LANDTAG RHEINLAND-PFALZ
17. Wahlperiode

Drucksache 17/10488
07. 11. 2019

# Gesetzentwurf

## der Fraktionen der SPD, FDP und BÜNDNIS 90/DIE GRÜNEN

## Landesgesetz zur Neufassung des Landesverfassungsschutzgesetzes und zur Änderung weiterer Gesetze

### A. Problem und Regelungsbedürfnis

Als Folge weltweiter Kriegs- und Konfliktherde sehen sich die Staaten Europas einer hohen Gefährdungslage durch den islamistischen Terrorismus ausgesetzt. Für die Bundesrepublik Deutschland ist nicht zuletzt seit dem Anschlag auf einen Berliner Weihnachtsmarkt am 19. Dezember 2016 deutlich geworden, dass jederzeit mit Anschlägen zu rechnen ist. In Rheinland-Pfalz scheiterte ein durch einen Minderjährigen geplanter Terroranschlag mit islamistischem Hintergrund auf einen Weihnachtsmarkt.

Die bundesweiten Erkenntnisse aus der Aufarbeitung der Mordserie des sogenannten Nationalsozialistischen Untergrunds (NSU) haben eindringlich verdeutlicht, dass aufseiten von Bund und Ländern Handlungsbedarf besteht. Das Bundesgesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) regelt daher den in Politik und Öffentlichkeit stark diskutierten Einsatz von Vertrauenspersonen sowie Verdeckten Mitarbeiterinnen und Mitarbeitern. Die dort formulierten Regelungen sind auch für die Länder wegweisend.

In der aktuellen Sicherheitslage treten zudem besonders die Bedrohungen durch den Rechtsextremismus und -terrorismus in den Vordergrund. Ursächlich für diese Entwicklung ist auch ein verändertes Kommunikationsverhalten, mit dem Rechtsextremisten die Anschlussfähigkeit an die Mitte der Gesellschaft anstreben. Dabei wird in der täglichen Kommunikation und Berichterstattung zunehmend deutlich, dass die Hemmschwellen des Sagbaren gesunken sind. Der steigenden Verbreitung von Hass und Hetze in den sozialen Medien gegenüber Ausländern, Menschen mit Migrationshintergrund, Angehörigen anderer Religionen oder politischer Ansichten und auch Personen des öffentlichen Lebens folgen zunehmend Taten. Vor dem Hintergrund der besorgniserregenden Zahlen, dass 77 Prozent der im Jahr 2018 festgestellten Hasspostings auf rechtsextremem Gedankengut basieren und von den bundesweit aktuell rund 24 000 Rechtsextremisten jeder Zweite vom Verfassungsschutz als gewaltorientiert eingestuft wird, ist eine frühzeitige Kenntnis, Einschätzung und Bekämpfung von rechtsextremistischen Bestrebungen dringend notwendig.

Vordringliche Aufgabe des Staates ist es, die Sicherheit seiner Bürgerinnen und Bürger zu gewährleisten und die Wehrhaftigkeit einer freiheitlichen und demokratischen Gesellschaftsordnung unter Beweis zu stellen. Gefahren und Radikalisierungstendenzen sowie insbesondere politisch motiviertem Extremismus sind mit allen zulässigen Mitteln des demokratischen Rechtsstaates entgegenzutreten. Ebenso ist die zunehmende Bedrohung durch Spionageaktivitäten und Cyber-Attacken fremder Staaten wirksam abzuwehren. Nachrichtendiensten, Polizei und Justiz kommen dabei eine wesentliche Rolle zu. In der Zusammenarbeit der Sicherheitsbehörden hat der Verfassungsschutz die besondere Aufgabe, Bedrohungen für die freiheitliche demokratische Grundordnung bereits im Vorfeld einer konkreten Gefahr zu erkennen und die politisch Verantwortlichen sowie die zuständigen Stellen zu informieren. Der Verfassungsschutz muss durch eine rechtsklare Gesetzgebung in der Lage sein, diese Aufgaben durch wirksame Befugnisse effektiv und zuverlässig zu erfüllen.

Ein effektiver Verfassungsschutz bedarf einer starken und transparenten parlamentarischen Kontrolle. Sie fördert das Vertrauen in die meist klandestine Tätigkeit des Ver-

Druck: Landtag Rheinland-Pfalz, 17. Januar 2020 – Vorabdruck verteilt am 7. November 2019

fassungsschutzes und stärkt die gesellschaftliche Akzeptanz. Die letzte grundlegende Modernisierung der parlamentarischen Kontrolle des Verfassungsschutzes erfolgte in den Jahren 1998 (Landesverfassungsschutzgesetz [LVerfSchG] vom 6. Juli 1998 [GVBl. S. 184], zuletzt geändert durch Artikel 3 des Gesetzes vom 22. Dezember 2015 [GVBl. S. 461], BS 12-2) und 2002 (Neufassung des Ausführungsgesetzes zu Artikel 10 GG und zur Fortentwicklung verfassungsschutzrechtlicher Vorschriften vom 16. Dezember 2002 [GVBl. S. 477]). Es besteht – auch vor dem Hintergrund eines Vergleichs mit der Entwicklung auf Bundesebene und in anderen Bundesländern – Bedarf für eine Fortentwicklung. Das Bundesverfassungsgericht hat in seinen Urteilen zur Antiterrordatei, aber auch zur Onlinedurchsuchung und zum Bundeskriminalamtgesetz (BKA-Gesetz) klare verfassungsrechtliche Grenzen zur Erhebung und Verwendung personenbezogener Daten durch die Sicherheitsbehörden gezogen.

## B. Lösung

Die Verfassungsschutzbehörde in dem fachlich zuständigen Ministerium in Rheinland-Pfalz erhält einen überarbeiteten Rechtsrahmen. Dieser orientiert sich an den Vereinbarungen im aktuellen rheinland-pfälzischen Koalitionsvertrag der Regierungsparteien, wonach das Landesverfassungsschutzgesetz mit Blick auf die Novellen in Bund und anderen Bundesländern zu überprüfen ist. Dabei soll die Arbeit des Verfassungsschutzes effektiviert und die parlamentarische Kontrolle gestärkt werden.

Schwerpunkte sind erweiterte Befugnisse zur Gewinnung relevanter Erkenntnisse, verstärkte parlamentarische Kontrolle sowie Datenschutzregelungen auf Grundlage der Rechtsprechung des Bundesverfassungsgerichts. Im Einzelnen werden die bereits im Rahmen des Polizei- und Ordnungsbehördengesetzes in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. September 2017 (GVBl. S. 237), BS 2012-1, normierten Befugnisse zur Identifizierung und Lokalisierung mobiler Telekommunikationsendgeräte (IMSI-Catcher) sowie zur Funkzellenabfrage auch für die Zwecke des Verfassungsschutzes geregelt. Aufgrund des technologischen Fortschritts und der zunehmenden Kommunikationsmöglichkeiten – auch des Beobachtungsfeldes – über das Internet erhält der Verfassungsschutz eine normenklare Rechtsgrundlage zur Datenerhebung in digitalen Medien. In Zukunft kann der Verfassungsschutz auch Bestandsdaten nach der Abgabenordnung (Kontostammdaten), dem Telekommunikations- und Telemediengesetz abfragen, Personen zur Beobachtung in polizeilichen Informationssystemen ausschreiben und Zugriff auf Videokameraaufnahmen im öffentlich zugänglichen Raum erhalten. Die vom Bundesgesetzgeber normierte Grenze für den Einsatz Verdeckter Mitarbeiterinnen und Mitarbeiter und Vertrauenspersonen wurde weitestgehend in den Gesetzentwurf übernommen.

Die parlamentarische Kontrolle wird darüber hinaus umfassend gestärkt und an die aktuellen Rechtserfordernisse angepasst. Die Mitglieder der Parlamentarischen Kontrollkommission erhalten das Recht, eine sachverständige Person zu beauftragen. Die Zuarbeit durch eine Geschäftsstelle wird gesetzlich verankert. Der Zugang zu Informationen wird verbessert, die Kontrollintensität erhöht. Durch die neu geschaffene Möglichkeit für die Parlamentarische Kontrollkommission, Vorgänge öffentlich zu bewerten und durch die Berichtspflicht der Parlamentarischen Kontrollkommission gegenüber dem Plenum werden Transparenz und demokratische Rückkopplung gestärkt. Die Zahl der Mitglieder und die Zusammensetzung der Parlamentarischen Kontrollkommission werden in Zukunft zu Beginn jeder Wahlperiode durch den Landtag bestimmt. Der Datenschutz wird in Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts zur Antiterrordatei, an das Urteil zur Onlinedurchsuchung sowie an die Entscheidung zum BKA-Gesetz gesetzlich fortgeschrieben. Es wird gesetzlich klargestellt, dass eine gezielte Beobachtung von Minderjährigen unter 14 Jahren grundsätzlich ausscheidet und eine diesbezügliche Verarbeitung personenbezogener Daten nur im Einzelfall und zum Schutz höchster Rechtsgüter unter Beachtung besonderer Prüf- und Löschfristen erfolgt.

## C. Alternativen

Keine.

## D. Kosten

Keine.

Der Landtag Rheinland-Pfalz hat das folgende Gesetz beschlossen:

# Landesverfassungsschutzgesetz (LVerfSchG)

## Inhaltsübersicht


**Teil 1**
**Auftrag**

§ 1 Auftrag
§ 2 Verfassungsschutzbehörde
§ 3 Zusammenarbeit
§ 4 Begriffsbestimmungen

**Teil 2**
**Aufgaben**

§ 5 Beobachtungsaufgaben
§ 6 Mitwirkungsaufgaben
§ 7 Unterrichtung der Landesregierung und der Öffentlichkeit

**Teil 3**
**Befugnisse**

§ 8 Grundsätze
§ 9 Allgemeine Befugnisse
§ 10 Verdeckte Mitarbeiterinnen und Mitarbeiter
§ 11 Vertrauenspersonen
§ 12 Überwachung des Brief-, Post- und Fernmeldeverkehrs
§ 13 Besondere Auskunftsverlangen
§ 14 Funkzellenabfrage
§ 15 Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten
§ 16 Inbesitznahme von Sachen
§ 17 Einsatz technischer Mittel zur akustischen Überwachung außerhalb von Wohnungen
§ 18 Einsatz technischer Mittel zur Wohnraumüberwachung
§ 19 Besondere Bestimmungen für Maßnahmen nach § 18
§ 20 Erhebung und Verarbeitung von Daten aus digitalen Medien
§ 21 Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums
§ 22 Amtshilfe bei Tarnmaßnahmen

**Teil 4**
**Datenverarbeitung**

§ 23 Verarbeitung personenbezogener Daten
§ 24 Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten
§ 25 Informationsübermittlung an die Verfassungsschutzbehörde
§ 26 Informationsübermittlung durch die Verfassungsschutzbehörde
§ 27 Übermittlungsverbote
§ 28 Besondere Pflichten bei der Übermittlung personenbezogener Daten
§ 39 Auskunft an Betroffene
§ 30 Datenschutzkontrolle

**Teil 5**
**Parlamentarische Kontrolle**

§ 31 Parlamentarische Kontrollkommission
§ 32 Beratungen
§ 33 Unterrichtungspflicht der Landesregierung
§ 34 Besondere Kontrollbefugnisse
§ 35 Umfang der Unterrichtungspflicht
§ 36 Geschäftsstelle
§ 37 Eingaben
§ 38 Bericht

**Teil 6**
**Schlussbestimmungen**

§ 39 Geltung des Landesdatenschutzgesetzes
§ 40 Einschränkung von Grundrechten
§ 41 Änderung des Landessicherheitsüberprüfungsgesetzes
§ 42 Änderung des Polizei- und Ordnungsbehördengesetzes
§ 43 Inkrafttreten

## Teil 1
## Auftrag

### § 1
### Auftrag

Der Verfassungsschutz dient dem Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder.

### § 2
### Verfassungsschutzbehörde

(1) Verfassungsschutzbehörde ist eine Abteilung in dem für Inneres zuständigen Ministerium.

(2) Verfassungsschutz und Polizei dürfen einander nicht angegliedert werden.

### § 3
### Zusammenarbeit

(1) Die Verfassungsschutzbehörde ist verpflichtet, mit dem Bund und den Ländern in Angelegenheiten des Verfassungsschutzes zusammenzuarbeiten.

(2) Die Behörden für Verfassungsschutz anderer Länder dürfen in Rheinland-Pfalz unter Beachtung der Bestimmungen dieses Gesetzes nur im Einvernehmen, das Bundesamt für Verfassungsschutz nur im Benehmen mit der Verfassungsschutzbehörde tätig werden. Die Verfassungsschutzbehörde darf nach Maßgabe dieses Gesetzes in den anderen Ländern tätig werden, soweit es die Rechtsvorschriften der betreffenden Länder zulassen.

### § 4
### Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind

1. Bestrebungen gegen den Bestand des Bundes oder eines Landes
   politisch bestimmte, ziel- und zweckgerichtete Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf gerichtet ist, die Freiheit des Bundes oder eines Landes von fremder Herrschaft aufzuheben, ihre staatliche Einheit zu beseitigen oder ein zu ihnen gehörendes Gebiet abzutrennen,
2. Bestrebungen gegen die Sicherheit des Bundes oder eines Landes
   politisch bestimmte, ziel- und zweckgerichtete Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf gerichtet ist, den Bund, ein Land oder deren Einrichtungen in ihrer Funktionsfähigkeit erheblich zu beeinträchtigen;
3. Bestrebungen gegen die freiheitliche demokratische Grundordnung
   politisch bestimmte, ziel- und zweckgerichtete Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf gerichtet ist, einen der in diesem Gesetz genannten Verfassungsgrundsätze zu beseitigen oder außer Geltung zu setzen.

Für einen Personenzusammenschluss handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. Verhaltensweisen von Einzelpersonen, die nicht in einem oder für einen

Personenzusammenschluss handeln, sind Bestrebungen im Sinne dieses Gesetzes, wenn sie gegen Schutzgüter dieses Gesetzes unter Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen.

(2) Verhaltensweisen oder Betätigungen von Personenzusammenschlüssen ohne feste hierarchische Organisationsstrukturen (unorganisierte Gruppen) können Bestrebungen im Sinne dieses Gesetzes sein.

(3) Die freiheitliche demokratische Grundordnung umfasst die zentralen Grundprinzipien, die für den freiheitlichen Verfassungsstaat unentbehrlich sind. Diese sind die Garantie der Menschenwürde, das Demokratieprinzip und das Rechtsstaatsprinzip.

## Teil 2
## Aufgaben

### § 5
### Beobachtungsaufgaben

Die Verfassungsschutzbehörde beobachtet
1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten in der Bundesrepublik Deutschland für eine fremde Macht,
3. Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, und
4. Bestrebungen und Tätigkeiten in der Bundesrepublik Deutschland, die gegen den Gedanken der Völkerverständigung oder das friedliche Zusammenleben der Völker gerichtet sind,

soweit tatsächliche Anhaltspunkte für den Verdacht solcher Bestrebungen oder Tätigkeiten vorliegen. Die Beobachtung erfolgt offen, soweit erforderlich verdeckt. Sie umfasst die gezielte und planmäßige Sammlung und Auswertung sach- und personenbezogener Daten.

### § 6
### Mitwirkungsaufgaben

(1) Die Verfassungsschutzbehörde wirkt mit
1. bei 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,
2. bei der Sicherheitsüberprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen,
3. bei technischen Sicherheitsmaßnahmen zum Schutze von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte und
4. bei der Geheimschutzbetreuung von nichtöffentlichen Stellen.

Bei der Mitwirkung nach Satz 1 Nr. 4 ist die Verfassungsschutzbehörde zur sicherheitsmäßigen Bewertung der An-

gaben der nichtöffentlichen Stelle unter Berücksichtigung der Erkenntnisse der Verfassungsschutzbehörden des Bundes und der Länder befugt. Sofern es im Einzelfall erforderlich erscheint, können bei der Mitwirkung nach Satz 1 Nr. 4 zusätzlich die sonstigen Nachrichtendienste des Bundes um Übermittlung und Bewertung vorhandener Erkenntnisse und um Bewertung übermittelter Erkenntnisse ersucht werden.

(2) Sie wirkt außerdem mit bei der Überprüfung von Personen in sonstigen gesetzlich bestimmten Fällen oder mit deren Einwilligung.

§ 7
Unterrichtung der Landesregierung
und der Öffentlichkeit

(1) Die Verfassungsschutzbehörde unterrichtet die Landesregierung regelmäßig und umfassend über Art und Ausmaß von Bestrebungen und Tätigkeiten nach § 5.

(2) Das fachlich zuständige Ministerium informiert die Öffentlichkeit über grundlegende Angelegenheiten des Verfassungsschutzes sowie über präventiven Wirtschaftsschutz, soweit Geheimhaltungserfordernisse nicht entgegenstehen.

## Teil 3
## Befugnisse

§ 8
Grundsätze

(1) Bei der Erfüllung der Aufgaben hat die Verfassungsschutzbehörde von mehreren möglichen und geeigneten Maßnahmen diejenige zu treffen, die einzelne Personen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht. Eine Maßnahme ist nur so lange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

(2) Sowohl bei der Erhebung als auch bei der Verwertung personenbezogener Daten achtet die Verfassungsschutzbehörde den besonderen Schutz des Kernbereichs privater Lebensgestaltung sowie den Schutz von Berufsgeheimnisträgern und ihnen gleichstehenden Personen.

