahrerforschende Erhebungseingriff (z.B. durch eine länger andauernde verdeckte Wohnraumüberwachung). Er muss daher allgemein nicht denselben Voraussetzungen unterliegen, unter denen dem Empfänger eine eigene Erhebungsbefugnis (mit entsprechender gefahrerforschenden Streubreite) eingeräumt werden könnte (vgl. BT-Drs. 18/4654, S. 33).

Die Restriktionen in Satz 1 gelten nur für Informationen, die mit nachrichtendienstlichen Mitteln gezielt gewonnen wurden, und erstrecken sich insbesondere nicht auf Zufallserkenntnisse außerhalb der Maßnahmerichtung. Bei letzteren kann nichts anderes gelten als bei außerdienstlichen Erkenntnissen des eingesetzten Beamten. Hier gibt es keinen Grund, die Übermittlung durch besondere gesetzliche Hürden einzuschränken. Unberührt bleiben freilich Einschränkungen, die sich aus dem Grundsatz der Verhältnismäßigkeit nach § 15 ergeben. Aus dem Erforderlichkeitsgrundsatz nach § 15 Abs. 1 folgt, dass Daten, die mit nachrichtendienstlichen Mitteln gewonnen wurden, nur übermittelt werden dürfen, wenn der Zweck nicht auch durch Übermittlung sonstiger Informationen zu erreichen ist.

In Nr. 1 und 2 werden die qualifizierten Übermittlungsschwellen des § 19 Abs. 1 Satz 1 Nr. 2 bis 4 des Bundesverfassungsschutzgesetzes übernommen. Nr. 3 und 4 der bundesgesetzlichen Regelung wurden in Nr. 2 zusammengefasst. Auf eine der Nr. 1 des Bundes entsprechende Vorschrift wurde verzichtet. Dass das Landesamt an Sicherheits- und Strafverfolgungsbehörden personenbezogene Daten zur Erfüllung eigener Aufgaben übermitteln darf, ergibt sich bereits aus § 4 Abs. 1 Satz 1.

Nach der Systematik des Gesetzentwurfs erfasst § 21 mithin nur die Übermittlung von Informationen, die nicht zum Zweck der eigenen Aufgabenerfüllung, sondern für Zwecke des Empfängers übermittelt werden.

Nr. 1 ermöglicht die Übermittlung zur Abwehr einer im Einzelfall bestehenden Gefahr für die bezeichneten Rechtsgüter. Diese Rechtsgüter zeichnen sich durch ein herausragendes öffentliches Schutzinteresse aus (vgl. BT-Drs. 18/4654, S. 33). Im Rahmen der Ausübung des Entschließungsermessens sind im jeweiligen Einzelfall nach Maßgabe des Verhältnismäßigkeitsgrundsatzes (§ 15) der Grad der jeweiligen Gefährdung der Rechtsgüter, die Wahrscheinlichkeit der Realisierung einer Störung und die Erkenntnisdichte zu berücksichtigen.

Nr. 2 regelt die Übermittlung zum Schutz strafrechtlich geschützter Güter. Diese werden weder durch die Nr. 1 noch durch den Satz 2 vollständig abgedeckt. Mit der Strafbewehrung als schärfster Sanktion, die dem Staat zur Verfügung steht, bringt die Rechtsordnung prinzipiell das herausragende öffentliche Interesse an der Vermeidung ethisch nicht mehr hinnehmbarer Verhaltensweisen zum Ausdruck. Jedenfalls, wenn es um die Verhütung von schweren Straftaten geht, darf die Informationsübermittlung daher nicht erst erfolgen, wenn die Gefahr bereits konkret vor ihrer Realisierung steht. Der Begriff der „Straftat von erheblicher Bedeutung“ umfasst Verbrechen i.S.v. § 12 Abs. 1 StGB und schwerwiegende Vergehen i.S.v. § 12 Abs. 2 StGB, wenn die Straftat im Einzelfall mindestens dem Bereich der mittleren Kriminalität zuzurechnen ist, sie den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (vgl. BT-Drs. 18/4654, S. 34; 16/5846, S. 40).

Nr. 3 enthält eine Auffangnorm zur Übermittlung von Informationen, die nicht dem informationellen Trennungsgebot unterliegen. Dieses beruht auf dem Gedanken, dass Nachrichtendienste und Sicherheitsbehörden über Datenerhebungs- und Eingriffsbefugnisse unterschiedlicher Reichweite verfügen, die durch einen freien Informationsaustausch nicht unterlaufen werden dürfen (BVerfGE 133, 277 Rn. 112ff.). Nach Ansicht des Bundesverfassungsgerichts kommt es deshalb insbesondere auf die Vergleichbarkeit der verschiedenen Informationszusammenhänge an, also wieweit die Bindungen der Datenerhebung seitens der übermittelnden Behörde denen entsprechen, unter denen die abfragenden Behörden Daten erheben können. Eine Zweckänderung ist danach ausgeschlossen, wenn mit ihr grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Ermittlungsmethoden umgangen werden, also die Informationen für den geänderten Zweck selbst auf entsprechender gesetzlicher Grundlage nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen (BVerfGE 133, 277 Rn. 114; 120, 351, 369; 109, 279, 377). Umgekehrt ergeben sich aus dem informationellen Trennungsgebot grundsätzlich keine Bedenken gegen eine Übermittlung der Informationen, soweit die Befugnisse zur Datenerhebung deckungsgleich sind. Schließlich hätte der Empfänger auf der Grundlage seiner eigenen Befugnisse die Informationen ja auch selbst erheben können. Beschränkend wirkt in dieser Fallkonstellation allerdings weiterhin der Grundsatz der Verhältnismäßigkeit (§ 15). Denn die mit der Informationsübermittlung verbundene Zweckänderung bedarf als Eingriff in das Rechts auf informationelle Selbstbestimmung einer eigenen Rechtfertigung. Insbesondere muss daher die Informationsübermittlung für den Empfänger zur Wahrnehmung seiner Aufgaben erforderlich sein.