§ 9
Allgemeine Befugnisse

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben nach § 5, zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge sowie zur Gewinnung, Erhaltung oder Überprüfung der Nachrichtenzugänge die erforderlichen offenen oder die im Sinne des Absatzes 2 verdeckten Maßnahmen treffen, insbesondere Informationen einschließlich personenbezogener Daten nach Maßgabe von Teil 4 verarbeiten, soweit nicht die §§ 10 bis 21 diese besonders regeln. Die Befugnisse gelten entsprechend für die Erfüllung der Aufgaben nach § 6; insoweit sind nur offene Maßnahmen zulässig. Die Maßnahmen sind auch dann zulässig, wenn Dritte unvermeidbar betroffen sind.

(2) Die Verfassungsschutzbehörde darf nach Maßgabe des Absatzes 3 Methoden und Gegenstände einschließlich technischer Mittel zur verdeckten Informationsbeschaffung (nachrichtendienstliche Mittel) einsetzen. Die nachrichtendienstlichen Mittel sind, soweit sie nicht in den §§ 10 bis 21 beson-

ders geregelt sind, in einer Dienstvorschrift zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen regelt. Die Dienstvorschrift ist der Parlamentarischen Kontrollkommission nach § 31 vorzulegen.

(3) Der Einsatz nachrichtendienstlicher Mittel zur Erhebung personenbezogener Daten ist zulässig
1. zur Gewinnung, Erhaltung oder Überprüfung von Nachrichtenzugängen,
2. gegenüber Personen, bei denen aufgrund tatsächlicher Anhaltspunkte der Verdacht von Bestrebungen oder Tätigkeiten nach § 5 vorliegt,
3. gegenüber Personen, von denen aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie für eine nach Nummer 2 betroffene Person oder Personengruppe Mitteilungen entgegennehmen oder weitergeben,
4. gegenüber Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst Bestrebungen oder Tätigkeiten im Sinne des § 5 nachgehen, jedoch tatsächliche hinreichende Anhaltspunkte für eine nicht nur vorübergehende Verbindung zu diesen bestehen oder
5. zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge.

(4) Der Einsatz nachrichtendienstlicher Mittel zur Erhebung personenbezogener Daten bei Minderjährigen ist frühestens ab Vollendung des 10. Lebensjahres und bis zur Vollendung des 14. Lebensjahres nur zu deren Schutz zulässig, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese den objektiven Tatbestand einer der in § 3 Abs. 1 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2007 I S. 154), zuletzt geändert durch Artikel 12 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202), genannten Straftatbestände verwirklichen werden, verwirklichen oder verwirklicht haben.

## § 10
## Verdeckte Mitarbeiterinnen und Mitarbeiter

(1) Die Verfassungsschutzbehörde darf eigene Mitarbeiterinnen und Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende (Verdeckte Mitarbeiterinnen und Mitarbeiter) zur Erfüllung ihrer Aufgaben nach § 5 unter den Voraussetzungen des § 9 Abs. 3 einsetzen.

(2) Verdeckte Mitarbeiterinnen und Mitarbeiter dürfen weder zur Gründung von Personenzusammenschlüssen, die Bestrebungen nach § 5 Satz 1 Nr. 1, 3 oder 4 verfolgen, noch zur steuernden Einflussnahme auf derartige Personenzusammenschlüsse eingesetzt werden. Sie dürfen in solchen Personenzusammenschlüssen oder für solche Personenzusammenschlüsse, einschließlich strafbarer Vereinigungen, tätig werden, um deren Bestrebungen aufzuklären. Im Übrigen dürfen Verdeckte Mitarbeiterinnen oder 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 Nachrichtenzugänge unumgänglich sind und
3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen.

Sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass Verdeckte Mitarbeiterinnen oder Mitarbeiter rechtswidrig einen Straftatbestand von erheblicher Bedeu-

tung verwirklicht haben, soll der Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden. Über Ausnahmen von Satz 4 entscheidet die Leitung der Verfassungsschutzbehörde.

(3) § 9 a Abs. 3 des Bundesverfassungsschutzgesetzes (BVerfSchG) vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 2 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097), gilt entsprechend.

(4) Absatz 1 und 2 sowie § 9 a Abs. 3 BVerfSchG finden entsprechende Anwendung auf solche Mitarbeiterinnen oder Mitarbeiter, die verdeckt Informationen in sozialen Netzwerken und sonstigen Kommunikationsplattformen im Internet erheben, auch wenn sie nicht unter einer auf Dauer angelegten Legende tätig werden.

(5) Über den Einsatz Verdeckter Mitarbeiterinnen und Mitarbeiter wird der Parlamentarischen Kontrollkommission in regelmäßigen Abständen, mindestens jedoch jährlich, umfassend Bericht erstattet.

§ 11
Vertrauenspersonen

(1) Für den Einsatz von Privatpersonen, deren planmäßige, dauerhafte Zusammenarbeit mit dem Verfassungsschutz Dritten nicht bekannt ist (Vertrauenspersonen), ist § 10 Abs. 1 bis 3 und Abs. 5 entsprechend anzuwenden.

(2) Über die Verpflichtung von Vertrauenspersonen entscheidet die Leitung der Verfassungsschutzbehörde. Als Vertrauenspersonen 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 oder eines Landesparlaments oder Mitarbeiterinnen und Mitarbeiter eines solchen Mitglieds sind oder
5. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe wegen eines Vergehens von erheblicher Bedeutung, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

Die Leitung der Verfassungsschutzbehörde kann eine Ausnahme von Nummer 5 zulassen, wenn die Verurteilung nicht als Täterin oder Täter eines Totschlags (§§ 212, 213 des Strafgesetzbuches) oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist und der Einsatz zur Aufklärung von Bestrebungen, die auf die Begehung von in § 3 Abs. 1 des Artikel 10-Gesetzes bezeichneten Straftaten gerichtet sind, unerlässlich ist. Im Falle einer Ausnahme nach Satz 3 ist der Einsatz nach höchstens sechs Monaten zu beenden, wenn er zur Erforschung der in Satz 3 genannten Bestrebungen nicht zureichend gewichtig beigetragen hat. Die Relevanz der gelieferten Informationen ist fortlaufend zu bewerten.

§ 12
Überwachung des Brief-, Post- und Fernmeldeverkehrs

Für die Überwachung des Brief-, Post- und Fernmeldeverkehrs einschließlich der Verarbeitung der durch eine solche Maßnahme erlangten personenbezogenen Daten gelten die Bestimmungen des Artikel 10-Gesetzes in Verbindung mit

dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vom 16. Dezember 2002 (GVBl. S. 477), zuletzt geändert durch Artikel 2 des Gesetzes vom 22. Dezember 2015 (GVBl. S. 461), BS 12-1.

§ 13
Besondere Auskunftsverlangen

(1) Die Verfassungsschutzbehörde darf im Einzelfall bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen unentgeltlich Auskünfte zu Konten, Kontoinhaberinnen und Kontoinhabern, sonstigen Berechtigten und weiteren am Zahlungsverkehr Beteiligten sowie zu Geldbewegungen und Geldanlagen einholen, wenn dies zur Erfüllung ihrer Aufgaben nach § 5 erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 genannten Schutzgüter vorliegen. Sie darf zur Erfüllung ihrer Aufgaben nach § 5 erforderliche Bestandsdaten durch Ersuchen an das Bundeszentralamt für Steuern nach § 93 b Abs. 1 der Abgabenordnung erheben.

(2) Die Verfassungsschutzbehörde darf im Einzelfall bei Verkehrsunternehmen unentgeltlich Auskünfte zu Namen, Anschriften, zur Inanspruchnahme und sonstigen Umständen von Transportleistungen einholen, wenn dies zur Erfüllung ihrer Aufgaben nach § 5 erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 genannten Schutzgüter vorliegen. Zur Auskunft sind ebenso die Betreiber von Computerreservierungssystemen und globalen Distributionssystemen verpflichtet.

(3) Die Verfassungsschutzbehörde darf im Einzelfall zur Erfüllung ihrer Aufgaben nach § 5 unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes bei Personen und Unternehmen, die geschäftsmäßig Postdienstleistungen erbringen, sowie bei denjenigen, die an der Erbringung dieser Dienstleistungen mitwirken, unentgeltlich Auskünfte zu Namen, Anschriften, Postfächern und sonstigen Umständen des Postverkehrs einholen.

(4) Die Verfassungsschutzbehörde darf im Einzelfall zur Erfüllung ihrer Aufgaben nach § 5 unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes bei denjenigen, die geschäftsmäßig Telekommunikationsdienste und Telemediendienste erbringen oder daran mitwirken, Auskünfte einholen über Telekommunikationsverkehrsdaten nach § 96 Abs. 1 Satz 1 Nr. 1 bis 5 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 12 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) und Telemediennutzungsdaten nach § 15 Abs. 1 des Telemediengesetzes (TMG) vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 11 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066). Die Auskünfte können auch in Bezug auf die zukünftige Telekommunikation und die zukünftige Nutzung von Telemedien verlangt werden.

(5) Soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörde nach § 5 erforderlich ist, darf von denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, Auskunft über die nach den §§ 95 und 111 TKG erhobenen Daten verlangt werden (§ 113 Abs. 1 Satz 1 TKG). Bezieht sich das Auskunftsverlangen nach Satz 1 auf 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 TKG), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Auskunft nach Satz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des TKG). Unter den Voraussetzungen des Satzes 1 darf die Verfassungsschutzbehörde auch Auskunft über Daten gemäß § 14 Abs. 1 TMG bei denjenigen verlangen, die Telemediendienste anbieten oder daran mitwirken (§ 14 Abs. 2 TMG).

(6) Soweit gesetzlich nichts anderes bestimmt ist, muss die Verfassungsschutzbehörde ihr Auskunftsverlangen gegenüber den verpflichteten Unternehmen nicht begründen; insbesondere muss sie nicht darlegen, ob und inwieweit die Voraussetzungen der Auskunftsansprüche nach Absatz 1 bis 5 gegeben sind. Die in Absatz 1 bis 3 genannten Unternehmen sind zur unentgeltlichen Auskunft verpflichtet. Aufgrund eines Auskunftsverlangens nach Absatz 4 und 5 haben diejenigen, die geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringen oder daran mitwirken, die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln. Die Verfassungsschutzbehörde hat für ihr erteilte Auskünfte nach Absatz 4 und Absatz 5 Satz 3 eine Entschädigung zu gewähren, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718, 776) in der jeweils geltenden Fassung bemisst; die Bestimmungen über die Verjährung in § 2 Abs. 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechend Anwendung. Die Auskunftsverlangen nach Absatz 1 bis 5 und die Auskunft selbst dürfen den Betroffenen oder Dritten vom Auskunftsgeber nicht mitgeteilt werden.

(7) Auskünfte nach Absatz 1 Satz 1 und Absatz 2 bis 4 dürfen nur auf Antrag eingeholt werden. Der Antrag ist durch die G10-Aufsichtsbeamtin oder den G10-Aufsichtsbeamten im Sinne des § 8 Abs. 3 des Landesgesetzes zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses schriftlich zu stellen und zu begründen. Über den Antrag entscheidet die Leitung der Verfassungsschutzbehörde durch Anordnung. Die fachlich zuständige Ministerin oder der fachlich zuständige Minister unterrichtet die nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildete Kommission unverzüglich über die Anordnungen vor deren Vollzug. Bei Gefahr im Verzug kann die fachlich zuständige Ministerin oder der fachlich zuständige Minister den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen. In diesem Fall hat die Unterrichtung der Kommission unverzüglich nachträglich zu erfolgen. Für die Aufgaben und Befugnisse der Kommission sowie die Mitteilung von Maßnahmen nach Absatz 1 Satz 1 und Absatz 2 bis Absatz 4 an die Betroffenen findet das Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses entsprechende Anwendung.

(8) Auf die Verarbeitung der nach Absatz 1 Satz 1, Absatz 2 bis Absatz 4 und Absatz 5 Satz 3 erhobenen personenbezogenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden.

(9) Über die nach Absatz 5 Satz 3 durchgeführten Maßnahmen unterrichtet die fachlich zuständige Ministerin oder der fachlich zuständige Minister die nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildete Kommission mindestens einmal im Jahr. Die Kommission kann jederzeit Einsicht in alle Unterlagen zu durchgeführten oder laufenden Maßnahmen nach Absatz 5 Satz 3 nehmen und deren Vorlage verlangen.

(10) Das fachlich zuständige Ministerium berichtet über die durchgeführten Maßnahmen nach Absatz 1 Satz 1, Absatz 2 Satz 1 sowie Absatz 3 und 4 dem parlamentarischen Kontrollgremium des Bundes unter entsprechender Anwendung des § 8 b Abs. 3 Satz 1 Halbsatz 2 BVerfSchG für dessen Berichte nach § 8 b Abs. 3 Satz 2 BVerfSchG.

## § 14
## Funkzellenabfrage

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben nach § 5 und unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes Auskunft über Verkehrsdaten ohne Kenntnis der Rufnummer oder einer anderen Kennung des zu überwachenden Anschlusses oder des Endgerätes einholen, sofern andernfalls die Erreichung des Zwecks der Maßnahme erheblich erschwert wäre.

(2) Die Maßnahme bedarf der Anordnung durch die Leitung der Verfassungsschutzbehörde. Die fachlich zuständige Ministerin oder der fachlich zuständige Minister unterrichtet die nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildete Kommission über die beschiedenen Anträge vor deren Vollzug. Bei Gefahr im Verzug kann die fachlich zuständige Ministerin oder der fachlich zuständige Minister den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen. In diesem Fall hat die Unterrichtung der Kommission unverzüglich nachträglich zu erfolgen. Für die Aufgaben und Befugnisse der Kommission sowie die Mitteilung von Maßnahmen nach Absatz 1 an die Betroffenen findet das Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses entsprechende Anwendung.

(3) In der Anordnung sind insbesondere
1. die Voraussetzungen nach Absatz 1 sowie die wesentlichen Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Datenerhebung richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Datenerhebung unter Benennung des Endzeitpunkts und
4. soweit möglich die genaue Telekommunikation, über die Verkehrsdaten erhoben werden soll, räumlich und zeitlich

zu bestimmen. Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Die Verarbeitung der durch Maßnahmen nach Satz 1 erhobenen Daten erfolgt in entsprechender Anwendung des § 4 des Artikel 10-Gesetzes. Hinsichtlich der Mitteilungen gilt § 12 des Artikel 10-Gesetzes entsprechend.

(4) Aufgrund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, unverzüglich Auskünfte über die Verkehrsdaten zu

erteilen. Von der Auskunftspflicht sind auch Verkehrsdaten erfasst, die erst nach der Anordnung anfallen. Ob und in welchem Umfang dafür Vorkehrungen zu treffen sind, richtet sich nach dem Telekommunikationsgesetz und den auf seiner Grundlage erlassenen Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen in den jeweils geltenden Fassungen. Hinsichtlich der Entschädigung gilt § 13 Abs. 6 Satz 4 entsprechend.

§ 15
Identifizierung und Lokalisierung
von mobilen Telekommunikationsendgeräten

(1) Zur Erfüllung ihrer Aufgaben nach § 5 darf die Verfassungsschutzbehörde unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes technische Mittel zur Ermittlung spezifischer Kennungen, insbesondere der Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, oder zur Ermittlung des Standorts eines mobilen Telekommunikationsendgeräts einsetzen.

(2) Personenbezogene Daten Dritter dürfen anlässlich einer Maßnahme nach Absatz 1 nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Über den Datenabgleich zur Ermittlung der Geräte- oder Kartennummer oder des Standorts eines mobilen Telekommunikationsendgeräts hinaus dürfen sie nicht verwendet werden.

(3) § 14 Abs. 2 und 3 findet entsprechende Anwendung.

§ 16
Inbesitznahme von Sachen

Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben nach § 5 vorübergehend Sachen zur Datenerhebung heimlich in Besitz nehmen und benutzen.

§ 17
Einsatz technischer Mittel zur akustischen
Überwachung außerhalb von Wohnungen

(1) Die Verfassungsschutzbehörde darf außerhalb von Wohnungen das nichtöffentlich gesprochene Wort mit verdeckten technischen Mitteln heimlich abhören und aufzeichnen, wenn dies zur Erfüllung ihrer Aufgaben nach § 5 erforderlich ist, tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 genannten Schutzgüter vorliegen und sofern die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(2) § 14 Abs. 2 und 3 gilt entsprechend.

§ 18
Einsatz technischer Mittel
zur Wohnraumüberwachung

(1) Die Verfassungsschutzbehörde darf im Rahmen der Erfüllung ihrer Aufgaben nach § 5 zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, verdeckte technische Mittel zur heimlichen optischen und akustischen Überwachung und Aufzeichnung in Wohnungen einsetzen, sofern die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Eine Maßnahme nach Satz 1 ist auch gegenüber einer Person zulässig, wenn Tatsachen über deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründen, dass sich innerhalb eines überschaubaren Zeitraums eine von ihr ausgehende, in Satz 1 genannte Gefahr realisieren wird.

(2) Die Maßnahme ist auch zulässig, wenn sie ausschließlich zum Schutz der dort für den Verfassungsschutz tätigen Personen erforderlich erscheint und von der Leitung der Verfassungsschutzbehörde angeordnet ist.

(3) Die Maßnahme darf nur in Wohnungen von Personen durchgeführt werden, gegen die aufgrund tatsächlicher Anhaltspunkte der Verdacht von Bestrebungen oder Tätigkeiten nach § 5 besteht. Wohnungen anderer Personen dürfen nur überwacht werden, wenn Tatsachen die Annahme rechtfertigen, dass sich eine Person nach Satz 1 dort aufhält und die Überwachung der Wohnung allein dieser Person zur Erforschung des Sachverhalts nicht Erfolg versprechend erscheint.

(4) Die Maßnahme nach Absatz 1 darf auf Antrag der Leitung der Verfassungsschutzbehörde nur durch ein Gericht angeordnet werden.