Satz 3 enthält eine Pflicht zur Informationsübermittlung in Angelegenheiten des Staats- und Verfassungsschutzes. Aus der Gesetzessystematik folgt, dass die für den besonderen Bereich des Staats- und Verfassungsschutzes geltende Regelung des Satz 3 gegenüber der allgemeinen Übermittlungsbefugnis in Satz 1 speziell ist. Nach § 21 Abs. 1 Satz 1 des Bundesverfassungsschutzgesetzes sind die Landesverfassungsschutzbehörden verpflichtet, unter den Voraussetzungen des § 20 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes im besonders sicherheitsrelevanten Bereich der Staatsschutzdelikte den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien Informationen einschließlich personenbezogener Daten zu übermitteln. Da dem Bundesgesetzgeber in Art. 73 Abs. 1 Nr. 10 des Grundgesetzes nur die Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder zusteht, erstreckt sich die Verpflichtung – wie § 21 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes ausdrücklich klarstellt – nicht auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslands. Diese Regelungslücke wird durch Satz 3 geschlossen. Andernfalls entstünde die paradoxe Situation, dass das Landesamt Informationen zwar an Staatsanwaltschaften und Polizeien anderer Länder, nicht aber an hessische Behörden übermitteln müsste. In Umsetzung der Empfehlung der Expertenkommission der Hessischen Landesregierung, die Übermittlungsvorschriften von Bund und Ländern zu harmonisieren, wird eine Übermittlungspflicht in das Hessische Verfassungsschutzgesetz implementiert.

Zu § 22 (Informationsübermittlung durch das Landesamt an Stationierungsstreitkräfte und an ausländische öffentliche Stellen)

Durch § 22 erhält das Landesamt die Befugnis zur Informationsübermittlung an die genannten Stellen.

Abs. 1 nimmt auf bestehende völkerrechtliche Verpflichtungen der Bundesrepublik Deutschland gegenüber den NATO-Partnern Bezug (ebenso § 19 Abs. 2 des Bundesverfassungsschutzgesetzes). Diese Verpflichtungen werden durch Abs. 1 nicht verändert, sondern lediglich für das Landesamt konkretisiert.

Abs. 2 lässt Informationsübermittlungen an befreundete Dienste zu (entspricht § 19 Abs. 3 des Bundesverfassungsschutzgesetzes). Auf solche Kontakte sind die Verfassungsschutzbehörden in Deutschland insbesondere bei der Terrorismus- und Spionagebekämpfung angewiesen. Im Rahmen der dazu notwendigen langfristigen Zusammenarbeit kann von den Kooperationspartnern die Übermittlung aufgabenrelevanter Informationen nur erwartet werden, wenn auch diese durch übermittelte Informationen von der Zusammenarbeit profitieren. Damit dieses „Gegenseitigkeitsprinzip“ nicht zu Lasten des Persönlichkeitsschutzes der betroffenen Person wirkt, beschränkt die Nr. 2 die Zulässigkeit der Übermittlung auf solche Informationen, die zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich sind.

Im Unterschied zum bisherigen Gesetz wird die Informationsübermittlung zur Erfüllung eigener Aufgaben des Landesamts für Verfassungsschutz nicht mehr explizit erwähnt, da sich die Befugnis hierzu bereits aus § 5 Abs. 1 Satz 1 Nr. 1 ergibt und § 19 nach neuer Systematik nur die Übermittlung zu Zwecken des Empfängers betrifft.

Zu Abs. 3:

Als weitere Übermittlungsschranke normiert Abs. 3 die über den Übermittlungsvorgang hinausreichende Wirkung des Zweckbindungsgrundsatzes. Die entsprechenden Regelungen des bisherigen Gesetzes, die über mehrere Absätze verstreut sind (§ 14 Abs. 1 Satz 3, Abs. 2 Satz 2, Abs. 3 Satz 4, Abs. 4 Satz 4 und 5), werden nun zentral in einem Absatz „hinter die Klammer gezogen“.

Satz 1 stellt entsprechend den Vorgaben des Bundesverfassungsgerichts (BVerfGE 109, 279, 334) die Übermittlung von Daten aus Maßnahmen nach den §§ 7 oder 8 an Behörden außerhalb des Verfassungsschutzverbunds (Polizei, Staatsanwaltschaft etc.) unter die zusätzliche verfahrensrechtliche Voraussetzung richterlicher Zustimmung nach § 9 Abs. 1. Über den Verweis auf § 9 Abs. 1 Satz 2 reicht im Eilfall auch eine Entscheidung der Behördenleitung oder ihrer Vertretung, die nachträglich richterlich genehmigt wird.

Satz 2 verpflichtet den Empfänger, die erhaltenen Informationen nur für den der Übermittlung zugrunde liegenden Zweck zu verwenden. Dadurch wird gewährleistet, dass sensible personenbezogene Daten im Bereich der für Sicherheitsaufgaben zuständigen Behörden nicht unkontrolliert gestreut werden können.

Eine „Weiterübermittlung“ durch die Empfängerbehörde zu anderen Zwecken kommt nur in Betracht, wenn für die Zweckänderung eine gesonderte gesetzliche Befugnis besteht.

Satz 3 statuiert für das Landesamt eine Pflicht zur Belehrung des Empfängers über die Zweckbindung der übermittelten Information. Soweit die Übermittlung nach Abs. 3 an Stellen im Ausland und nicht-öffentliche Stellen erfolgt, ist der Empfänger zusätzlich darauf hinzuweisen, dass das Landesamt sich das Recht vorbehält, über die Verwendung der Daten Auskunft zu verlangen. Dieser Vorbehalt kompensiert den Umstand, dass die Empfänger nicht in gleicher Weise der staatlichen Kontrolle durch deutsche Behörden und Gerichte unterliegen wie inländische öffentliche Stellen.

Zu Abs. 4:

Nach der Rechtsprechung steht dem für den Verfassungsschutz zuständigen Ministerium aus seiner Stellung als Aufsichtsbehörde über das Landesamt kein generelles Selbsteintrittsrecht dergestalt zu, dass es beim Landesamt gespeicherte personenbezogene Daten nach außen weiterleiten darf (BVerwG Buchholz 11 Art. 2 GG, Nr. 86 Rn. 19ff.). Daher normiert Abs. 4 eine entsprechende Befugnis.

Zu § 23 (Informationsübermittlung durch das Landesamt an Stellen außerhalb des öffentlichen Bereichs)

§ 23 ermöglicht ausnahmsweise auch eine Informationsübermittlung an Stellen außerhalb des öffentlichen Bereichs (bisher § 14). Eine solche Befugnis ist notwendig, um z.B. Fluggesellschaften oder Banken warnen zu können, wenn gewalttätige Extremisten ihre Dienste nutzen wollen. In materieller Hinsicht ist die Übermittlungsbefugnis dadurch begrenzt, dass die Weitergabe der Information zum Schutz vor den in § 3 dieses Gesetzes und § 3 des Bundesverfassungsschutzgesetzes genannten Bestrebungen, Tätigkeiten und Gefahren erforderlich ist. Als zusätzliche verfahrenstechnische Absicherung bedarf es der Zustimmung der zuständigen Aufsichtsbehörde. Der zweite Halbsatz erlaubt eine vorherige Generalzustimmung für bestimmte abgrenzbare Fallgruppen, z.B. für die Mitteilung an Sicherheitsbeauftragte in der Wirtschaft nach § 3 Abs. 2 Nr. 2 des Bundesverfassungsschutzgesetzes, dass hinsichtlich einer bestimmten Person keine Sicherheitsbedenken bestehen.

Zu § 24 (Übermittlungsverbote)

Die Neufassung des bisherigen § 15 dient der Konkretisierung der dort bereits genannten „Sicherheitsinteressen“ und soll die Rechtssicherheit erhöhen. Die ausdrückliche Aufnahme des Quellenschutzes als Grund für ein Übermittlungsverbot soll die besondere Schutzwürdigkeit verdeutlichen. Das Erwähnen des „Schutzes operativer Maßnahmen“ bringt zum Ausdruck, dass zwischen Strafrechtspflege und Verfassungsschutz kein Subordinationsverhältnis besteht, sondern deren jeweilige Belange im Kollisionsfall in einen möglichst schonenden Ausgleich zu bringen sind.

Die im Gesetz geregelten Übermittlungsvorschriften verfolgen als normatives Ziel die Zusammenarbeit der Sicherheitsbehörden durch einen verbesserten Informationsaustausch.

Die hierfür maßgeblichen Grundsätze hat die Bund-Länder-Kommission Rechtsterrorismus in ihrem Abschlussbericht differenziert herausgearbeitet.

Auch ist eine entsprechende Forderung im Abschlussbericht des Bundestagsuntersuchungsausschusses „Rechtsterrorismus“ (NSU I, S. 865, Empfehlung Nr. 47) zu finden. Gründe des Quellen- und sonstigen Geheimschutzes können einer Übermittlung danach nicht generell, sondern nur nach Abwägung der widerstreitenden Interessen entgegenstehen.

In Abs. 1 Nr. 2 wird deshalb klargestellt, dass Gründe des Quellenschutzes und des Schutzes operativer Maßnahmen als Sicherheitsinteressen zu qualifizieren sind, die im Einzelfall einer Informationsübermittlung entgegenstehen können. Das Übermittlungsverbot des Abs. 1 Nr. 2 steht einer Information der Strafverfolgungsbehörden über Straftaten von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern sowie Vertrauensleuten nach § 13 Abs. 2 Satz 4 i.V.m. § 14 Abs. 1 nicht entgegen. Für die Übermittlung von Informationen aus einer verdeckten Wohnraum- oder Onlineüberwachung, für die nach der Rechtsprechung des Bundesverfassungsgerichts besondere Anforderungen gelten (vgl. BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 u.a., Rn. 320), ergeben sich bereits aus § 9 Abs. 3 qualifizierte Voraussetzungen für Zweckänderungen, die auch bei der Übermittlung zu beachten sind.