(5) Die Anordnung ergeht schriftlich. Sie muss die zu überwachende Wohnung und die Person, gegen die sich die Maßnahme richtet, so genau bezeichnen, wie dies nach den zur Zeit der Anordnung vorhandenen Erkenntnissen möglich ist. Art, Umfang und Dauer der Maßnahmen sind bestimmt zu bezeichnen. Die Anordnung ist auf höchstens einen Monat zu befristen. Verlängerungen um jeweils einen weiteren Monat sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. In der Begründung der Anordnung sind die Voraussetzungen und die wesentlichen Gründe einzelfallbezogen darzustellen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(6) Die Maßnahme darf nur angeordnet und durchgeführt werden, soweit nicht aufgrund tatsächlicher Anhaltspunkte, insbesondere hinsichtlich der Art der überwachten Räumlichkeit und des Verhältnisses der überwachten Personen zueinander, anzunehmen ist, dass durch die Überwachung Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Die Maßnahme ist unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte oder Handlungen erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Für die Entscheidung über die Verwertbarkeit dieser Daten gilt § 3 a Satz 3 bis 6 Artikel 10-Gesetz in Verbindung mit § 2 Abs. 3 des Landesgesetzes zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses entsprechend. Ist die Überwachung nach Satz 2 unterbrochen worden, darf sie unter den in Satz 1 genannten Voraussetzungen fortgeführt werden.

(7) Ein Eingriff in ein nach den §§ 53 und 53 a der Strafprozessordnung (StPO) geschütztes Vertrauensverhältnis ist unzulässig. § 3 b Abs. 2 Artikel 10-Gesetz gilt entsprechend. Satz 1 findet keine Anwendung, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person selbst im Verdacht von Bestrebungen oder Tätigkeiten nach § 5 steht.

### § 19
### Besondere Bestimmungen für Maßnahmen nach § 18

(1) Daten aus dem Kernbereich privater Lebensgestaltung oder aus Eingriffen entgegen § 18 Abs. 7 dürfen vorbehaltlich der Entscheidung nach § 18 Abs. 6 Satz 3 nicht verwertet werden.

Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation ist zu löschen, wenn sie für Zwecke einer etwaigen gerichtlichen Überprüfung nicht mehr erforderlich ist. Soweit die Verarbeitung von Daten nach § 18 der gerichtlichen Kontrolle unterliegt, fällt sie nicht in die Kontrollkompetenz der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

(2) Eine Verwertung der bei einer Maßnahme nach § 18 Abs. 2 erlangten Daten für Zwecke der Abwehr von Gefahren für die öffentliche Sicherheit, insbesondere solcher für die freiheitliche demokratische Grundordnung, ist zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt worden ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen.

(3) Die aus einer Maßnahme nach § 18 gewonnenen personenbezogenen Daten sind zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

(4) Die Leitung der Verfassungsschutzbehörde kann anordnen, dass bei der Übermittlung auf die Kennzeichnung nach Absatz 3 verzichtet wird, soweit und solange dies unerlässlich ist, um die Geheimhaltung einer Beschränkungsmaßnahme nicht zu gefährden und das Gericht zugestimmt hat. Bei Gefahr im Verzug kann die Anordnung bereits vor der Zustimmung getroffen werden. Wird die Zustimmung versagt, ist die Kennzeichnung durch die empfangende Stelle unverzüglich nachzuholen; die übermittelnde Behörde hat sie hiervon zu unterrichten.

(5) Die Verfassungsschutzbehörde kann nach § 18 erhobene personenbezogene Daten an öffentliche Stellen übermitteln, soweit dies zur Erfüllung von deren Aufgaben unter Beachtung des § 26 Abs. 2 Satz 3 erforderlich ist

1. zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr, einer Lebensgefahr oder einer Gefahrenlage gemäß § 18 Abs. 1 Satz 2, oder
2. zur Verfolgung besonders schwerer Straftaten nach § 100 b Abs. 2 StPO, soweit die Daten einen konkreten Ermittlungsansatz erkennen lassen.

Personenbezogene Daten aus einer optischen Wohnraumüberwachung dürfen nicht für Zwecke der Strafverfolgung übermittelt werden. Absatz 2 bleibt unberührt. Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(6) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten der betroffenen oder einer dritten Person in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig, worauf die empfangende Stelle hinzuweisen ist. Über die Übermittlung entscheidet eine Mitarbeiterin oder ein Mitarbeiter der übermittelnden Stelle, die oder der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren.

(7) Sind die durch eine Maßnahme nach § 18 erlangten personenbezogenen Daten zur Erfüllung des der Maßnahme zugrunde liegenden Zwecks und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, sind

sie unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Die Akten sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung folgt, zu vernichten. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung der Maßnahme zurückgestellt ist, dürfen die Daten ohne Einwilligung der oder des Betroffenen nur zu diesem Zweck verwendet werden; die Verarbeitung der Daten ist entsprechend einzuschränken.

(8) Die Betroffenen der Maßnahme sind nach Beendigung zu benachrichtigen, wenn eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Lässt sich zu diesem Zeitpunkt noch nicht abschließend beurteilen, ob diese Voraussetzung erfüllt ist, unterbleibt die Benachrichtigung so lange, bis eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Die Zurückstellung der Benachrichtigung bedarf der gerichtlichen Entscheidung, sofern eine Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme erfolgt ist. Über die Dauer der weiteren Zurückstellungen, die zwölf Monate jeweils nicht überschreiten dürfen, entscheidet das Gericht. Eine abschließende Entscheidung kann frühestens fünf Jahre nach Beendigung der Maßnahme durch das Gericht getroffen werden.

(9) Für gerichtliche Entscheidungen ist das Oberverwaltungsgericht Rheinland-Pfalz zuständig. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung.

### § 20
### Erhebung und Verarbeitung von Daten aus digitalen Medien

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben nach den §§ 5 und 6 zur Erhebung und Verarbeitung von Daten aus öffentlich zugänglichen digitalen Medien die nach pflichtgemäßem Ermessen erforderlichen Maßnahmen treffen, soweit nicht Absatz 2 und 3 diese besonders regeln.

(2) Maßnahmen zur nicht verdeckten Erhebung und Verarbeitung von Daten, die mithilfe einer Legende unter Ausnutzung des schutzwürdigen Vertrauens der betroffenen Person in die Identität und Motivation des Kommunikationspartners durchgeführt werden, sind nur zur Erfüllung von Aufgaben nach § 5 zulässig und bedürfen der Anordnung durch die Leitung der Verfassungsschutzbehörde.

(3) Soweit durch einen verdeckten Zugriff auf zugangsgesicherte digitale Medien oder Endgeräte auf dem hierfür technisch vorgesehenen Weg Informations-, Kommunikations- und sonstige Inhalte erhoben und verarbeitet werden sollen, ohne selbst Kommunikationsadressat und ohne von den an der Kommunikation teilnehmenden oder anderen berechtigten Personen hierzu autorisiert zu sein, sind die Bestimmungen des Artikel 10-Gesetzes sowie des Landesgesetzes zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses entsprechend anzuwenden.

### § 21
### Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben nach § 5 unentgeltlich auf verfügbare Einrichtungen zur Videobeobachtung des öffentlich zugänglichen Raums zu-

greifen. Die Betreiber oder die verfügungsberechtigten Personen haben den Bediensteten der Verfassungsschutzbehörde auf Verlangen unverzüglich Zutritt zu den Räumlichkeiten, in der sich die Einrichtung befindet, zu gewähren und die Mitbenutzung der Einrichtung zu dulden.

(2) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben nach § 5 auf gespeicherte Bild- und Tonaufzeichnungen aus Videoüberwachungen des öffentlich zugänglichen Raums zugreifen, wenn tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 genannten Schutzgüter vorliegen. Die Betreiber haben der Verfassungsschutzbehörde die relevanten Daten auf Verlangen unverzüglich und unentgeltlich zur Verfügung zu stellen. Die Verfassungsschutzbehörde hat die angeforderten Bild- und Tonaufzeichnungen soweit wie möglich nach Datum, Ort und Zeit einzugrenzen und dies dem Betreiber mitzuteilen.

(3) Die überlassenen Bild- und Tonbandaufzeichnungen sind unverzüglich zurückzugeben, zu löschen oder zu vernichten, soweit die Voraussetzungen in Absatz 2 nicht mehr vorliegen oder die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind.

### § 22
### Amtshilfe bei Tarnmaßnahmen

Die zuständigen öffentlichen Stellen des Landes und der kommunalen Gebietskörperschaften leisten der Verfassungsschutzbehörde für ihre Tarnmaßnahmen auf deren Ersuchen unverzüglich Hilfe.

## Teil 4
## Datenverarbeitung

### § 23
### Verarbeitung personenbezogener Daten

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, soweit

1. tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten nach § 5 vorliegen,
2. dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 5 erforderlich ist,
3. dies für die Erfüllung ihrer Aufgaben nach § 6 erforderlich ist,
4. dies zur Gewinnung, Erhaltung oder Überprüfung der Nachrichtenzugänge zu Bestrebungen oder Tätigkeiten nach § 5 erforderlich ist,
5. dies zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge der Verfassungsschutzbehörde gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist oder
6. die oder der Betroffene eingewilligt hat.

Personenbezogene Daten in Dateien, die der Auswertung zur Erfüllung der Aufgaben nach den §§ 5 und 6 dienen, müssen durch Akten oder andere Datenträger belegbar sein. Zur Erfüllung von Aufgaben nach § 6 Abs. 1 Satz 1 Nr. 1 und 2 sowie Abs. 2 dürfen personenbezogene Daten, die für Zwecke nach § 5 erhoben wurden, verarbeitet werden. Im Übrigen muss vorbehaltlich der Regelung in Absatz 4 die Verarbeitung personenbezogener Daten der Erfüllung derselben Aufgabe und dem Schutz derselben Rechtsgüter dienen, welche Gründe für die Erhebung waren. Für die Verwendung von personenbezogenen Daten, die mit Maßnahmen nach § 18

erhoben wurden, müssen im Einzelfall Tatsachen für eine dringende Gefahr für die öffentliche Sicherheit, insbesondere eine gemeine Gefahr, Lebensgefahr oder eine Gefahrenlage im Sinne des § 18 Abs. 1 Satz 2 vorliegen.

(2) Daten über Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst Bestrebungen oder Tätigkeiten nach § 5 nachgehen oder Verbindungen zu solchen haben (Unbeteiligte), dürfen nur dann verarbeitet werden, wenn

1. dies für die Erforschung von Bestrebungen oder Tätigkeiten nach § 5 erforderlich ist,
2. die Erforschung des Sachverhaltes auf andere Weise aussichtslos oder wesentlich erschwert wäre und
3. überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen.

Absatz 1 Satz 4 und 5 gelten entsprechend. Daten Unbeteiligter dürfen auch verarbeitet werden, wenn sie mit zur Erfüllung der Aufgaben nach den §§ 5 und 6 erforderlichen Informationen untrennbar verbunden sind. Daten, die für das Verständnis der zu verarbeitenden Informationen nicht erforderlich sind, sind unverzüglich zu löschen. Dies gilt nicht, wenn die Löschung nicht oder nur mit einem unvertretbaren Aufwand möglich ist; in diesem Falle ist die Verarbeitung der Daten einzuschränken.

(3) Werden personenbezogene Daten mit Kenntnis der Betroffenen erhoben, ist der Erhebungszweck anzugeben. Betroffene sind auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(4) Zur Erfüllung der Aufgaben nach § 5 können personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeitet werden, wenn mindestens vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und die Daten auch für den geänderten gesetzlichen Zweck hätten erhoben werden können. Absatz 1 Satz 5 gilt entsprechend.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verarbeitet werden, dürfen für andere Zwecke nur insoweit verarbeitet werden, als dies zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit, insbesondere für Leib, Leben oder Freiheit einer Person erforderlich ist. Für Daten, die aus Maßnahmen nach § 18 erlangt wurden, müssen im Einzelfall Tatsachen für eine dringende Gefahr für die öffentliche Sicherheit, insbesondere eine gemeine Gefahr, Lebensgefahr oder eine Gefahrenlage im Sinne des § 18 Abs. 1 Satz 2 vorliegen.

## § 24
## Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten

(1) Die Verfassungsschutzbehörde hat in Dateien im Sinne des § 23 Abs. 1 Satz 2 gespeicherte personenbezogene Daten zu berichtigen, wenn sie unrichtig sind; sie sind zu ergänzen, wenn sie unvollständig sind. Gleiches gilt, wenn sie im Einzelfall feststellt, dass in Akten gespeicherte personenbezogene Daten unrichtig oder unvollständig sind.

(2) Die Verfassungsschutzbehörde hat in Dateien im Sinne des § 23 Abs. 1 Satz 2 gespeicherte personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre

Kenntnis für die Erfüllung der Aufgaben nach den §§ 5 und 6 nicht mehr erforderlich ist. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen von Betroffenen beeinträchtigt würden. Die den zu löschenden personenbezogenen Daten entsprechenden Akten oder Aktenbestandteile sind zu vernichten, wenn eine Trennung von anderen Daten, die zur Erfüllung der Aufgaben nach den §§ 5 und 6 weiterhin erforderlich sind, mit vertretbarem Aufwand möglich ist. Absatz 5 Satz 1 bleibt unberührt. Satz 2 bis Satz 4 gilt entsprechend für sonstige Akten, wenn die Verfassungsschutzbehörde die Voraussetzungen nach Satz 1 im Einzelfall feststellt. Die Verarbeitung personenbezogener Daten ist einzuschränken, sofern trotz des Vorliegens für deren Voraussetzungen eine Löschung nach Satz 2 oder eine Vernichtung nach Satz 3 bis Satz 5 nicht vorzunehmen ist.

(3) Die Verfassungsschutzbehörde prüft bei der Einzelfallbearbeitung und nach von ihr festzusetzenden Fristen, in den Fällen des § 5 Satz 1 Nr. 2 und des § 6 spätestens nach fünf Jahren und in den Fällen des § 5 Satz 1 Nr. 1, 3 und 4 spätestens nach drei Jahren, ob in Dateien im Sinne des § 23 Abs. 1 Satz 2 gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Gespeicherte personenbezogene Daten über Bestrebungen und Tätigkeiten nach § 5 Satz 1 Nr. 1, 3 und 4 sind spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, die Leitung der Verfassungsschutzbehörde stellt im Einzelfall fest, dass die weitere Speicherung zur Erfüllung der Aufgaben nach den §§ 5 und 6 oder zur Wahrung schutzwürdiger Interessen Betroffener erforderlich ist.

(4) Die in Dateien oder zu ihrer Person geführten Akten gespeicherten Daten über Minderjährige vor Vollendung des 14. Lebensjahres sind spätestens nach zwei Jahren zu löschen, es sei denn, dass weitere Erkenntnisse nach § 5 angefallen sind. Ab Vollendung des 14. Lebensjahres sind die in Dateien oder zu ihrer Person geführten Akten gespeicherten Daten 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 nach § 5 angefallen sind. Personenbezogene Daten über das Verhalten von Minderjährigen vor Vollendung des 16. Lebensjahres dürfen nach den Bestimmungen dieses Gesetzes nicht an ausländische oder über- oder zwischenstaatliche Stellen übermittelt werden.

(5) Eine Vernichtung von Akten erfolgt nicht, wenn sie nach den Bestimmungen des Landesarchivgesetzes (LArchG) vom 5. Oktober 1990 (GVBl. S. 277), zuletzt geändert durch Gesetz vom 27. November 2015 (GVBl. S. 383), BS 224-10, dem Landesarchiv zur Übernahme anzubieten und zu übergeben sind. Die Beschränkung der Sperrfrist in § 3 Abs. 3 Satz 5 LArchG kann aufgehoben werden, soweit die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister erklärt, dass das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten würde. Eine Entscheidung über die Aufhebung der Beschränkung ergeht im Einvernehmen mit der für das Archivwesen zuständigen Ministerin oder dem für das Archivwesen zuständigen Minister.

§ 25
Informationsübermittlung
an die Verfassungsschutzbehörde

(1) Die öffentlichen Stellen des Landes und der kommunalen Gebietskörperschaften übermitteln von sich aus der Verfassungsschutzbehörde Informationen, soweit nach ihrer Beurteilung tatsächliche Anhaltspunkte dafür bestehen, dass diese für die Erfüllung der Aufgaben nach § 5 erforderlich sind.

(2) Die Verfassungsschutzbehörde kann über alle Angelegenheiten, deren Kenntnis zur Erfüllung ihrer Aufgaben nach den §§ 5 und 6 erforderlich ist, von den öffentlichen Stellen des Landes und den kommunalen Gebietskörperschaften Informationen und die Vorlage von Unterlagen verlangen. Das Ersuchen braucht nicht begründet zu werden; die Verfassungsschutzbehörde trägt die Verantwortung für dessen Rechtmäßigkeit. Ein Ersuchen soll nur dann gestellt werden, wenn die Informationen nicht aus allgemein zugänglichen Quellen oder nur mit übermäßigem Aufwand oder nur durch eine die Betroffenen stärker belastende Maßnahme erhoben werden können. Die ersuchten Stellen haben die verlangten Informationen unverzüglich und unentgeltlich zur Verfügung zu stellen.