Abs. 2 konkretisiert die im Rahmen von Abs. 1 Nr. 1 und 2 zu treffende Abwägungsentscheidung (vgl. hierzu die Empfehlungen der BLKR, Abschlussbericht vom 30. April 2013, Rn. 697ff. Durch die in Satz 1 enthaltene Abwägungsregel, die ihrerseits eine Rückausnahme für den Fall enthält, dass eine gegenwärtige Gefahr für hochrangige Rechtsgüter oder die Verfolgung besonders schwerer Straftaten eine Gefahr nur um den Preis einer Gefahr für gleichwertige Rechtsgüter beseitigt werden kann, wird einerseits klargestellt, dass der Quellenschutz nicht absolut gilt, anderseits der Gefahr vorgebeugt, dass eine Informationsübermittlung wegen Überwiegens der Gründe des Quellenschutzes vorschnell unterbleibt. Satz 2 und 3 sichern die Entscheidung darüber, ob die Voraussetzungen von Satz 1 zu bejahen sind und die Informationsübermittlung erfolgt, verfahrensrechtlich ab. Dies geschieht durch einen Entscheidungsvorbehalt der Behördenleitung bzw. ihrer Vertretung und die Pflicht zur Information des für den Verfassungsschutz zuständigen Ministeriums als Aufsichtsbehörde, das wiederum die Parlamentarische Kontrollkommission zu unterrichten hat.

Zu § 25 (Minderjährigenschutz)

Entspricht dem bisherigen § 16. Inhaltlich bestehen keine Änderungen.

Zu § 26 (Nachberichtspflicht)

Entspricht dem bisherigen § 17. Inhaltlich bestehen keine Änderungen.

Zu § 27 (Auskunft)

§ 27 überführt die bislang in § 18 enthaltene Auskunft in eine Regelung, die zum einen das berechtigte Informationsinteresse der betroffenen Person gewährleisten, gleichzeitig aber unverhältnismäßigen Verwaltungsaufwand verhindern soll.

Das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes) gewährleistet nach der Rechtsprechung des Bundesverfassungsgerichts unter den Bedingungen der modernen Datenverarbeitung die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfGE 115, 166, 188; 65, 1, 43). Fehlender Zugang zum Wissen Dritter über die eigene Person kann die von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes geschützte individuelle Selbstbestimmung berühren. Daher kann dieses Grundrecht seinem Träger auch Rechtspositionen verschaffen, die den Zugang zu den über ihn gespeicherten persönlichen Daten betreffen (vgl. BVerfG NJW 2006, 1116 Rn. 21f.; BVerfGE 65, 1, 43). Insbesondere, wenn Daten für die betroffene Person nicht unmittelbar wahrnehmbar gespeichert und verarbeitet werden, sieht das Bundesverfassungsgericht in der gesetzlichen Gewährung eines Auskunftsanspruchs ein wichtiges verfahrensrechtliches Instrument, um Transparenz herzustellen und effektiven Individualrechtsschutz zu gewährleisten (BVerfGE 133, 277 Rn. 208ff.).

§ 27 konkretisiert auf der Ebene des Gesetzes diese verfassungsrechtlichen Vorgaben. Die Vorschrift tritt an die Stelle der allgemeinen Regelung in § 18 HDSG, die nach § 16 nicht anwendbar ist.

Zu Abs. 1:

Satz 1 enthält die gesetzliche Anspruchsgrundlage für den Auskunftsanspruch. Anspruchsberechtigt ist der Betroffene i.S.v. § 2 Abs. 1 HDSG. Die Geltendmachung des Anspruchs setzt einen Antrag der betroffenen Person voraus. Diesen trifft eine Mitwirkungsobliegenheit. Um dem Landesamt eine Prüfung des Auskunftsbegehrens zu ermöglichen und dabei einer Ausforschung vorbeugen zu können, verlangt Satz 1, dass der Betroffene ein besonderes Interesse an der Auskunft darlegt (vgl. auch § 15 Abs. 1 Satz 1 des Bundesverfassungsschutzgesetzes).

Die Auskunftserteilung durch das Landesamt erfolgt unentgeltlich, d.h. es werden weder Gebühren noch Auslagen geltend gemacht. Dies folgt aus der Natur des Anspruchs als Schutzrecht der betroffenen Person.

Satz 2 enthält die dem Informationsinteresse dienende Klarstellung, wonach Antragsteller, die kein besonderes Interesse an einer Auskunft dargelegt haben, zunächst auf dieses Erfordernis hinzuweisen sind. Ferner darf das Landesamt einen unsubstantiiert bleibenden Antrag nicht ohne weiteres ablehnen. Vielmehr hat die Behörde, nachdem der vorgeschriebene Hinweis auf die Mitwirkungspflicht erteilt wurde und dennoch keine entsprechende Substantiierung erfolgte, nach pflichtgemäßem Ermessen zu entscheiden.

Das Ermessen ist nach Maßgabe des Zwecks der Regelung auszuüben. Dieser besteht darin, einen im Hinblick auf das Informationsinteresse unverhältnismäßigen Verwaltungsaufwand zu vermeiden und Ausforschungsgefahren zu begegnen, und muss im Hinblick auf das jeweilige Informationsinteresse den Grundsatz der Verhältnismäßigkeit wahren (BVerfG NVwZ 2001, 185, 186).