(3) Bestehen nur allgemeine, nicht auf konkrete Fälle bezogene tatsächliche Anhaltspunkte nach § 5, so kann die Verfassungsschutzbehörde die Übermittlung von Informationen einschließlich personenbezogener Daten von öffentlichen Stellen des Landes und der kommunalen Gebietskörperschaften nur verlangen, soweit dies erforderlich ist zur Aufklärung von Tätigkeiten nach § 5 Satz 1 Nr. 2 sowie von Bestrebungen und Tätigkeiten, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die Schutzgüter nach § 5 Satz 1 Nr. 1, Nr. 3 oder Nr. 4 gerichtet sind. Die Verfassungsschutzbehörde kann auch Einsicht in die amtlichen Dateien und sonstigen Informationsbestände nehmen, soweit dies zur Aufklärung der in Satz 1 genannten Tätigkeiten oder Bestrebungen zwingend erforderlich ist und durch eine andere Art der Übermittlung der Zweck der Maßnahme gefährdet oder Betroffene unverhältnismäßig beeinträchtigt würden. Die Übermittlung personenbezogener Daten ist auf Name, Anschrift, Tag und Ort der Geburt, Staatsangehörigkeit sowie auf im Einzelfall durch die Verfassungsschutzbehörde festzulegende Merkmale zu beschränken.

(4) Die Übermittlung personenbezogener Daten, die aufgrund einer Maßnahme nach § 100 a StPO bekannt geworden sind, ist für Zwecke der Aufgabenerfüllung nach diesem Gesetz nur dann zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass jemand eine der in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat. Auf deren Verwertung durch die Verfassungsschutzbehörde findet § 4 des Artikel 10-Gesetzes entsprechende Anwendung.

(5) Die Verfassungsschutzbehörde darf anstelle eines Verlangens nach Absatz 2 oder § 18 Abs. 3 Satz 2 BVerfSchG automatisierte Abrufverfahren nutzen, soweit die Nutzung eines automatisierten Abrufverfahrens durch die Verfassungsschutzbehörden und das diesbezügliche Verfahren ausdrücklich gesetzlich geregelt sind. Die Einrichtung eines automatisierten Abrufverfahrens wird von der Leitung der Verfassungsschutzbehörde angeordnet.

(6) Die Verfassungsschutzbehörde kann Personen sowie die von ihr benutzten oder eingesetzten Kraftfahrzeuge zur Mitteilung über das Antreffen in dem polizeilichen Informationssystem ausschreiben, wenn dies zur Erfüllung ihrer Aufgaben nach § 5 erforderlich ist. Eine polizeiliche Aufgabenwahrnehmung wird dadurch nicht veranlasst. Die Polizei übermittelt Erkenntnisse zum Antreffen der Person oder Feststellen des Kraftfahrzeugs an die Verfassungsschutzbehörde. Die Ausschreibung ist gegenüber der betroffenen Person sowie Dritten geheim zu halten. Die Maßnahme nach Satz 1 darf nur durch die Leitung der Verfassungsschutzbehörde angeordnet werden. Die Maßnahme ist auf höchstens sechs Monate zu befristen. Die Verlängerung der Maßnahme um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Liegen die Voraussetzungen für die Ausschreibung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung unverzüglich zu löschen.

(7) Vorschriften zur Informationsübermittlung an die Verfassungsschutzbehörde nach anderen Gesetzen bleiben unberührt.

§ 26
Informationsübermittlung
durch die Verfassungsschutzbehörde

(1) Die Verfassungsschutzbehörde darf an öffentliche Stellen personenbezogene Daten zur Erfüllung von Aufgaben im Sinne der §§ 5 und 6 übermitteln, soweit gesetzlich nichts anderes bestimmt ist. Die empfangende Stelle darf personenbezogene Daten nur zu dem Zweck verarbeiten, zu dem sie ihr übermittelt wurden, soweit gesetzlich nichts anderes bestimmt ist und eine von der Verfassungsschutzbehörde mitgeteilte Verarbeitungsbeschränkung nicht entgegensteht.

(2) Für andere Aufgaben darf die Verfassungsschutzbehörde, soweit gesetzlich nichts anderes bestimmt ist, personenbezogene Daten, welche mit nachrichtendienstlichen Mitteln erhoben wurden, nur übermitteln an

1. die Dienststellen der Stationierungsstreitkräfte im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. 1961 II S. 1183 – 1218 –), geändert durch Abkommen vom 18. März 1993 (BGBl. 1994 II S. 2594),
2. die Staatsanwaltschaften und die Polizeibehörden zur Verfolgung von Staatsschutzdelikten, den in § 100 a StPO und § 131 des Strafgesetzbuches genannten Straftaten und sonstigen Straftaten im Rahmen der organisierten Kriminalität; Staatsschutzdelikte sind die in den §§ 74 a und 120 des Gerichtsverfassungsgesetzes genannten Straftaten sowie sonstige Straftaten, bei denen aufgrund ihrer Zielsetzung, des Motivs der Täterin oder des Täters oder der Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, dass sie gegen die in Artikel 73 Nr. 10 Buchst. b oder Buchst. c des Grundgesetzes (GG) genannten Schutzgüter gerichtet sind,
3. die Polizeibehörden, soweit sie gefahrenabwehrend tätig sind, wenn dies zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich ist und die Übermittlung der Ab-

wehr einer im Einzelfall bestehenden erheblichen Gefahr oder der vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung gemäß § 28 Abs. 3 des Polizei- und Ordnungsbehördengesetzes in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. September 2017 (GVBl. S. 237), BS 2012-1, dient, oder

4. andere öffentliche Stellen, wenn die empfangende Stelle die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für erhebliche Zwecke der öffentlichen Sicherheit sowie des Jugendschutzes benötigt.

Eine Datenübermittlung ist auch zulässig zum Schutz der Mitarbeiterinnen und Mitarbeiter der vorgenannten Stellen. Die Übermittlung ist in den Fällen der Nummern 2 und 3 nur zulässig, wenn der mit der Verarbeitung der übermittelten personenbezogenen Daten beim Datenempfänger verfolgte Zweck eine Neuerhebung durch die empfangende Stelle mit vergleichbaren Mitteln rechtfertigen würde. Absatz 5 bleibt unberührt.

(3) Personenbezogene Daten, welche nicht mit nachrichtendienstlichen Mitteln erhoben wurden, darf die Verfassungsschutzbehörde an öffentliche Stellen übermitteln, soweit dies für die Aufgabenwahrnehmung der empfangenden Stelle oder zum Schutz von Mitarbeiterinnen und Mitarbeitern erforderlich ist.

(4) Die Verfassungsschutzbehörde erteilt Auskunft einschließlich personenbezogener Daten aus vorhandenen Datenbeständen über gerichtsverwertbare Tatsachen in den Fällen der Mitwirkung im Sinne von § 6 Abs. 2.

(5) Die Verfassungsschutzbehörde darf personenbezogene Daten an ausländische Nachrichtendienste angrenzender Staaten, an andere ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung ihrer Aufgaben nach den §§ 5 und 6 oder zur Wahrung erheblicher Sicherheitsinteressen der empfangenden Stelle erforderlich ist. Die Übermittlung an ausländische Nachrichtendienste geschieht im Einvernehmen mit dem Bundesamt für Verfassungsschutz. Sie unterbleibt in allen Fällen, in denen auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen Betroffener entgegenstehen. Die Übermittlung ist aktenkundig zu machen. Die empfangende Stelle ist darauf hinzuweisen, dass die übermittelten personenbezogenen Daten nur zu dem Zweck genutzt werden dürfen, zu dem sie ihr übermittelt wurden und sich die Verfassungsschutzbehörde vorbehält, Auskunft über die Nutzung der personenbezogenen Daten zu verlangen.

(6) Personenbezogene Daten dürfen an nichtöffentliche Stellen nur übermittelt werden, wenn dies

1. zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen im Sinne des Landessicherheitsüberprüfungsgesetzes,
2. zur Abwehr sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht,
3. zum Schutz der Volkswirtschaft vor sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten oder vor der planmäßigen Unterwanderung von Wirtschaftsunternehmen

durch die in § 4 Abs. 1 Satz 1 Nr. 2 und 3 genannten Bestrebungen oder

4. zum Schutz von Leib, Leben, Freiheit einer Person

erforderlich ist. Die Übermittlung bedarf der Zustimmung der Leitung der Verfassungsschutzbehörde. Sie ist aktenkundig zu machen. Die empfangende Stelle ist darauf hinzuweisen, dass die übermittelten personenbezogenen Daten nur zu dem Zweck genutzt werden dürfen, zu dem sie ihr übermittelt wurden, und dass die Verfassungsschutzbehörde sich vorbehält, Auskunft über die Verarbeitung der personenbezogenen Daten zu verlangen.

(7) Bei der Übermittlung von Informationen an die Öffentlichkeit nach § 7 Abs. 2 dürfen auch personenbezogene Daten bekannt gegeben werden, wenn die Bekanntgabe für das Verständnis des Zusammenhangs oder der Darstellung von Bestrebungen und Tätigkeiten nach § 5 erforderlich ist und das öffentliche Interesse an der Bekanntgabe das schutzwürdige Interesse der betroffenen Person überwiegt.

(8) Vorschriften zur Informationsübermittlung durch die Verfassungsschutzbehörde nach anderen Gesetzen bleiben unberührt.

## § 27
## Übermittlungsverbote

Die Übermittlung von personenbezogenen Daten nach den §§ 25 und 26 unterbleibt, soweit

1. für die übermittelnde Stelle erkennbar ist, dass die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen,
2. überwiegende Sicherheitsinteressen dies erfordern, insbesondere der Schutz von Nachrichtenzugängen und operativen Maßnahmen oder sonstige Geheimhaltungsgründe entgegenstehen oder
3. besondere gesetzliche Übermittlungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

## § 28
## Besondere Pflichten bei der Übermittlung personenbezogener Daten

(1) Erweisen sich personenbezogene Daten nach ihrer Übermittlung nach den Bestimmungen dieses Gesetzes als unvollständig oder unrichtig, so sind sie unverzüglich gegenüber der empfangenden Stelle zu berichtigen, es sei denn, hierfür besteht keine sachliche Notwendigkeit. Die Berichtigung ist zu vermerken.

(2) Die empfangende Stelle prüft, ob die nach den Bestimmungen dieses Gesetzes übermittelten personenbezogenen Daten für die Erfüllung ihrer Aufgaben erforderlich sind. Ergibt die Prüfung, dass sie nicht erforderlich sind, hat sie die Unterlagen zu vernichten. Die Vernichtung kann unterbleiben, wenn die Trennung von anderen personenbezogenen Daten, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist, in diesem Fall ist die Verarbeitung der personenbezogenen Daten insoweit einzuschränken.

§ 29
Auskunft an Betroffene

(1) Die Verfassungsschutzbehörde erteilt Betroffenen über zu ihrer Person in Akten und Dateien im Sinne des § 23 Abs. 1 Satz 2 gespeicherte Daten sowie über den Zweck und die Rechtsgrundlage für deren Verarbeitung auf Antrag unentgeltlich Auskunft. Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und auf die empfangende Stelle bei Übermittlungen. Über personenbezogene Daten in nichtautomatisierten Dateien und Akten, die nicht zur Person von Betroffenen geführt werden, ist Auskunft nur zu erteilen, soweit Angaben gemacht werden, die ein Auffinden der personenbezogenen Daten mit angemessenem Aufwand ermöglichen. Ein Recht auf Akteneinsicht besteht nicht.

(2) Die Auskunftserteilung unterbleibt, soweit
1. durch sie eine Gefährdung der Aufgabenerfüllung zu besorgen ist,
2. durch sie Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise der Verfassungsschutzbehörde zu befürchten ist,
3. sie die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen Dritter geheimgehalten werden müssen.

Die Entscheidung trifft die Leitung der Verfassungsschutzbehörde oder eine von dieser hierzu besonders beauftragte Person.

(3) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Die Gründe der Auskunftsverweigerung sind aktenkundig zu machen. Wird die Auskunftserteilung abgelehnt, sind Betroffene auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit wenden können. Mitteilungen der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit an Betroffene dürfen keine Rückschlüsse auf den Erkenntnisstand der Verfassungsschutzbehörde zulassen, sofern diese nicht einer weitergehenden Auskunft zugestimmt hat.

§ 30
Datenschutzkontrolle

(1) Der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit obliegt die Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen aus diesem Gesetz sowie aus anderen für die Verfassungsschutzbehörde geltenden Gesetzen. Soweit die Einhaltung von Bestimmungen der Kontrolle durch die Kommission nach § 31 oder durch die nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildete Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten, es sei denn, die betreffende Kommission ersucht die Landesbeauftragte oder den Landesbeauftragten, die Einhaltung der Bestimmungen über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(2) Zur Ausübung der Kontrolle ist der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit auf Verlangen Zutritt zu den Diensträumen zu gewähren. Ihr oder ihm ist ferner Auskunft zu erteilen und Einsicht in alle Dateien, Akten und sonstige Unterlagen zu gewähren, soweit nicht die fachlich zuständige Ministerin oder der fachlich zuständige Minister im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet wird.

(3) Die Befugnis nach Absatz 2 erstreckt sich auf Weisung und unter der Aufsicht der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit auch auf deren oder dessen Bedienstete, soweit für diese eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 12 des Landessicherheitsüberprüfungsgesetzes vom 8. März 2000 (GVBl. S. 70, BS 12-3) in der jeweils geltenden Fassung durchgeführt worden ist.

## Teil 5
## Parlamentarische Kontrolle

### § 31
### Parlamentarische Kontrollkommission

(1) Die Landesregierung unterliegt hinsichtlich der Tätigkeit der Verfassungsschutzbehörde der parlamentarischen Kontrolle durch die Parlamentarische Kontrollkommission. Die Rechte des Landtags, seiner Ausschüsse und der nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildeten Kommission bleiben unberührt.

(2) Der Landtag bestimmt zu Beginn jeder Wahlperiode die Zahl der Mitglieder der Parlamentarischen Kontrollkommission und ihre Zusammensetzung. Er wählt die Mitglieder der Parlamentarischen Kontrollkommission aus seiner Mitte. Gewählt ist, wer die Stimmen der Mehrheit der Mitglieder des Landtags auf sich vereint. Scheidet ein Mitglied aus dem Landtag oder aus seiner Fraktion aus oder wird es Mitglied der Landesregierung, verliert es seine Mitgliedschaft in der Parlamentarischen Kontrollkommission. Für dieses Mitglied ist unverzüglich ein neues zu wählen. Das Gleiche gilt, wenn aus sonstigen Gründen ein Mitglied aus der Parlamentarische Kontrollkommission ausscheidet.

(3) Die Parlamentarische Kontrollkommission übt die Kontrolle auch über das Ende der Wahlperiode hinaus so lange aus, bis der nachfolgende Landtag die Mitglieder gemäß Abs. 2 gewählt hat.

(4) In ihrer konstituierenden Sitzung wählt die Parlamentarische Kontrollkommission eine Vorsitzende oder einen Vorsitzenden sowie deren oder dessen Vertreterin oder Vertreter und gibt sich eine Geschäftsordnung.

### § 32
### Beratungen

(1) Die Parlamentarische Kontrollkommission soll mindestens alle drei Monate zusammentreten. Darüber hinaus hat die oder der Vorsitzende die Parlamentarische Kontrollkommission unverzüglich einzuberufen, wenn es eines ihrer Mitglieder oder die Verfassungsschutzbehörde verlangt.

(2) Die Beratungen der Parlamentarischen Kontrollkommission sind geheim. Die Mitglieder der Kommission sowie das Personal der Geschäftsstelle nach § 36 sind zur Geheimhaltung

sämtlicher Angelegenheiten verpflichtet, die ihnen hinsichtlich der Tätigkeit der Parlamentarischen Kontrollkommission bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden.

(3) Absatz 2 gilt nicht für Bewertungen bestimmter Vorgänge durch die Parlamentarische Kontrollkommission, wenn ein erhebliches öffentliches Interesse an der Veröffentlichung naheliegt und eine Mehrheit von mindestens zwei Dritteln ihrer Mitglieder nach Anhörung der Landesregierung in die Veröffentlichung der Bewertung eingewilligt hat. Den die Bewertung nicht stützenden Kommissionsmitgliedern ist es erlaubt, der Kommission eine abweichende Bewertung vorzulegen, die zu veröffentlichen ist.

(4) Soweit für die jeweiligen Bewertungen eine Sachverhaltsdarstellung unerlässlich ist, ist den Belangen des Geheimschutzes unter Berücksichtigung der Maßgaben des § 35 Abs. 2 Satz 1 Rechnung zu tragen.

§ 33
Unterrichtungspflicht der Landesregierung

(1) Die Landesregierung unterrichtet die Parlamentarische Kontrollkommission im Abstand von höchstens sechs Monaten umfassend über die allgemeine Tätigkeit der Verfassungsschutzbehörde. Über Vorgänge von besonderer Bedeutung unterrichtet sie unverzüglich. Auf Verlangen eines Mitglieds hat sie auch über sonstige Vorgänge zu berichten.

(2) Die Unterrichtung umfasst auch die Überwachung des Brief-, Post- und Fernmeldeverkehrs nach § 12 und die Einholung von Auskünften nach § 13 Abs. 1 bis 4. Es ist ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben.

(3) Über den nach §§ 10 und 11 erfolgten Einsatz Verdeckter Mitarbeiterinnen und Mitarbeiter sowie Vertrauenspersonen, den erfolgten Einsatz technischer Mittel zur Wohnraumüberwachung nach § 18 Abs. 1 und, soweit gemäß § 19 Abs. 2 richterlich überprüfungsbedürftig, nach § 18 Abs. 2 unterrichtet die Landesregierung den Landtag jährlich. Die parlamentarische Kontrollkommission übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus.

(4) Die übrigen in diesem Gesetz geregelten Unterrichtungspflichten bleiben unberührt.

§ 34
Besondere Kontrollbefugnisse

(1) Im Rahmen ihres Kontrollrechts ist den Mitgliedern der Parlamentarischen Kontrollkommission auf ihr Verlangen Einsicht in Akten, Schriftstücke oder Dateien der Verfassungsschutzbehörde zu gewähren.