Satz 3 regelt den Umfang der Auskunftserteilung. Gegenstand der Auskunft sind grundsätzlich alle zur betroffenen Person gespeicherten Daten unabhängig von der Art der Aktenführung und der Form der Speicherung; also nicht nur die im elektronischen Fachverfahren hinterlegten, sondern auch die in einem Dokumenten-Management-System (DMS) gespeicherten personenbezogenen Daten. Erfasst werden alle personenbezogenen Daten, die einen Bezug zur betroffenen Person aufweisen, ohne dass zwischen Daten „zur Person“ und Daten „über die Person“ zu differenzieren wäre (vgl. BVerwG Buchholz 402.71 BNDG Nr. 2 Rn. 30ff. zu § 15 des Bundesverfassungsschutzgesetzes). Der somit grundsätzlich weit zu bestimmende Auskunftsanspruch wird allerdings durch Nr. 1 und 2 des Satzes 3 in zweierlei Hinsicht eingeschränkt:

Nr. 1 stellt klar, dass der Auskunftsanspruch nach Satz 1 sich abweichend von § 18 Abs. 3 Satz 1 Nr. 3 HDSG nicht auf die Angaben über Herkunft und Empfänger der Daten erstreckt. Diese inhaltliche Begrenzung der Auskunftspflicht trägt den spezifischen Geheimhaltungsinteressen des Landesamts Rechnung.

Nr. 2 zielt auf einen Ausgleich zwischen dem Auskunftsinteresse der betroffenen Person und dem mit der Auskunftserteilung verbundenen Aufwand des Landesamts. Soweit Daten zu einer Person strukturiert in einer Datei gespeichert und daher über einen entsprechenden Suchbegriff auffindbar sind, ist das Landesamt in der Lage, auf die Daten kurzfristig zuzugreifen und sich mit ihrer Hilfe ein Bild von der betroffenen Person zu machen. Bei dieser typischen Fallkonstellation besteht ein erhebliches Interesse der betroffenen Person an einer diesbezüglichen Auskunft, die dann auch ohne größeren Verwaltungsaufwand erteilt werden kann. Anders verhält es sich bei einzelnen, aus anderem Anlass gespeicherten Daten, die nicht strukturiert mit der betroffenen Person verknüpft werden und, da eine Rasterfahndung rechtlich nicht zulässig ist, nicht durch automatisierte Suche aufgefunden werden können. Die zur Erfüllung des Auskunftsbegehrens erforderliche Durchsicht der in Betracht kommenden Vorgänge würde in vielen Fällen einen erheblichen Aufwand erfordern, dem ein deutlich geringeres Interesse der betroffenen Person an dieser Auskunft gegenübersteht, weil die typische Gefahrenlage für das Recht auf informationelle Selbstbestimmung, dem der Auskunftsanspruch begegnen will, kaum gegeben ist (vgl. OVG Nordrhein-Westfalen NVwZ-RR 2009, 505/506; die hiergegen erhobene Verfassungsbeschwerde wurde nicht zur Entscheidung angenommen, s. BVerfG, B. v. 17. Mai 2011, Az. 1 BvR 780/09). Zwar können Vorgänge auch Daten Dritter (nicht-NADIS-erfasste Personen) enthalten, diese sind aber für das Landesamt nicht gezielt auffindbar. Daran ändert auch eine etwaige elektronische Aktenführung nichts. Da es sich um keine Zielpersonen des Verfassungsschutzes handelt, ist zudem eine Identifizierung der Person auf der vorhandenen Datengrundlage in der Regel kaum zuverlässig möglich, d.h. es kann typischerweise nicht festgestellt werden, ob solche Daten einer anfragenden Person zuordenbar sind. Amtsermittlungen des Landesamts zur weiteren Abklärung entsprechen meist nicht dem Interesse der betroffenen Person (vgl. BT-Drs. 18/4654, S. 31 zu § 15 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes).

Angesichts dieser von der typischen Fallkonstellation differierenden Sachlage macht die Nr. 2 die Auskunft über personenbezogene Daten, bei denen keine strukturierte Speicherung in automatisierten Dateien erfolgt ist, von Angaben der betroffenen Person, die das Auffinden ermöglichen, und einer Verhältnismäßigkeitsabwägung zwischen dem mit der Identifizierung und Zusammenstellung der Daten erforderlichen Verwaltungsaufwand und dem Informationsinteresse der betroffenen Person abhängig. Insoweit konkretisiert die Formulierung der Nr. 2 die rechtlich erheblichen Gesichtspunkte der auf dieselbe Fallgestaltung zugeschnittenen Neuregelung in § 15 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes.

Satz 4 enthält Regelungen zum Verfahren, d.h. dem „Wie“ der Auskunftserteilung. Die Verfahrensgestaltung, insbesondere die Form der Auskunftserteilung ist in das pflichtgemäße Ermessen des Landesamts gestellt. Dagegen besteht hinsichtlich des „Ob“ der Auskunft nach Satz 1 kein Ermessensspielraum. Zur Frage des „Wie“ gehört auch die Entscheidung darüber, ob bei Anträgen von Personen, zu denen mehrere hundert Einzelinformationen vorliegen, anstelle einer vollumfänglichen Auflistung der Einzelinformationen eine „zusammengefasste“ Auskunft erteilt wird.