(2) Den Mitgliedern der Parlamentarischen Kontrollkommission ist jederzeit Zutritt zur Verfassungsschutzbehörde zu gewähren.

(3) Die Mitglieder der Parlamentarischen Kontrollkommission können Angehörige der Verfassungsschutzbehörde sowie das für die Tätigkeit der Verfassungsschutzbehörde zuständige Mitglied der Landesregierung befragen.

(4) Zur Wahrnehmung ihrer Kontrollaufgaben kann die Parlamentarische Kontrollkommission mit einer Mehrheit von zwei Dritteln ihrer Mitglieder nach Anhörung der Landes-

regierung im Einzelfall eine sachverständige Person mit einer bestimmt zu bezeichnenden Untersuchung beauftragen. Die oder der Sachverständige hat der Parlamentarischen Kontrollkommission über das Ergebnis der Untersuchungen zu berichten. § 32 Abs. 2, § 34 Abs. 1 und 2, § 34 Abs. 3 Alternative 1 und § 35 gelten entsprechend. § 36 Satz 5 gilt entsprechend, soweit im Zuge der Untersuchung vorgesehen ist, dass von der sachverständigen Person geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse zur Kenntnis genommen werden.

§ 35
Umfang der Unterrichtungspflicht

(1) Die Verpflichtung der Landesregierung zur Unterrichtung nach diesem Gesetz erstreckt sich nur auf Informationen und Gegenstände, die der Verfügungsberechtigung der Verfassungsschutzbehörde unterliegen.

(2) Soweit es aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig ist oder der Kernbereich exekutiver Eigenverantwortung betroffen ist, kann die Landesregierung sowohl die Unterrichtung nach § 33 als auch die Erfüllung von Verlangen nach § 34 Abs. 1 verweigern sowie den in § 34 Abs. 3 genannten Personen die Erteilung der Auskunft untersagen. Macht die Landesregierung hiervon Gebrauch, hat sie dies der Parlamentarischen Kontrollkommission gegenüber zu begründen.

§ 36
Geschäftsstelle

Der Parlamentarischen Kontrollkommission wird eine beim Landtag gesondert einzurichtende Geschäftsstelle zugeordnet. Aufgabe der Geschäftsstelle ist es, die Tätigkeit der Parlamentarischen Kontrollkommission zu koordinieren und sie in der Ausübung ihrer Kontrollbefugnisse zu unterstützen. Sie wird von einer Beamtin oder einem Beamten geleitet, die oder der die Befähigung zum Richteramt besitzt. Die Leiterin oder der Leiter der Geschäftsstelle sowie das weitere zugeordnete Personal werden im Auftrag der Parlamentarischen Kontrollkommission tätig und sind insoweit nur dieser unterstellt. Vor der Aufnahme seiner Tätigkeit in der Geschäftsstelle ist für das Personal eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 12 des Landessicherheitsüberprüfungsgesetzes vom 8. März 2000 (GVBl. S. 70, BS 12-3) in der jeweils geltenden Fassung durchzuführen.

§ 37
Eingaben

(1) Angehörigen der Verfassungsschutzbehörde ist es gestattet, sich in dienstlichen Angelegenheiten, jedoch nicht im eigenen oder im Interesse anderer Angehöriger dieser Behörde, ohne Einhaltung des Dienstweges unmittelbar an die Parlamentarische Kontrollkommission zu wenden. Wegen der Tatsache der Eingabe dürfen sie dienstlich weder gemaßregelt oder sonst benachteiligt werden. Die Parlamentarische Kontrollkommission übermittelt die Eingaben der Landesregierung zur Stellungnahme. Den Namen der mitteilenden Person gibt sie nur bekannt, soweit dies zur Aufklärung des Sachverhalts erforderlich scheint.

(2) An den Landtag gerichtete Eingaben von Bürgerinnen und Bürgern über ein sie betreffendes Verhalten der Verfassungsschutzbehörde sind der Parlamentarischen Kontrollkommission zur Kenntnis zu geben.

§ 38
Bericht

Die Parlamentarische Kontrollkommission erstattet dem Landtag möglichst in der Mitte und am Ende jeder Wahlperiode Bericht über ihre Kontrolltätigkeit. Über die Einholung von Auskünften nach § 13 Abs. 1 bis 4 berichtet die Parlamentarische Kontrollkommission dem Landtag jährlich. Der Bericht enthält Angaben zur Durchführung der Maßnahmen sowie Art, Umfang und Anordnungsgründen. Dabei sind die Grundsätze des § 32 Abs. 2 zu beachten.

**Teil 6**
**Schlussbestimmungen**

§ 39
Geltung des Landesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach den §§ 5 und 6 durch die Verfassungsschutzbehörde findet das Landesdatenschutzgesetz (LDSG) vom 8. Mai 2018 (GVBl. S. 93, BS 204-1) keine Anwendung. Die §§ 14, 15, 27, 33 Abs. 1 bis Abs. 4, 34, 35, 37 Abs. 1 bis Abs. 4, 38 Abs. 1 bis Abs. 4 und Abs. 6, 39, 42 Abs. 1, 51, 53 LDSG gelten entsprechend.

§ 40
Einschränkung von Grundrechten

Aufgrund dieses Gesetzes können das Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG und Artikel 4 a der Verfassung für Rheinland-Pfalz, das Grundrecht auf Unverletzlichkeit der Wohnung aus Artikel 13 GG und Artikel 7 der Verfassung für Rheinland-Pfalz sowie das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses aus Artikel 10 GG und Artikel 14 der Verfassung für Rheinland-Pfalz eingeschränkt werden.

§ 41
Änderung
des Landessicherheitsüberprüfungsgesetzes

Das Landessicherheitsüberprüfungsgesetz vom 8. März 2000 (GVBl. S. 70), zuletzt geändert durch Artikel 4 des Gesetzes vom 22. Dezember 2015 (GVBl. S. 461), BS 12-3, wird wie folgt geändert:

§ 4 Abs. 3 erhält folgende Fassung:

„(3) Mitwirkende Behörde bei der Sicherheitsüberprüfung ist die Verfassungsschutzbehörde im Sinne des § 2 des Landesverfassungsschutzgesetzes (LVerfSchG) vom *[Datum]* 2019 (GVBl. S. *[...]*), BS *[...-.]*; sie wird nur auf Ersuchen der zuständigen Stelle tätig.“

§ 42
Änderung
des Polizei- und Ordnungsbehördengesetzes

Das Polizei- und Ordnungsbehördengesetz in der Fassung vom 10. November 1993 (GVBl. S. 595), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. September 2017 (GVBl. S. 237), BS 2012-1, wird wie folgt geändert:

§ 29 Abs. 8 Satz 3 erhält folgende Fassung:

„§ 31 Abs. 1 Satz 2, § 31 Abs. 2 bis 4 und § 32 Abs. 2 und 3 des Landesverfassungsschutzgesetzes gelten entsprechend.“

§ 43
Inkrafttreten

(1) Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

(2) Gleichzeitig tritt das Landesverfassungsschutzgesetz vom 6. Juli 1998 (GVBl. S. 184), zuletzt geändert durch Artikel 3 des Gesetzes vom 22. Dezember 2015 (GVBl. S. 461), BS 12-2, außer Kraft.

# Begründung

## A. Allgemeines

Das geltende Landesverfassungsschutzgesetz (LVerfSchG) stammt hinsichtlich des Grundtextes sowie der Systematik aus dem Jahre 1998 (GVBl. 1998, S. 184, BS 12-2). In der Zwischenzeit wurde das Gesetz mehrfach durch Änderungsgesetze, zuletzt durch Artikel 3 des Gesetzes vom 22. Dezember 2015 (GVBl. S. 461), angepasst. Der vorliegende Gesetzentwurf sieht einen modifizierten Rechtsrahmen für den rheinland-pfälzischen Verfassungsschutz vor, der Schwerpunkte bei erweiterten Befugnissen, einer gestärkten parlamentarischen Kontrolle sowie beim Datenschutz setzt. Die bereits in der Inhaltsübersicht zum Ausdruck kommende Schwerpunktsetzung stützt sich dabei auf die Vereinbarung der rheinland-pfälzischen Koalitionsparteien, einen Rechtsvergleich jüngerer Gesetzesnovellen in Bund und Ländern vorzunehmen sowie die parlamentarische Kontrolle des Verfassungsschutzes zu stärken (vgl. Koalitionsvertrag 2016 bis 2021, S. 84).

Der vorliegende Gesetzentwurf berücksichtigt im Rahmen der Aufgabenerfüllung die Verhältnismäßigkeit im Hinblick auf die zu schützenden Belange einer freiheitlichen Gesellschaft, in der sich Bürgerinnen und Bürger nach ihrem Belieben frei entfalten können sowie das Sicherheitsbedürfnis der Menschen als Voraussetzung des freiheitlichen und friedlichen Zusammenlebens in besonderem Maße. Besonders eingriffsintensive Maßnahmen werden an besonders restriktive Voraussetzungen geknüpft und nur zum Schutze der höchsten Rechtsgüter von Verfassungsrang zugelassen.

Die dem Verfassungsschutz im Rahmen des gesetzlichen Auftrags eingeräumten Befugnisse zur Erhebung personenbezogener Daten im Vorfeld konkreter Gefahren werden unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) normiert. Gleiches gilt für die Verarbeitung personenbezogener Daten. Die Entscheidungen des Bundesverfassungsgerichtes (BVerfG) zur Antiterrordatei (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07) sowie zur Onlinedurchsuchung (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07) werden berücksichtigt. Die jüngere Entscheidung des BVerfG zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) findet Beachtung, soweit keine bereichsspezifischen Besonderheiten für das Recht der Nachrichtendienste existieren (vgl. hierzu BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 116-122). Das BVerfG hat in der Entscheidung zum BKA-Gesetz die Zulässigkeit polizeilicher Überwachungsmaßnahmen im Vorfeld präzisiert und die verdeckte Datenerhebung durch die Polizei bereits im Vorfeld konkreter Terrorgefahren und zur Verhütung terroristischer Straftaten zugelassen. Gerade für den Verfassungsschutz gelten die bundesverfassungsgerichtlich zugestandenen Befugnisse im Vorfeld konkreter Terrorgefahren insoweit uneingeschränkt. Als nachrichtendienstliche Gefahrenerforschungsbehörde ist Hauptaufgabe die verdeckte Vorfeldaufklärung extremistischer und terroristischer Bestrebungen.

Neben der Änderung des Gesetzesaufbaus sowie redaktionellen Anpassungen sieht der Gesetzentwurf folgende wesentlichen Neuerungen vor:

1. In § 4 Abs. 2 wird ergänzend klargestellt, dass Verhaltensweisen oder Betätigungen von Personen ohne feste hierarchische Organisationsstruktur (unorganisierte Gruppen) Bestrebungen im Sinne dieses Gesetzes sein können.

2. In § 4 Abs. 3 werden die zentralen Grundprinzipien der freiheitlichen demokratische Grundordnung einfachgesetzlich geregelt. Das BVerfG hat im jüngsten NPD-Verbotsverfahren die Menschenwürde, das Rechtsstaatsprinzip sowie das Demokratieprinzip als die zentralen Grundprinzipien der freiheitlichen demokratischen Grundordnung benannt (vgl. BVerfG, Urteil vom 17. Januar 2017, 2 BvB 1/13).

3. In § 5 Satz 2 wird klargestellt, dass die Beobachtung durch den Verfassungsschutz grundsätzlich offen, erforderlichenfalls verdeckt erfolgt.

4. In § 6 Abs. 2 werden Überprüfungen von Personen (Erkenntnisabfragen) für sonstige gesetzliche Fälle oder mit Einwilligung der oder des Betroffenen als Mitwirkungsaufgabe des Verfassungsschutzes normiert.

5. § 7 Abs. 2 regelt die Verpflichtung des für den Verfassungsschutz zuständigen Ministeriums, die Öffentlichkeit über grundlegende Angelegenheiten des Verfassungsschutzes zu informieren. Diese Pflicht besteht vorbehaltlich entgegenstehender Geheimhaltungserfordernisse.

6. § 9 Abs. 1 ist als nachrichtendienstliche Generalklausel ausgestaltet. Die Verfassungsschutzbehörde ist danach befugt, zur Aufgabenerfüllung nach § 5, zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge sowie zur Gewinnung, Erhaltung oder Überprüfung der Nachrichtenzugänge die erforderlichen offenen und verdeckten Maßnahmen zu treffen, soweit nicht §§ 10 bis 21 diese besonders regeln. Maßnahmen sind auch zulässig, wenn Dritte unvermeidbar betroffen sind. Die Befugnisse gelten entsprechend für die Erfüllung der Aufgaben nach § 6; insoweit sind nur offene Maßnahmen zulässig.

7. Nachrichtendienstliche Mittel werden in § 9 Abs. 2 Satz 1 als Methoden und Gegenstände einschließlich technischer Mittel zur verdeckten Informationsbeschaffung legaldefiniert und die Verfassungsschutzbehörde zu deren Einsatz ermächtigt. Nachrichtendienstliche Mittel einschließlich deren Anordnungsbefugnis, welche nicht in §§ 9 bis 21 besonders geregelt werden, sind in einer Dienstvorschrift zu benennen (§ 9 Abs. 2 Satz 2). Die Dienstvorschrift ist der Parlamentarischen Kontrollkommission vorzulegen (§ 9 Abs. 2 Satz 3).

8. § 9 Abs. 3 benennt die Voraussetzungen für den Einsatz nachrichtendienstlicher Mittel sowie die Personen, gegenüber denen nachrichtendienstliche Mittel zulässig sind.

9. § 9 Abs. 4 macht die Beobachtung Minderjähriger mit nachrichtendienstlichen Mitteln vor Vollendung des 14. Lebensjahres abhängig von tatsächlichen Anhaltspunkten für die Planung, Begehung oder Verwirklichung der Straftatbestände in § 3 des Artikel 10-Gesetzes.

10. § 10 regelt den Einsatz Verdeckter Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes sowie rechtliche Grenzen. § 10 Abs. 2 Satz 2 und 3 schafft eine strafbefreiende Befugnis zur Aufklärung von Bestrebungen nach § 5 Satz 1 Nr. 1, 3, oder 4. Der Einsatz zur Gründung derartiger Bestrebungen oder zur steuernden Einflussnahme auf solche ist unzulässig. Bei tatsächlichen Anhaltspunkten dafür, dass die Verdeckte Mitarbeiterin oder der Verdeckte Mitarbeiter rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht hat, soll der Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden (§ 10 Abs. 2 Satz 4). Über Ausnahmen entscheidet die Leitung der Verfassungsschutzbehörde. In § 10 Abs. 3 wird deklaratorisch auf § 9 a Abs. 3 Bundesverfassungsschutzgesetz (BVerfSchG) verwiesen, welcher spezifische Möglichkeiten der Verfahrenseinstellung oder Klagerücknahme durch die Staatsanwaltschaft bestimmt.

11. Die Regelungen in § 10 Abs. 1 bis 3 werden auch auf Mitarbeiterinnen und Mitarbeiter erstreckt, die verdeckt Informationen in sozialen Netzwerken und sonstigen Kommunikationsplattformen im Internet erheben, auch wenn sie nicht dauerhaft unter einer Legende tätig sind.

12. § 11 regelt den Einsatz von Vertrauenspersonen sowie dessen rechtliche Grenzen. Die Vorschriften über den Einsatz von Verdeckten Mitarbeiterinnen und Mitarbeitern gelten entsprechend. § 11 Abs. 2 regelt die Entscheidungskompetenz der Leitung der Verfassungsschutzbehörde sowie Ausschlussgründe der Anwerbung und des Einsatzes.

13. § 12 verweist für die Überwachung des Brief-, Post- und Fernmeldeverkehrs einschließlich der Datenverarbeitung deklaratorisch auf das Artikel 10-Gesetz.

14. Besondere Auskunftsersuchen in § 13 Abs. 1 bis 3 zu Verkehrs-, Finanz- und Postdienstleistungen werden auch für den Bereich extremistischer Bestrebungen (§ 5 Satz 1 Nr. 1), mithin für alle Bestrebungen im Sinne des § 5 geregelt. Die Unternehmen haben eine unentgeltliche Auskunftspflicht (§ 13 Abs. 6). Die Pflicht zur Auskunft über Verkehrsdienstleistungsdaten, insbesondere Flugverkehrsdaten, haben zukünftig auch die Betreiber von Computerreservierungs- und Globalen Distributionssystemen (§ 13 Abs. 2 Satz 2).

15. Mit § 13 Abs. 1 Satz 2 wird eine Befugnis zur Kontostammdatenabfrage beim Bundeszentralamt für Steuern geschaffen.

16. Der veraltete Begriff der Teledienste wird in § 13 Abs. 4 durch Telemedien ersetzt. Der Verfassungsschutz darf über die in § 96 Abs. 1 Nr. 1 bis 5 Telekommunikationsgesetz (TKG) und § 15 Abs. 1 Telemediengesetz (TMG) genannten Verkehrsdaten Auskünfte einholen.

17. Die Auskunft über Bestandsdaten zu Telekommunikation und zu Telemedien wird in § 13 Abs. 5 geregelt.

18. Mit § 14 wird eine Befugnis zur Funkzellenabfrage geschaffen.

19. Mit § 15 wird eine Rechtsgrundlage für den Einsatz eines sog. IMSI-Catchers zur Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten geschaffen.

20. § 16 sieht zur Erfüllung der Aufgaben nach § 5 die Befugnis vor, Sachen zur Datenerhebung heimlich und vorübergehend in Besitz nehmen.

21. In § 17 ist zukünftig der Einsatz technischer Mittel zur akustischen Überwachung außerhalb der Wohnung geregelt.

22. Der Einsatz technischer Mittel zur Wohnraumüberwachung (§§ 18 und 19) wird im Hinblick auf den Kernbereichsschutz an die Vorgaben des BVerfG angepasst. Die Maßnahme wird bereits im Vorfeld konkreter Gefahren gegenüber Personen zugelassen, deren individuelles Verhalten die Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraumes eine terroristische Straftat begehen wird. Anordnendes Gericht ist gemäß § 19 Abs. 9 zukünftig das Oberverwaltungsgericht Rheinland-Pfalz. Eine Eilanordnungskompetenz bei Gefahr im Verzug entfällt.

23. Mit § 20 wird eine Rechtsgrundlage zur Datenerhebung aus digitalen Medien geschaffen. Der Verfassungsschutz darf zur Erfüllung seiner Aufgaben nach den §§ 5 und 6 die erforderlichen Maßnahmen in Bezug auf digitale Medien treffen, soweit nicht die Absätze 2 und 3 diese besonders regeln. Absatz 2 macht die legendierte Erkenntnisgewinnung unter Ausnutzung schutzwürdigen Vertrauens des Betroffenen in die Identität und Motivation des Kommunikationspartners abhängig von der Anordnung der Leitung der Verfassungsschutzbehörde. Absatz 3 erlaubt unter den Voraussetzungen und den Verfahrensvorschriften des Artikel 10-Gesetzes den Zugriff auf zugangsgesicherte Telekommunikationsinhalte und sonstige Informations- und Kommunikationsinhalte in digitalen Medien auf dem hierfür technisch vorgesehenen Weg, ohne selbst Kommunikationsadressat und ohne von den an der Kommunikation teilnehmenden Personen oder anderen Berechtigten hierzu autorisiert zu sein (z. B. Eindringen in ein E-Mail-Postfach oder Auslesen von Endgeräten, sofern die Zugangsdaten bekannt geworden sind).

24. § 21 regelt die Zugriffsbefugnis des Verfassungsschutzes auf Einrichtungen zur Videoüberwachung sowie gespeicherte Bild- und Tonaufzeichnungen (Videografie) aus der Videoüberwachung des öffentlich zugänglichen Raums. Ein Zugriff auf Aufzeichnungen ist nur bei schwerwiegenden Gefahren für die in § 5 genannten Schutzgüter zulässig.

25. In § 23 Abs. 1 Satz 1 Nummer 6 wird gesetzlich klargestellt, dass personenbezogene Daten mit Einwilligung der oder des Betroffenen durch den Verfassungsschutz verarbeitet werden dürfen.

26. In § 23 Abs. 1 Satz 3 wird klargestellt, dass die Verarbeitung personenbezogener Daten derselben Aufgabe und dem Schutz derselben Rechtsgüter dienen muss, welche Grund der Erhebung waren (Grundsatz der Zweckbindung). Die Verarbeitung personenbezogener Daten aus der besonders eingriffsintensiven Maßnahme der Wohnraumüberwachung ist nur bei Tatsachen für im Einzelfall bestehende dringende Gefahren für die öffentliche Sicherheit, insbesondere eine gemeine Gefahr oder eine Lebensgefahr oder eine Gefahrenlage im Sinne des § 18 Abs. 1 Satz 2 zulässig (§ 23 Abs. 1 Satz 4).

27. Gemäß § 23 Abs. 4 wird der durch das BVerfG im Urteil zum BKA-Gesetz entwickelte Grundsatz der hypothetischen Datenneuerhebung in das Gesetz aufgenommen (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 283). Danach können personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, nur weiterverarbeitet werden, wenn mindestens vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und die Daten auch für den geänderten Zweck nach diesem Gesetz hätten erhoben werden können. Der Verweis in § 23 Abs. 4 stellt klar, dass die aus Maßnahmen der Wohnraumüberwachung erlangten personenbezogenen Daten nur bei Vorliegen von Tatsachen für im Einzelfall bestehende dringende Gefahren für die öffentliche Sicherheit, insbesondere bei einer gemeinen Gefahr oder einer Lebensgefahr oder einer Gefahrenlage im Sinne des § 18 Abs. 1 Satz 2 für andere Zwecke verarbeitet werden dürfen.

28. § 24 Abs. 5 schafft die gesetzliche Möglichkeit, die in § 3 Abs. 3 Satz 5 des Landesarchivgesetzes vom 5. Oktober 1990, zuletzt geändert durch Gesetz vom 27. November 2015 (GVBl. S. 383), BS 224-10, geregelte Beschränkung der Sperrfrist für die öffentliche Nutzung von Archivgut aufzuheben, wenn die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister erklärt, dass das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde. Die Entscheidung ergeht im Einvernehmen mit der für das Archivwesen zuständigen Ministerin oder dem für das Archivwesen zuständigen Minister.

29. Mit § 25 Abs. 5 wird eine Rechtsgrundlage zur Nutzung automatisierter Abrufverfahren eingeführt, soweit die Nutzung eines automatisierten Abrufverfahrens durch die Verfassungsschutzbehörden ausdrücklich gesetzlich geregelt wird.

30. Mit § 25 Abs. 6 erhält der Verfassungsschutz eine Rechtsgrundlage zur Ausschreibung von verfassungsschutzrelevanten Personen und Kraftfahrzeugkennzeichen in polizeilichen Informationssystemen (POLIS). Eine polizeiliche Aufgabe ergibt sich daraus nicht.

31. Der durch das BVerfG in dem Urteil zum BKA-Gesetz entwickelte Grundsatz der hypothetischen Datenneuerhebung (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 283) wird auch bei der zweckändernden Übermittlung personenbezogener Daten an die Staatsanwaltschaft und Polizeibehörden zur Bedingung gemacht (§ 26 Abs. 2 Satz 3). Die Übermittlung personenbezogener Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, ist danach nur zulässig, wenn die neue Verarbeitung der übermittelten Daten eine Neuerhebung durch die empfangende Stelle mit vergleichbaren Mitteln rechtfertigen würde. Personenbezogene Daten, welche nicht mit nachrichtendienstlichen Mitteln erhoben wurden, können dagegen zur einfachen Aufgabenwahrnehmung der empfangenden Stelle übermittelt werden (§ 26 Abs. 3).

32. In § 27 Abs. 2 Satz 2 und Absatz 3 ist eine Datenübermittlungsregelung zum Schutz von Mitarbeiterinnen und Mitarbeitern öffentlicher Stellen geschaffen worden. Die Übermittlung ist unabhängig davon zulässig, ob die zu übermittelnden Daten mit nachrichtendienstlichen Mitteln erhoben wurden oder nicht.

33. Die Parlamentarische Kontrolle wird gestärkt.

34. Das in Ergänzung und Umsetzung des Europäischen Gemeinschaftsrechts (Verordnung (EU) 2016/679 – Datenschutzgrundverordnung – und Richtlinie (EU) 2016/680) novellierte Landesdatenschutzgesetz (LDSG) vom 8. Mai 2018 (GVBl. S. 93, BS 204-1) findet keine Anwendung. Die Datenschutzgrundverordnung entfaltet mangels Regelungskompetenz der Europäischen Union im Bereich des Verfassungsschutzes (vgl. Artikel 4 Abs. 2 Satz 3 EU-Vertrag) ebenso keine unmittelbare Wirkung. Für die Aufgabenwahrnehmung des Verfassungsschutzes bildet dieses Gesetz ein bereichsspezifisches Datenschutzvollsystem. Einige im LDSG bzw. Europäischen Gemeinschaftsrecht getroffenen Regelungen sind aber auch im Aufgabenbereich der §§ 5 und 6 angemessen und gelten daher gemäß § 39 Satz 2 entsprechend.

## B. Zu den einzelnen Bestimmungen

Zu § 1 (Auftrag)

Absatz 1 definiert den in Artikel 73 Abs. 1 Nr. 10 b Grundgesetz (GG) vorgesehenen Auftrag des Verfassungsschutzes. Der Verfassungsschutz dient demnach dem Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder.

Zu § 2 (Verfassungsschutzbehörde)

Zu Absatz 1

Mit Absatz 1 wird die bisherige Organisationsform des Verfassungsschutzes in Rheinland-Pfalz beibehalten. Insoweit handelt es sich um eine rein deklaratorische Bestimmung.

Zu Absatz 2

Absatz 2 bestimmt das Trennungsgebot zwischen Polizei und Verfassungsschutz. Zum einen ist hiervon die institutionelle Trennung zwischen diesen Behörden umfasst. Der Verfassungsschutzbehörde stehen keine exekutiven polizeilichen Befugnisse, insbesondere keine Zwangsbefugnisse zu. Demnach darf sie die Polizeibehörde auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, die sie selbst nicht durchführen darf. Schließlich besteht auch eine informationelle Trennung zwischen Polizei und Verfassungsschutz, sodass der Austausch personenbezogener Daten die Ausnahme und nicht die Regel ist.

Zu § 3 (Zusammenarbeit)

Zu Absatz 1

Die Pflicht zur Zusammenarbeit zwischen Bund und Ländern ergibt sich bereits aus § 1 Abs. 2 BVerfSchG. Insoweit handelt es um eine rein deklaratorische Vorschrift.

Zu Absatz 2

In Absatz 2 wird festgelegt, inwieweit andere Verfassungsschutzbehörden auf dem Gebiet des Landes Rheinland-Pfalz tätig werden dürfen. Im Verhältnis zu einer anderen Landesbehörde ist das Einvernehmen herzustellen. Dieses dient in erster Linie der operativen Abstimmung. Im Übrigen hat die

Verfassungsschutzbehörde des betreffenden Landes die materiellen Bestimmungen dieses Gesetzes zu beachten, wenn und soweit sie im Hoheitsgebiet des Landes Rheinland-Pfalz tätig wird. Im Falle des § 5 Abs. 1 BVerfSchG kann das Bundesamt für Verfassungsschutz in den Ländern im Rahmen einer vorherigen Benehmensherstellung tätig werden, soweit die Voraussetzungen hierfür vorliegen. Die Verfassungsschutzbehörde ist vorher und möglichst schriftlich über das Vorhaben des Bundesamtes für Verfassungsschutz zu unterrichten. Ist eine vorherige Unterrichtung nicht möglich, so ist diese unverzüglich nachzuholen. Der Verfassungsschutzbehörde ist zudem Gelegenheit zur Stellungnahme zu geben.

Mit Satz 2 wird die Verfassungsschutzbehörde ermächtigt, im Einvernehmen mit anderen Ländern auf deren Gebiet tätig zu werden.

Zu § 4 (Begriffsbestimmungen)

Die Bestimmung erläutert die in den §§ 1 und 5 angesprochenen Schutzgüter und definiert einige zentrale Begriffe im Interesse der Normenklarheit und zur Erhöhung der Rechtssicherheit bei der Aufgabenerfüllung.

Zu Absatz 1

In Absatz 1 wird der für die Beobachtung maßgebliche Begriff „Bestrebung“ als politisch motivierte Verhaltensweise beschrieben. Die Bestimmung geht weiter davon aus, dass es für ein Vorliegen einer solchen Bestrebung erforderlich ist, dass in einem oder für einen Personenzusammenschluss verfassungsfeindliche Ziele oder Zwecke verfolgt werden. Verhaltensweisen von Einzelpersonen sind nach Satz 3 dann als Bestrebung anzusehen, soweit diese gegen Schutzgüter dieses Gesetzes unter Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen. Die bloße verfassungsfeindliche Gesinnung als solche ist irrelevant. Da allerdings auch von Einzelpersonen, die bisher nicht durch Bestrebungen in Erscheinung getreten sind und daher nicht beobachtet werden konnten, aufgrund einer möglicherweise schnellen Radikalisierung erhebliche Gefahren ausgehen können, sind an die Annahme von Verhaltensweisen, die die verfassungsschutzrechtlichen Schutzgüter erheblich beschädigen können, keine zu hohen Anforderungen zu stellen. Insoweit reichen im Sinne von § 5 Satz 1 tatsächliche Anhaltspunkte für den Verdacht aus, dass die besagten Schutzgüter von der betreffenden Einzelperson mit einer gewissen Wirkmächtigkeit beeinträchtigt werden könnten. Bei erstmalig aufkommenden Erkenntnissen zu einer Person ohne erkennbaren Bezug zu einem Personenzusammenschluss handelt es sich hierbei um eine Prognoseentscheidung der Verfassungsschutzbehörde, die auch aufgrund nachrichtendienstlichen Erfahrungswissens getroffen wird. Erkenntnisse zu der betreffenden Person über die bisherige Anwendung von Gewalt – auch in anderen Zusammenhängen als mit den verfassungsfeindlichen Verhaltensweisen – werden in diese Prognoseentscheidung mit einbezogen.

Die Beobachtung der verfassungsfeindlichen Beeinflussung anderer Gruppierungen ist ebenfalls Aufgabe der Verfassungsschutzbehörde, muss jedoch nicht gesondert und ausdrücklich geregelt werden. Von einer verfassungsfeindlichen Zielsetzung ist auszugehen, wenn Aufgaben, Programme und Parolen verfassungsfeindlicher Gruppen unverändert oder ungeprüft übernommen werden, wenn die Führungsgremien weitgehend mit Mitgliedern verfassungsfeindlicher Gruppen durchsetzt oder unterwandert sind oder wenn Gruppierungen bis hin zur Existenzgefährdung von der Finanzierung durch verfassungsfeindliche Organisationen abhängig sind. Die verlangte verfassungsfeindliche Tendenz muss weiterhin eine gewisse Handlungsintensität erreicht haben, um sie als beobachtungswürdig einstufen zu können. Nach Absatz 1 Satz 2 erfordert diese eine nachdrückliche Unterstützung.

Zu Absatz 2

Absatz 2 soll solche Personenzusammenschlüsse erfassen, die über keine feste Organisationsstruktur verfügen, deren Verhaltensweisen jedoch dennoch gegen die Schutzgüter dieses Gesetzes gerichtet sind. Hierdurch wird klarstellend geregelt, dass z. B. auch Verhaltensweisen von Personen des sogenannten Reichsbürger- und Selbstverwalterspektrums eine Gefahr für die freiheitliche demokratische Grundordnung darstellen können.

Zu Absatz 3

Absatz 3 ist dem Urteil des BVerfG zum jüngeren NPD-Verbotsverfahren entnommen (BVerfG, Urteil vom 17. Januar 2017 – 2 BvB 1/13, Rn. 535 ff. – juris). Als wesentliche Grundprinzipien der freiheitlichen demokratischen Grundordnung hat das BVerfG die Menschenwürde, das Rechtsstaatsprinzip sowie das Demokratieprinzip benannt.

Zu § 5 (Beobachtungsaufgaben)

Die Bestimmung beschreibt die originären Aufgaben der Verfassungsschutzbehörde in Anlehnung an § 3 BVerfSchG. Der dortige Aufgabenkatalog wird im Wesentlichen wörtlich übernommen. Diese Übereinstimmung ist im Interesse eines wirksamen und einheitlichen Verfassungsschutzes in Bund und Ländern (Verfassungsschutzverbund) sachgerecht. Der Begriff der Beobachtung kennzeichnet die Verfassungsschutzbehörde als Nachrichtendienst. Diese umfasst neben der zielgerichteten Wahrnehmung von Personen bzw. Objekten auch die Informationsverarbeitung, so auch das Sammeln und Auswerten von Informationen. In Satz 2 wird klargestellt, dass im Rahmen des allgemeinen Verhältnismäßigkeitsgrundsatzes die Beobachtung nur dann verdeckt erfolgt, soweit ein milderes Mittel, z. B. offene Ermittlungen, nicht gleich erfolgversprechend erscheinen.

Zu § 6 (Mitwirkungsaufgaben)

Zu Absatz 1

Die Bestimmung ist weitgehend wortgleich dem § 3 Abs. 2 BVerfSchG entnommen und benennt als Mitwirkungsaufgaben den vorbeugenden personellen Geheim- und Sabotageschutz und den vorbeugenden materiellen Geheimschutz. Nach dem Wortlaut wird die Verfassungsschutzbehörde erst auf Veranlassung von anderen zuständigen Stellen tätig und ist nicht federführende Organisation bei der Sicherheitsüberprüfung. Die Durchführung der Mitwirkungsaufgaben obliegt der Verfassungsschutzbehörde. Sie arbeitet unabhängig und eigenverantwortlich entsprechend den bestehenden Bestimmungen. Die beantragende Stelle ist jedoch ihrerseits dafür verantwortlich, dass im Falle des Satzes 1 Nummer 2 die Überprüfung nur für solche Personen erbeten wird, die die dort genannten Voraussetzungen erfüllen. Die näheren

Voraussetzungen sowie die Ausgestaltung des Verfahrens bei einer solchen Überprüfung richten sich nach dem Landessicherheitsüberprüfungsgesetz vom 8. März 2000 (GVBl. S. 70), zuletzt geändert durch Artikel 4 des Gesetzes vom 22. Dezember 2015 (GVBl. S. 461), BS 12-3. Satz 1 Nr. 4 stellt eine Folgeänderung aufgrund der Regelung in § 3 Abs. 2 Satz 1 Nr. 5 BVerfSchG dar.

Zu Absatz 2

Absatz 2 sieht als Mitwirkungsaufgabe der Verfassungsschutzbehörde eine Überprüfung (Erkenntnisabfrage) in sonstigen gesetzlich vorgesehenen Fällen und auch dann vor, wenn die oder der Betroffene eingewilligt hat. Einschlägig sind hier insbesondere Überprüfungen im Rahmen eines Einstellungsverfahrens (z. B. für die Polizei) oder eines Akkreditierungsverfahrens, z. B. bei der Zulassung von Überwachungspersonal zu Großveranstaltungen.