Zu Abs. 2:

Abs. 2 übernimmt inhaltlich die Regelung des bisherigen § 18 Abs. 2. Die darin abschließend aufgeführten Tatbestände umfassen Fallgestaltungen, bei denen das Recht auf informationelle Selbstbestimmung des Einzelnen hinter dem vorrangigen öffentlichen Interesse unter dem Gesichtspunkt der Inneren Sicherheit zurückzutreten hat. Auch wenn das Auskunftsrecht der betroffenen Person dem Grundrecht auf informationelle Selbstbestimmung Rechnung trägt, besteht es nicht absolut. Vielmehr sind Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit zulässig (BVerfGE 65, 1, 44ff.). Die in Abs. 2 aufgeführten Gründe der Inneren Sicherheit stellen ein solches überwiegendes Allgemeininteresse dar.

Unter die Nr. 2 können Auskunftsersuchen fallen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass diese nicht aufgrund eines individuellen Informationsinteresses gestellt werden, sondern ausschließlich, um die Arbeitsweise und den Kenntnisstand des Landesamts für Verfassungsschutz auszuforschen bzw. um bewusst signifikanten Verwaltungsaufwand zu erzeu-

gen. An die Annahme einer solchen Fallgestaltung sind strenge Anforderungen zu stellen. Von einem Ausforschungsversuch oder einer rechtsmissbräuchlichen Ausübung des Auskunftsrechts darf ausnahmsweise nur dann ausgegangen werden, wenn offenkundig mehrere Anträge von Personen eingehen, die etwa einem regional eingrenzbaren Beobachtungsobjekt angehören oder wenn öffentlich zu einer „Auskunftskampagne“ aufgerufen wird.

Liegen daher einer oder mehrere der in Nr. 1 bis 4 aufgeführten Versagungsgründe vor, hat die Auskunftserteilung zu unterbleiben.

Zu Abs. 3:

Abs. 3 umfasst die Regelungen des bisherigen § 18 Abs. 4. Satz 1 lässt die Ablehnung der Auskunftserteilung ohne Begründung zu. Es liegt damit ein Fall des § 39 Abs. 2 Nr. 4 HVwVfG vor, wonach ein Verwaltungsakt keiner Begründung bedarf, wenn sich dies aus einer Rechtsvorschrift ergibt. Der Ausschluss der Begründung ist mit dem Rechtsstaatsprinzip vereinbar. Er findet seine Rechtfertigung darin, dass eine Begründung immer gewisse Hinweise auf die Art der Erkenntnisse bzw. den Grund, warum die Auskunft nicht erteilt werden kann, beinhalten müsste.

Satz 2 enthält als Kompensation der fehlenden Begründung eine dem § 18 Abs. 6 Satz 3 HDSG entsprechende Belehrungspflicht hinsichtlich der Möglichkeit der betroffenen Person, sich an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten zu wenden.

Satz 3 untersagt es der oder dem Hessischen Datenschutzbeauftragten allerdings, ohne Zustimmung des Landesamts in eine Mitteilung an die betroffene Person Informationen aufzunehmen, die Rückschlüsse auf den Erkenntnisstand des Verfassungsschutzes zulassen, da andernfalls die Ablehnungsgründe des Abs. 2 umgangen und die dahinter stehenden Gesichtspunkte der inneren Sicherheit beeinträchtigt würden.

Zum Vierten Teil (Schlussvorschriften)

Zu § 28 (Einschränkung von Grundrechten)

Nach Art. 19 Abs. 1 Satz 2 des Grundgesetzes muss ein Gesetz die von ihm eingeschränkten Grundrechte unter Angabe des Artikels nennen. Auch wenn die Verfassung des Landes Hessen keine entsprechende Vorschrift kennt, werden nach ständiger Übung der Gesetzgebung bei der Umsetzung von Art. 19 Abs. 1 Satz 2 des Grundgesetzes auch die entsprechenden Grundrechtsartikel der Verfassung mitzitiert. Bisher war dies in § 23 erfolgt.

Im neuen § 28 wird im Hinblick auf die Fortentwicklung der Rechtsprechung des Bundesverfassungsgerichts (vgl. insbesondere BVerfGE 122, 342, 366ff.) die Versammlungsfreiheit nach Art. 8 des Grundgesetzes und Art. 14 der Verfassung des Landes Hessen zitiert. Außerdem wird zitiert das Brief-, Post- und Fernmeldegeheimnis nach Art. 10 des Grundgesetzes und Art. 12 der Verfassung des Landes Hessen, das insbesondere durch Auskunftsersuchen nach § 11 eingeschränkt wird, sowie das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 des Grundgesetzes und Art. 8 der Verfassung des Landes Hessen, in das durch Überwachungsmaßnahmen nach § 7 eingegriffen wird. Die Datenerhebung sowohl mittels offener Informationsquellen als auch mit nachrichtendienstlichen Mitteln kann auch einen Eingriff in die nach Art. 8 des Grundgesetzes und Art. 14 der Verfassung des Landes Hessen geschützte Versammlungsfreiheit bedeuten und wird deshalb zitiert.

Nicht zitiert wird das Grundrecht auf informationelle Selbstbestimmung, das über Art. 2 Abs. 1 des Grundgesetzes unter dem Vorbehalt der verfassungsmäßigen Ordnung steht und daher nicht dem Zitiergebot unterliegt (vgl. BVerfG NJW 1999, 3399, 3400; BVerfGE 10, 89, 99).