Zu § 7 (Unterrichtung der Landesregierung und der Öffentlichkeit)

Zu Absatz 1

Absatz 1 stellt klar, dass die Sammlung und Auswertung der Informationen nicht Selbstzweck ist, sondern der Erfüllung der Pflicht dient, die Landesregierung über verfassungsschutzrelevante Erkenntnisse zu unterrichten. Den zuständigen Stellen soll somit ermöglicht werden, rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren im Sinne des § 5 zu treffen. Dies ist vor dem Hintergrund zu sehen, dass die Verfassungsschutzbehörde keine polizeilichen Exekutivbefugnisse hat, sondern durch ihre Tätigkeit im Vorfeld konkreter Gefahren und des Strafrechts eine effektive Gefahrenabwehr durch zuständige andere Behörden, insbesondere die Polizei, ermöglichen soll.

Zu Absatz 2

Absatz 2 regelt die Unterrichtung der Öffentlichkeit über grundlegende Angelegenheiten des Verfassungsschutzes durch das fachlich zuständige Ministerium. Auf diese Weise soll die Öffentlichkeit über Bestrebungen und Tätigkeiten nach § 5 informiert werden. Es dürfen keine Geheimhaltungsgründe entgegenstehen. Für die Unterrichtung ist keine besondere Form vorgesehen. Sie erfolgt zumeist durch einen Verfassungsschutzbericht.

Die Sensibilisierung von Öffentlichkeit und Unternehmen für Fragen des Wirtschaftsschutzes ist zu intensivieren, um Unternehmen vor Wirtschafts- und Konkurrenzspionage zu schützen und eine nationale Strategie für den Wirtschaftsschutz aufzusetzen. Wirtschaftsschutz bedeutet vor allem Information, Sensibilisierung und Prävention von Unternehmen sowie Forschungs- und Wissenschaftseinrichtungen über bzw. vor Risiken des illegalen „Know-how“-Transfers (Wirtschaftsspionage/Konkurrenzausspähung). Der Wirtschaftsschutz stellt eine der Schwerpunktaufgaben der präventiven Spionageabwehr der Verfassungsschutzbehörde dar, die weiter verstärkt werden soll. Angesichts der Bedeutung dieser Aufgaben werden sie gesetzlich geregelt. Die Regelung trägt zugleich dem Umstand Rechnung, dass unter Umständen zur sachgerechten Öffentlichkeitsunterrichtung auch personenbezogene Daten bekannt gegeben werden müssen (vgl. § 26 Abs. 7).

Die Öffentlichkeitsunterrichtung kann, wenn dies sachlich geboten erscheint, auch bereits Verdachtsfälle einschließen.

Zu § 8 (Grundsätze)

Mit dieser Bestimmung, welche Teil 3 des Gesetzes mit den Regelungen über die Befugnisse der Verfassungsschutzbehörde einleitet, werden bestimmte Rechtsgrundsätze festgelegt. Diese haben, wie bei der Regelung des Verhältnismäßigkeitsgrundsatzes in Absatz 1, aufgrund der verfassungsrechtlichen Bindung der Verfassungsschutzbehörde an Gesetz und Recht (Artikel 20 Abs. 3 des Grundgesetzes) überwiegend deklaratorischen Charakter. Gleichwohl sollen diese geltenden Rechtsgrundsätze aufgrund des Eingriffscharakters der in Teil 3 geregelten Befugnisse an dieser Stelle im Gesetz besonders hervorgehoben werden.

Zu Absatz 1

Diese Bestimmung, die im Bundesrecht auch in § 8 Abs. 5 BVerfSchG verankert ist, ist im Wesentlichen aus der bisherigen Regelung in § 8 Abs. 2 LVerfSchG übernommen. In ihr ist geregelt, dass die zur Verfolgung eines legitimen Zwecks bei der Aufgabenerfüllung durch die Verfassungsschutzbehörde ergriffenen möglichen und geeigneten Maßnahmen auch erforderlich und angemessen sein müssen. Dass zur Verfolgung dieses Zwecks stets das zur Zielerreichung führende mildeste Mittel gegenüber der betroffenen Personen anzuwenden ist, ergibt sich in diesem Gesetzentwurf etwa auch aus § 5 Satz 2. Danach erfolgt die Beobachtung grundsätzlich offen und mit verdeckten Mitteln nur insoweit, wie dies für die Aufgabenerfüllung im Einzelfall erforderlich ist. Maßnahmen mit geringerer Eingriffstiefe in die Freiheitsrechte der betroffenen Person haben demnach stets Vorrang, wenn der damit verfolgte Zweck genauso gut und effektiv erreicht werden kann.

Zu Absatz 2

Der Kernbereich privater Lebensgestaltung, wozu insbesondere die Intimsphäre zählt, ist nach ständiger Rechtsprechung des BVerfG in seiner Gesamtheit absolut geschützt und unantastbar. Dementsprechend sind den Kernbereich privater Lebensgestaltung zuzuordnende höchstpersönliche Vorgänge pauschal der Ausforschung durch die Nachrichtendienste entzogen. Eine Güterabwägung findet nicht statt; vielmehr ist jeglicher – über das zu einer persönlichkeitsrechtlichen Qualifikation nötige Durchsehen oder Anhören hinausgehende – Eingriff in diesen Kernbereich unzulässig. Nicht dem Kernbereich zuzurechnen ist die Kommunikation unmittelbar über Sachverhalte mit Sozialbezug, wie Straftaten oder extremistische Bestrebungen, selbst wenn sie zugleich Höchstpersönliches zum Gegenstand hat (BVerfGE 141, 220 – Rn. 119 ff.).

Gesetzlich ist der Schutz des Kernbereichs privater Lebensgestaltung sowie von bestimmten Berufsgeheimnisträgern bislang nur für Maßnahmen nach dem Artikel 10-Gesetz (§§ 3 a, 3 b) sowie beim Einsatz technischer Mittel zur Wohnraumüberwachung nach den §§ 18 und 19 dieses Gesetzentwurfs ausdrücklich geregelt, wobei in § 18 Abs. 6 Satz 3 und Abs. 7 Satz 2 auf das Artikel 10-Gesetz verwiesen wird.

Mit Absatz 2 wird klargestellt, dass der Kernbereichsschutz sowie der Schutz von Berufsgeheimnisträgern und ihnen gleichstehenden Personen auch für sämtliche andere Maßnahmen gelten, mit denen die Verfassungsschutzbehörde personenbezogene Daten erhebt und weiter verarbeitet. In dieser Hinsicht ist die Durchführung einer Maßnahme – sobald dies ohne Gefährdung eingesetzter Personen möglich ist – solange zu

unterbrechen, wie Anhaltspunkte dafür bestehen, dass Inhalte den Kernbereich privater Lebensgestaltung betreffend erfasst werden.

Mit Blick auf den Schutz der Berufsgeheimnisträger fallen unter die ihnen gleichstehenden Personen insbesondere die in § 53 a StPO genannten, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken. Die Achtung des Schutzes der Berufsgeheimnisträger und der ihnen gleichstehenden Personen durch die Verfassungsschutzbehörde greift unmittelbar ab dem Zeitpunkt, ab dem sie positive Kenntnis dieses Umstandes hat und hinsichtlich der Verwertung bereits erhobener Daten auch rückwirkend.

Zu § 9 (Allgemeine Befugnisse)

Aufgrund des vorfeldbezogenen Aufgabenspektrums haben Verfassungsschutzbehörden des Bundes und der Länder als Nachrichtendienste weitreichende Befugnisse zur Datensammlung, die weder hinsichtlich der konkreten Tätigkeitsfelder spezifisch ausdefiniert noch hinsichtlich der jeweils einzusetzenden Mittel detailscharf ausgestaltet sind (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn 117 – juris). In der Rechtsprechung des BVerfG ist dabei eine deutliche Unterscheidung polizeilicher und nachrichtendienstlicher Befugnisse feststellbar (vgl. dazu BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn 115 ff. – juris). Diese Differenzierung ist nachvollziehbar, da wesentliche Unterschiede in der polizeilichen und nachrichtendienstlichen Aufgabenwahrnehmung bestehen und der Rechtsrahmen für die jeweiligen Befugnisse bezogen auf die jeweils verfolgten Aufgaben verhältnismäßig ausgestaltet ist. Speziell zum Recht der Nachrichtendienste hat das BVerfG daher einen weniger detaillierten Regelungsansatz inzident anerkannt und die Eingriffsschwellen für nachrichtendienstliche Gefahrenerforschung in der Vergangenheit niedriger gesehen (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 255 – juris; BVerfG, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, Rn. 177 – juris; BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn 117 – juris).

Zu Absatz 1

Die Bestimmung stellt im Sinne einer Generalklausel die allgemeine Befugnisnorm für die Verfassungsschutzbehörde dar, um Maßnahmen im Rahmen der Aufgabenerfüllung gemäß § 5, zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge sowie zur Überprüfung der Nachrichtenzugänge treffen zu können. Die Maßnahmen können für jedermann offen erkennbar, erforderlichenfalls verdeckt erfolgen. Das Abstellen auf die Erforderlichkeit als wesentliches Element des Verhältnismäßigkeitsprinzips normiert den behördlichen Prüfungszwang, dass kein milderes, gleichsam effektives Mittel zur Aufgabenerfüllung zur Verfügung steht. Soweit die jeweiligen Befugnisse in §§ 10 bis 21 gesondert geregelt sind, gehen diese Vorschriften der allgemeinen Befugnisnorm vor. Der Einsatz nachrichtendienstlicher Mittel im Rahmen der Mitwirkungsaufgaben gemäß § 6 ist nicht zulässig (Satz 2). Wenn Dritte unvermeidbar von Maßnahmen der Verfassungsschutzbehörde betroffen sind, so macht dieser Umstand die Maßnahme nicht unzulässig. Jedoch muss stets geprüft werden, ob eine Drittbetroffenheit unter Verhältnismäßigkeitsgesichtspunkten vermeidbar oder hinnehmbar ist.

Zu Absatz 2

Absatz 2 definiert nachrichtendienstliche Mittel als Methoden und Gegenstände einschließlich technischer Mittel zur verdeckten Informationsbeschaffung. Die Verfassungsschutzbehörde ist als Nachrichtendienst hierzu befugt. Die Legaldefinition der nachrichtendienstlichen Mittel konkretisiert insoweit die erforderlichen verdeckten Maßnahmen in Absatz 1 und macht diese abhängig von einer spezialgesetzlichen Regelung in den §§ 10 bis 21 oder der Benennung in einer gesonderten Dienstvorschrift. Wegen der Grundrechtsrelevanz von verdeckten Maßnahmen für die Persönlichkeitsrechte von Betroffenen ist die Dienstvorschrift, welche auch die Zuständigkeiten für die Anordnungen regelt, der Parlamentarischen Kontrollkommission vorzulegen. Damit soll der mit der Kontrolle des Verfassungsschutzes gemäß §§ 31 ff. befassten Parlamentarischen Kontrollkommission Klarheit über die verschiedenen Möglichkeiten der verdeckten Datenerhebung sowie über die jeweilige Anordnungskompetenz verschafft werden.

Zu Absatz 3

Die Bestimmung macht den Einsatz nachrichtendienstlicher Mittel zur Erhebung personenbezogener Daten, soweit dieser nicht in den §§ 10 bis 21 besonders geregelt ist, von den Voraussetzungen in den Nummern 1 bis 5 abhängig. Nachrichtendienstliche Mittel sind danach zulässig zur Gewinnung, Erhaltung oder Überprüfung von Nachrichtenzugängen (Nummer 1), gegenüber Personen, bei denen tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten nach § 5 vorliegen (Nummer 2), gegenüber Nachrichten- und Kontaktmittlern (Nummer 3) und gegenüber Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst Bestrebungen oder Tätigkeiten gemäß § 5 nachgehen, jedoch hinreichende Anhaltspunkte für eine Verbindung zu diesen bestehen (Nummer 4). Bei Personen gemäß Nummer 4 muss eine Beziehung zu der Bestrebung oder Tätigkeit nach § 5 sowie regelmäßiger Austausch bzw. Kommunikation vorliegen. Eine bloß flüchtige Verbindung ist dagegen nicht ausreichend. Nummer 5 dient der Eigensicherung der Behörde und ihrer Mitarbeiterinnen und Mitarbeiter.

Zu Absatz 4

Minderjährige bedürfen eines besonderen Schutzes, der typische Aspekte der Jugendphase berücksichtigt. Hierzu gehören die Bewältigung alterstypischer Entwicklungsaufgaben, wie familiäre Ablösung, soziale Neuorientierung und die Entwicklung einer eigenen (auch politischen) Identität. Absatz 4 stellt klar, dass der Einsatz nachrichtendienstlicher Mittel gegenüber Minderjährigen ab Vollendung des 10. Lebensjahres und bis zur Vollendung des 14. Lebensjahres nur ausnahmsweise zulässig ist, nämlich bei tatsächlichen Anhaltpunkten für die Planung, Begehung oder Verwirklichung einer der in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftatbestände. Da Minderjährige vor Vollendung des 14. Lebensjahres nicht schuldfähig sind, genügt die Verwirklichung des objektiven Tatbestandes. Insoweit wird mit der Vorschrift der Einsatz nachrichtendienstlicher Mittel bei Personen unter 14 Jahren nur auf Extremfälle, nämlich auf die Planung, Begehung und Verwirklichung staatsgefährdender terroristischer Straftaten beschränkt. Hierdurch wird verdeutlicht,

dass in der Regel, außerhalb dieser Fälle, Radikalisierungstendenzen vornehmlich im Rahmen von Präventionsarbeit entgegengewirkt werden muss.

Zu §§ 10 und 11 (Verdeckte Mitarbeiterinnen und Mitarbeiter/Vertrauenspersonen)

Die planmäßige und systematische Informationsbeschaffung durch heimlich eingesetzte Personen ist ein unverzichtbares Mittel zur Aufklärung von Bestrebungen im Sinne des § 5. Hierbei können nicht nur Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde, sondern auch Vertrauenspersonen zum Einsatz kommen. Zur Stärkung der Akzeptanz und Transparenz wird nunmehr in § 11 der Einsatzrahmen gesetzlich festgelegt, wie dies auch der Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus (BLKR) vom 30. April 2013 (S. 282, Rn. 649, 650) empfohlen hat.

Zu § 10 (Verdeckte Mitarbeiterinnen und Mitarbeiter)

Zu Absatz 1

Absatz 1 räumt der Verfassungsschutzbehörde die Befugnis zum Einsatz verdeckter Mitarbeiterinnen und Mitarbeiter ein. Der Begriff wird legaldefiniert und erfasst danach den verdeckten Einsatz von Mitarbeiterinnen und Mitarbeitern unter einer auf Dauer angelegten Tarnidentität. Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde, die zwar verdeckt, aber nicht unter einer Legende operieren (z. B. Teilnahme im Social Media unter „Nicknames“) sind keine verdeckten Mitarbeiterinnen und Mitarbeiter. Grundsätzliche Voraussetzung des Einsatzes ist die allgemeine Befugnis zum Einsatz nachrichtendienstlicher Mittel gemäß § 9 Abs. 3.

Fachlich erforderlich ist es in Abgrenzung zur Bundesregelung in § 9 a Abs. 1 BVerfSchG, den Einsatz von verdeckten Mitarbeiterinnen und Mitarbeitern nicht nur zum Zweck der Aufklärung von Bestrebungen, sondern vielmehr auch auf sicherheitsgefährdende und/oder geheimdienstliche Tätigkeiten in der Bundesrepublik Deutschland für eine fremde Macht zu erstrecken.

Ebenfalls beschränkt sich der dauerhafte Einsatz von verdeckten Mitarbeiterinnen und Mitarbeitern im Unterschied zur Bundesregelung nicht ausschließlich auf besonders bedeutsame Bestrebungen, insbesondere solche mit Gewaltbezug. Die Beschränkung auf Bundesebene rechtfertigt sich durch die Zentralstellenfunktion des Bundesamtes für Verfassungsschutz, die eine stärkere Fokussierung des Aufgabenbereichs auf gewaltbereite Bestrebungen erfordert, und stellt eine effiziente Ressourcensteuerung des Bundes in Angelegenheiten des Verfassungsschutzes sicher (Bundestagsdrucksache 18/4654, S. 26). Im Rahmen der arbeitsteiligen Zusammenarbeit der Verfassungsschutzbehörden von Bund und Ländern im Verbund hat dies zwangsläufig einen erweiterten Beobachtungauftrag aufseiten der Landesverfassungsschutzbehörden zur Folge, der auch nicht gewaltorientierte Bestrebungen einbezieht. Nur auf diese Weise ist sichergestellt, dass verfassungsfeindliche Bestrebungen, die sich nicht auf die Ausübung von Gewalt, sondern auf das Ausnutzen demokratischer Strukturen stützen, indem sie z. B. unter dem Deckmantel einer Partei im Sinne des Artikel 21 GG agieren, frühzeitig erkannt und mit rechtsstaatlichen Mitteln bekämpft werden können.

Zu Absatz 2

Die Befugnis zum Einsatz verdeckter Mitarbeiterinnen und Mitarbeiter als nachrichtendienstliches Mittel wird durch Absatz 2 gesetzlichen Schranken unterworfen. Insoweit übernimmt der Gesetzestext die Vorschriften des BVerfSchG inhaltlich ohne Einschränkung.

Nach Satz 1 ist eine steuernde Einflussnahme auf Personenzusammenschlüsse, die Bestrebungen verfolgen, selbst mit dem Ziel, diese abzuschwächen, ausgeschlossen. Ferner dürfen von der Verfassungsschutzbehörde keine strafbaren Vereinigungen überhaupt erst gegründet werden.