Zu § 29 (Aufhebung bisherigen Rechts)

Da der Gesetzentwurf eine vollständige Novellierung vornimmt, wird das bislang geltende Gesetz über das Landesamt für Verfassungsschutz aufgehoben.

Zu § 30 (Inkrafttreten)

Entspricht dem bisherigen § 24. Aufgrund der fortwährenden Notwendigkeit eines Hessischen Verfassungsschutzgesetzes als Rechtsgrundlage für die Arbeit des Landesamts sieht der Entwurf keine Befristung vor.

Zu Artikel 2 (Verfassungsschutzkontrollgesetz)

A. Allgemeines

Das Land Hessen ist entschlossen, sich Angriffen auf die freiheitliche demokratische Grundordnung zu erwehren. Hierbei steht notwendig neben dem bereits konstruktiven, durch Art. 79 Abs. 3 des Grundgesetzes formulierten verfassungsimmanenten Verfassungsschutz der nachrichtendienstliche Verfassungsschutz. Um dieser Aufgabe gerecht zu werden, ist das für den Nachrichtendienst zuständige Landesamt für Verfassungsschutz mit Befugnissen ausgestattet, die es ihm ermöglichen, zeitlich vor dem Eintritt einer konkreten Gefahr Informationen zu erheben und nachrichtendienstliche Mittel einzusetzen. Neben der organisatorischen Trennung des Landesamts für Verfassungsschutz von Polizei und anderen Exekutivbehörden bedarf dessen im Wesentlichen im Verborgenen bleibende Tätigkeit wegen der damit verbundenen geringeren Kontrollmöglichkeiten durch die Öffentlichkeit und die Judikative einer besonderen Kontrolle durch das Parlament. Diese wird durch eine eigene Kontrollkommission ausgeübt.

Um die Bedeutung der parlamentarischen Kontrolle und den Grundsatz der Gewaltenteilung zu unterstreichen, wird die bisher als Teil des Gesetzes über das Landesamt für Verfassungsschutz geregelte parlamentarische Kontrolle nun in ein eigenständiges Gesetz überführt.

Die Regelungen des Gesetzes zur parlamentarischen Kontrolle des Verfassungsschutzes in Hessen orientieren sich an denen des entsprechenden Gesetzes zur parlamentarischen Kontrolle durch den Bundestag.

B. Zu den einzelnen Vorschriften

Zu § 1 (Parlamentarische Kontrolle)

Mit Abs. 2 bis 5 wird die Mitgliedschaft in der Parlamentarischen Kontrollkommission entsprechend der bundesrechtlichen Regelung in § 2 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes vom 29. Juli 2009 (BGBl. I S. 2346), zuletzt geändert durch Gesetz vom 5. Januar 2017 (BGBl. I S. 17), neu geregelt (Begründung vgl. BT-Drs. 16/12411, S. 9 und BT-Drs. 08/1599, S. 7).

Zu § 2 (Geheimhaltung, Protokollierung, Verwendung von mobilen Geräten)

§ 2 regelt die Geheimhaltung der von der Parlamentarischen Kontrollkommission beratenen Sachverhalte. Sie gilt sowohl formell für die Sitzungen (§ 2 Abs. 1 Satz 1 bis 3) als auch über die Sitzungen hinaus (§ 2 Abs. 1 Satz 4).

Jedem Mitglied der Parlamentarischen Kontrollkommission obliegt es persönlich, die Geheimhaltung zu gewährleisten. Die oder der Vorsitzende der Parlamentarischen Kontrollkommission hat vor jeder Sitzung auf die grundsätzliche Geheimhaltung und die damit verbundene Obliegenheit hinzuweisen.

Das Sicherstellen der Geheimhaltung umfasst es auch, Dritten keinen erleichterten Zugang zu den in den Sitzungen erörterten Inhalten und Informationen zu geben. Dies betrifft nicht nur handschriftliche Notizen, sondern auch Mobiltelefone, tragbare elektronische Datenverarbeitungsgeräte oder sonstige Geräte zur Aufzeichnung von Bild- und Tondaten, die technisch sehr einfach manipulierbar sind. Hierdurch besteht die Gefahr der Zweckentfremdung durch Dritte (Abhören etc.), ohne dass der eigentliche Nutzer hiervon Kenntnis erlangt. Notizen sind daher sorgfältig zu verwahren oder zu vernichten, der Gebrauch der genannten Geräte während der Sitzungen der Parlamentarischen Kontrollkommission ist nicht gestattet. Sinn und Zweck ist es, Aufnahmen durch Sitzungsteilnehmer zu verhindern und so der wissentlichen oder unwissentlichen Verbreitung der Inhalte vorzubeugen.

Anders stellt sich die Situation mit Blick auf die vorgesehene Protokollierung der Sitzungen dar. Das Protokoll wird angefertigt, um den Verlauf der Sitzung, die gestellten Fragen und die vorgetragenen Argumente zu einem späteren Zeitpunkt nachvollziehen zu können. Das bedeutet auch, dass den im Protokoll festgehaltenen Inhalten eine besondere Bedeutung für die parlamentarische Kontrolle zukommt. Der Geheimschutz im Übrigen bleibt unberührt, die Aufzeichnungen selbst sind binnen einer Frist von zwei Wochen nach Fertigstellung des Protokolls zu löschen.

Zu § 3 (Pflicht der Landesregierung zur Unterrichtung)

In Abs. 1 und 2 sind nunmehr aus systematischen Gründen die im bisherigen § 22 Abs. 1 und 2 geregelten Unterrichtungspflichten enthalten.

Abs. 3 Nr. 1 sieht eine Unterrichtung über Auskunftsersuchen nach § 11 HVSG im Abstand von höchstens sechs Monaten vor und berücksichtigt damit auch die Regelung des § 8b Abs. 10 i.V.m. § 8b Abs. 3 Satz 1 des Bundesverfassungsschutzgesetzes, wonach eine gleichwertige parlamentarische Kontrolle durch den Landesgesetzgeber zu regeln ist.

Abs. 3 Nr. 2 enthält erstmals die Verpflichtung zu einem jährlichen Lagebericht über die in den Buchstaben a und b genannten Maßnahmen bzw. Einsätze. Dies betrifft die Wohnraumüberwachung (§ 7 HVSG), die sog. Online-Durchsuchung (§ 8 HVSG), den Einsatz eines IMSI-Catchers (§ 10 HVSG), den Einsatz von Verdeckten Mitarbeiterinnen und Verdeckten Mitar-

beitern (§ 13 HVSG) sowie Vertrauensleuten (§ 14 HVSG, s. dazu auch § 9b Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes). Damit wird der besonderen Sensibilität der Materie Rechnung getragen.

Abs. 4 setzt die Vorgabe aus § 8b Abs. 10 Satz 1 des Bundesverfassungsschutzgesetzes um, wonach den Verfassungsschutzbehörden der Länder die Befugnisse nach § 8a Abs. 2 Satz 1 Nr. 4 und 5 des Bundesverfassungsschutzgesetzes (entspricht § 11 Abs. 4 Nr. 2 und 3 HVSG) nur zustehen, wenn eine Verpflichtung zur Berichterstattung über die durchgeführten Maßnahmen an das Parlamentarische Kontrollgremium des Bundes durch den Landesgesetzgeber geregelt ist.

Zu § 4 (Befugnisse der Parlamentarischen Kontrollkommission)

Die Vorschrift entspricht weitgehend dem bisherigen § 22.

Geschaffen wurde ein Akteneinsichtsrecht für jedes individuelle Mitglied der Parlamentarischen Kontrollkommission. Hierdurch wird die Kontrollfunktion insgesamt gestärkt, weil die Ausübung des Akteneinsichtsrechts nun nicht mehr von einem Mehrheitsbeschluss abhängt, sondern individuell geltend gemacht werden kann.

Zu 5 (Mitarbeiterinnen und Mitarbeiter)

Zur Unterstützung ihrer Tätigkeit erhalten die Mitglieder der Parlamentarischen Kontrollkommission die Möglichkeit, die Beratungsgegenstände mit einer Mitarbeiterin oder einem Mitarbeiter zu erörtern.

Zu § 6 (Berichterstattung)

Mit Blick auf die gesamtgesellschaftliche Aufgabe und Bedeutung der Extremismusprävention und damit zusammenhängend die Bedeutung des Verfassungsschutzes und seiner parlamentarischen Kontrolle wird eine Pflicht zur Berichterstattung über die Kontrolltätigkeit der Parlamentarischen Kontrollkommission an den Landtag eingeführt.

Satz 3, 1. Halbsatz verpflichtet die Parlamentarische Kontrollkommission zu einem jährlichen Bericht gegenüber dem Landtag. Dies betrifft Maßnahmen von besonderer Eingriffstiefe: die Wohnraumüberwachung (§ 7 HVSG), die sog. Online-Durchsuchung (§ 8 HVSG), den Einsatz eines IMSI-Catchers (§ 10 HVSG) sowie besondere Auskunftsersuchen (§ 11 HVSG). In den Fällen des § 11 Abs. 4 Nr. 2 und 3 HVSG ergibt sich aus § 8b Abs. 10 Satz 1 i.V.m. § 8b Abs. 3 Satz 2 des Bundesverfassungsschutzgesetzes die Notwendigkeit einer Regelung zur Berichtspflicht.

Mit jeder Ausweitung des Kenntnisträgerkreises sind Geheimschutzrisiken verbunden, weshalb die Berichtspflicht gegenüber dem Landtag nicht auf den besonders sensiblen Bereich des Einsatzes von Verdeckten Mitarbeiterinnen, Verdeckten Mitarbeitern und Vertrauensleuten erstreckt wird.

Hinsichtlich des Umfangs der Berichterstattung nennt der Satz 3, 1. Halbsatz – wie in § 8b Abs. 3 Satz 2 i.V.m. § 8b Abs. 10 des Bundesverfassungsschutzgesetzes für Auskunftsersuchen zu Verkehrsdaten geregelt – für alle genannten Auskunftsersuchen und Maßnahmen die Art und den Umfang der Ersuchen und Maßnahmen sowie die maßgeblichen Anordnungsgründe.

Mit Satz 3, 2. Halbsatz wird klargestellt, dass bei der Berichterstattung der Parlamentarischen Kontrollkommission gegenüber dem Landtag die Grundsätze des § 2 Abs. 1 über die Geheimhaltung zu beachten sind.

Zu Artikel 3 (Inkrafttreten)

Diese Vorschrift regelt das Inkrafttreten des Gesetzes.

Wiesbaden, . Oktober 2017

Für die Fraktion der CDU

Für die Fraktion BÜNDNIS 90/DIE GRÜNEN