Dagegen ist nach Satz 2 die Infiltration solcher Vereinigungen generell zulässig. Ein Vereinigungsverbot steht der Aufklärung der Vereinigung von innen, durch Insider, nicht entgegen. Satz 3 regelt sonstige Maßnahmen, die rechtlich geschützte Interessen berühren. Hierbei wird zwischen Individualrechten und öffentlichen Interessen unterschieden. Soweit öffentliche Interessen berührt sind, ist die Maßnahme nur zulässig, wenn sie für die Durchführung der Aufklärung deswegen erforderlich ist, weil sie für die Akzeptanz im aufzuklärenden Umfeld unerlässlich (Nummer 2) und nicht unverhältnismäßig ist (Nummer 3). Durch den gegenüber in § 9 a Abs. 2 Satz 3 BVerfSchG geringfügig abweichenden Wortlaut soll verdeutlicht werden, dass in Satz 3 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 der Gefahr einer Enttarnung zu entgehen, was wiederum die Voraussetzung für den Zugang zu konspirativ ausgetauschten Informationen ist. Beispiele hierfür sind etwa das Verwenden von Kennzeichen verfassungswidriger Organisationen oder ein Verstoß gegen das versammlungsrechtliche Vermummungsverbot.

Die grundrechtsrelevante Regelung zu Individualrechtseingriffen erfolgt in Nummer 1 durch einen generellen Ausschluss dieser Befugnis. Unberührt bleiben sonstige bestehende Befugnisse, speziell zur Datenerhebung gemäß § 23 Abs. 1 i. V. m. § 9 Absatz 1.

Satz 4 enthält in Übereinstimmung mit dem Bundesrecht Regelungen zur Einsatzbeendigung und Informationsweitergabe an die Strafverfolgungsbehörde. Bei Straftaten von erheblicher Bedeutung soll der Einsatz grundsätzlich abgebrochen werden. Dies gilt nicht nur bei einem entsprechenden Einsatzverhalten, sondern für jedwedes Verhalten, auch wenn es nicht im Zusammenhang mit dem Einsatz steht.

Satz 5 sieht eine Ausnahme von der Einsatzbeendigung und der Informationsweitergabe an die Strafverfolgungsbehörden vor. Für die insoweit zu treffende Ermessensentscheidung liegt die Zuständigkeit bei der Leitung der Verfassungsschutzbehörde. Der Verweis auf Satz 4 stellt klar, dass es sich hierbei nicht um eine Ausnahmebefugnis zu den Verboten in Satz 1 und 3 handelt. Das Regel-/Ausnahmeverhältnis zwischen Satz 4 und 5 gibt eindeutig zu erkennen, dass das in Satz 5 eingeräumte Ermessen bei der Entscheidung über die Fortsetzung des Einsatzes und über die Unterrichtung der Strafverfolgungsbehörde restriktiv zu handhaben ist. Eine Ausnahme von der Informationsweitergabe an die Strafverfolgungsbehörde scheidet jedenfalls dann aus, soweit tatsäch-

liche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Verfolgung von Staatsschutzdelikten erforderlich ist. Die Übermittlungsverbote nach § 27 sind angesichts der rechtsstaatlichen Sensitivität des Vorgangs restriktiv anzuwenden.

Zu Absatz 3

In Absatz 3 wird auf die Bundesregelung verwiesen. Aufgrund der abschließenden Regelung der StPO hat der Bundesgesetzgeber in § 9 a Abs. 3 Satz 5 BVerfSchG die Einstellungsmöglichkeit auch für die Länder geregelt. Insoweit ist die Regelung in Absatz 3 rein deklaratorisch. Eine Einstellungsmöglichkeit besteht hiernach nur, wenn der Einsatz zur Aufklärung von Bestrebungen erfolgte, die auf die Begehung einer Straftat gemäß § 3 Abs. 1 des Artikel 10-Gesetzes gerichtet sind.

Zu Absatz 4

In Zuge des technischen Fortschritts verlagert sich die Informationsbeschaffung von der realen vermehrt in die digitale Welt. Um diesem Umstand Rechnung zu tragen, verweist Absatz 4 für Mitarbeiterinnen oder Mitarbeiter, welche verdeckt Informationen in sozialen Netzwerken und sonstigen Kommunikationsplattformen im Internet erheben (vgl. § 20 Abs. 2), auch wenn sie nicht unter einer auf Dauer angelegten Legende tätig werden, vollumfänglich auf die Absätze 1 bis 3. Eine Gleichbehandlung mit den verdeckten Mitarbeiterinnen und Mitarbeitern im Sinne des § 10 Abs. 1 ist sachlich durch die diesbezüglich vergleichbare Interessenlage gerechtfertigt. Diese 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 Teilnehmerinnen und Teilnehmer zu gewinnen.

Zu Absatz 5

Damit sich die zur Kontrolle der Verfassungsschutzbehörde berufene Parlamentarische Kontrollkommission ein Bild über die nachrichtendienstliche Zugangslage unter Einsatz von Verdeckten Mitarbeiterinnen und Mitarbeitern verschaffen kann, ist mit Absatz 5 eine regelmäßige Berichtspflicht vorgesehen, die mindestens einmal jährlich durch die Verfassungsschutzbehörde zu erfüllen ist. Die Berichtspflicht besteht über die Verweisung in § 11 Abs. 1 auch hinsichtlich des Einsatzes von Vertrauenspersonen.

Zu § 11 (Vertrauenspersonen)

Zu Absatz 1

Die Regelung verweist für den Einsatz von Vertrauenspersonen auf die Regelung zu Verdeckten Mitarbeiterinnen und Mitarbeitern. Der Anwendungsbereich des § 11 Absatz 1 in Verbindung mit § 10 Abs. 2 ist auf das der Verwaltung zurechenbare Verhalten der Vertrauensperson beschränkt. Von der Norm sind daher lediglich Tätigkeiten von Vertrauenspersonen erfasst, die im Rahmen der Auftragssteuerung durch die Verfassungsschutzbehörde erfolgen. Die Einstellungsmöglichkeit nach § 10 Abs. 3 gilt ebenfalls entsprechend.

Zu Absatz 2

Absatz 2 entspricht weitestgehend der Bundesregelung in § 9 b Abs. 2 BVerfSchG. Die Ausschlusskriterien des Anforderungsprofils sind als gemeinsame Standards von der Innenministerkonferenz in ihrer Sitzung vom 22. bis 24. Mai 2013 beschlossen und in innerdienstlichen Vorschriften bereits umgesetzt worden. Nummer 1 verbietet den Einsatz von nicht voll Geschäftsfähigen, insbesondere Minderjährigen.

Mit Nummer 2 soll verhindert werden, dass sich eine finanzielle Abhängigkeit nachteilig auf die Nachrichtenbeschaffung auswirkt. Insofern bestünde die Gefahr, dass durch solche Personen frei erfundene Sachverhalte mitgeteilt würden. Da es sich um einen persönlichen Ausschlussgrund handelt, ist Nummer 2 nicht einschlägig, wenn im besonders begründeten Einzelfall aus fachlichen Gründen einerseits Vertrauenspersonen legendengerecht entsprechend materiell unterstützt werden müssen und andererseits aus operativen Gründen zu diesem Vertrauensperson-Einsatz keine Aufklärungsalternative besteht. Soweit unter Beachtung von Nummer 2 Prämien gezahlt werden, hat die Verfassungsschutzbehörde darauf zu achten, dass die Mittel nicht etwa der aufzuklärenden Organisation zufließen. Allerdings wird realistischerweise kaum nachvollziehbar sein, aus welchen Quellen Mittel stammen, die die Vertrauensperson einem Beobachtungsobjekt zuwendet. Da sie jedoch nicht von den Prämien der Verfassungsschutzbehörde abhängig sein darf, können sie aus anderen Quellen geleistet werden.

Nummer 3 schließt eine Anwerbung von Teilnehmerinnen oder Teilnehmern eines Aussteigerprogramms aus. Insoweit steht das vorrangige Interesse entgegen, die Ausstiegsbereitschaft nicht zu gefährden.

Nummer 4 soll die Unabhängigkeit von Parlamentsabgeordneten schützen. Erfasst werden nicht nur Abgeordnete des Bundes oder Landes, sondern auch solche, die auf Ebene der Europäischen Union gewählt wurden.

Nummer 5 normiert einen Ausschlussgrund wegen vorausgegangener Straftaten, da diese die Ungeeignetheit einer Person indizieren. In Abweichung zur bundesrechtlichen Regelung wird klarstellend in der zweiten Alternative jedoch darauf abgestellt, ob sich in dem Bundeszentralregister Eintragungen von Freiheitsstrafen wegen eines Vergehens von erheblicher Bedeutung, deren Vollstreckung nicht zur Bewährung ausgesetzt wurde, befinden. Ausschlusskriterium ist nicht die Freiheitsstrafe als solche, die vollstreckt wurde, sondern die Schwere der begangenen Tat. Insoweit werden nicht grundsätzlich solche Personen als ungeeignet angesehen, deren Sozialprognose im Sinne des § 56 StGB lediglich aufgrund mehrmaliger Tatbegehungen von nicht erheblichen Straftaten als negativ beurteilt werden musste (z. B. bei mehrfacher Leistungserschleichung gemäß § 265 a StGB).

Satz 2 lässt unter engen Voraussetzungen Ausnahmen von Satz 1 Nummer 5 unter Abwägung der konkreten Umstände zu. Hierbei ist im Rahmen der Abwägung zum einen personenbezogen der Stand der Resozialisierung mit einzubeziehen. Soweit der früheren Straftat keine indizielle Wirkung mehr dafür zukommt, dass die Person im Einsatz unzuverlässig sein wird, steht einer Verpflichtung insoweit nichts entgegen. Zum anderen muss objektbezogen das Ausmaß der Bedrohung und die Verfügbarkeit alternativer Nachrichtenzugänge betrachtet werden. Zur Aufklärung terroristischer Organisationen müssen unter ganz besonderen Umständen wegen der herausragenden Gefährdung womöglich Vorbestrafte unabhängig vom Resozialisierungsstand als Vertrauensperson einsetzbar sein, wenn dieser Nachrichtenzugang alternativlos ist.

Eine absolute Grenze gilt jedoch bei der Verurteilung als Täterin oder Täter eines Totschlags oder einer allein mit lebenslanger Freiheitsstrafe bedrohten Straftat. Solche durch die Rechtsordnung mit dem Höchstmaß der Strafzumessung belegten Fälle schwerster Kriminalität schließen eine Anwerbung als Vertrauensperson aus.

Durch die Zuständigkeitsregelung in Satz 3 ist verfahrensmäßig eine besondere Prüfung generell gewährleistet und damit zugleich auch die besondere Würdigung von Ausnahmesachverhalten.

Zu § 12 (Überwachung des Brief-, Post- und Fernmeldeverkehrs)

Die Bestimmung verweist hinsichtlich der Überwachung des Brief-, Post- und Fernmeldeverkehrs und der Verarbeitung der dabei erhobenen personenbezogenen Daten deklaratorisch auf die Vorschriften des Artikel 10-Gesetzes.

Zu § 13 (Besondere Auskunftsverlangen)

In Absatz 1 bis 3 werden die Auskunftsverlangen gegenüber Verkehrsgesellschaften, Kreditinstituten und Postdienstleistern im Wesentlichen gemäß der geltenden Rechtslage in den Gesetzentwurf übernommen. Die Vorschrift deckt sich insoweit mit § 8 a Abs. 2 Satz 1 Nr. 1 und 2 BVerfSchG. Die Befugnisse werden auf die Beobachtung extremistischer Bestrebungen gemäß § 5 Satz 1 Nr. 1 ausgedehnt. Das BVerfG hat bereits eine entsprechende Ausdehnung bei Erhebungen von Kontoinhalten und Kontobewegungen ausdrücklich für verfassungsgemäß angesehen (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 313 – juris).

Zu Absatz 1

Die Regelung entspricht im Wesentlichen der bisherigen Rechtslage in § 10 a Abs. 1 LVerfSchG, wird allerdings auf Bestrebungen gemäß § 5 Satz 1 Nummer 1 erweitert. In Absatz 1 Satz 2 wird die Befugnis zur Kontostammdatenauskunft geschaffen, für die der Bundesgesetzgeber gemäß § 93 Abs. 8 Satz 1 Nummer 3 Abgabenordnung (AO) eine Öffnungsklausel für den Landesgesetzgeber vorgesehen hat. Danach erteilt das Bundeszentralamt für Steuern den Verfassungsschutzbehörden der Länder auf Ersuchen Auskunft über die in § 93 b Abs. 1 AO bezeichneten Bestandsdaten (sog. Kontostammdaten), soweit dies für ihre Aufgabenerfüllung erforderlich ist und durch Landesgesetz ausdrücklich zugelassen wird. Kontostammdaten sind insbesondere die Nummer eines Kontos oder eines Depots, der Tag der Einrichtung und der Tag der Auflösung, die Namen sowie – bei natürlichen Personen – der Geburtstag des Inhabers oder Verfügungsberechtigten (§ 93 b Abs. 1 AO in Verbindung mit § 24 c Abs. 1 des Kreditwesengesetzes). Die Kontostammdatenauskunft kann dabei insbesondere der Vorbereitung einer Auskunft über Kontoinhaltsdaten und Kontobewegungen nach Absatz 1 Satz 1 dienen, für welche überhaupt ein kontoführendes Institut bekannt sein muss.

Zu Absatz 2

Absatz 2 Satz 1 entspricht weitgehend der geltenden Regelung in § 10 a Abs. 2 LVerfSchG, wird allerdings auf Bestrebungen gemäß § 5 Satz 1 Nummer 1 erweitert (vgl. oben). Der ausdrücklich weit gefasste Begriff der Verkehrsunternehmen trägt den 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 die Verfassungsschutzbehörde die Befugnis, künftig u. a. auch bei Fernbus- und Eisenbahntransportunternehmen Auskünfte einzuholen. Zu Auskünften, insbesondere zu Flugverkehrsdaten, sind gemäß Absatz 2 Satz 2 zukünftig auch die Betreiber von Computerreservierungssystemen (CRS) und globalen Distributionssystemen verpflichtet (GDS). Diese Erweiterung trägt dem Umstand Rechnung, dass die Betreiber von CRS und GDS digitale reise- und informationslogistische Systeme mit relevanten Reisedaten (u. a. Kundendaten, Vakanzen, Leistungen etc.) bereithalten, die insbesondere Fluglinien aber auch Reiseanbieter nutzen und die relevanten Daten darin einspeisen.

Zu Absatz 3

Absatz 3 entspricht der geltenden Regelung in § 10 a Abs. 3 LVerfSchG, wird allerdings auf Bestrebungen gemäß § 5 Satz 1 Nummer 1 erweitert (vgl. oben). Der Eingriff in Artikel 10 GG bedingt die Erfüllung der Voraussetzungen des § 3 Abs. 1 Artikel 10-Gesetz sowie das Verfahren in Absatz 7.

Zu Absatz 4

Absatz 4 entspricht der bisherigen Regelung in § 10 a Abs. 4 LVerfSchG. Es wurden lediglich zur Rechtsklarheit redaktionelle Änderungen vorgenommen. So wurde der veraltete Begriff der Teledienste durch den Begriff Telemedien ersetzt sowie klargestellt, dass Telekommunikationsverbindungsdaten Verkehrsdaten gemäß § 96 Abs. 1 Satz 1 Nr. 1 bis 5 Telekommunikationsgesetz (TKG) und Telemediennutzungsdaten Nutzungsdaten gemäß § 15 Abs. 1 Satz 2 Nr. 1 bis 3 Telemediengesetz (TMG) umfassen.

Zu Absatz 5

Absatz 5 schafft die Befugnis zur Auskunft über Telekommunikations-Bestandsdaten nach § 113 Abs. 1 TKG. Die Regelungsmöglichkeit ist in § 113 Abs. 3 Nummer 3 TKG für die Verfassungsschutzbehörden der Länder ausdrücklich vorgesehen. Während für das automatisierte Auskunftsverfahren nach § 112 TKG, bei dem die Bundesnetzagentur die Daten auf Ersuchen an die in § 112 Abs. 2 TKG genannten Behörden zu übermitteln hat, eine schlichte Datenerhebungsgeneralklausel genügt, hat das BVerfG bereits im Jahr 2012 eine eigene Landesregelung für das manuelle Auskunftsverfahren für erforderlich gehalten (Beschluss vom 24. Januar 2012, 1 BvR 1299/05). Die Regelung in Absatz 5 Satz 1 erlaubt es zur Erfüllung der Aufgaben des Verfassungsschutzes gemäß § 5 die von den Telekommunikationsunternehmen nach §§ 95 und 111 TKG gespeicherten Bestandsdaten zu erheben.

Die Telekommunikationsunternehmen sind nach § 111 TKG verpflichtet, die von ihnen vergebenen bzw. bereitgestellten Rufnummern, Anschlusskennungen, Mobilfunkendgerätenummern sowie die zugehörigen Daten der Anschlussinhaber wie Namen, Anschrift und Geburtsdaten (Bestandsdaten) zu speichern, um diese für die Aufgabenwahrnehmung der Sicherheitsbehörden verfügbar zu halten und die Datenbasis für die in §§ 112 und 113 TKG geregelten automatisierten und manuellen Auskunftsverfahren zu schaffen.

Die von § 111 TKG erfassten Daten ermöglichen die individualisierende Zuordnung von Telekommunikationsnummern

zu den jeweiligen Anschlussinhabern und damit zu deren potenziellen und typischen Nutzerinnen oder Nutzern. Nähere private Daten enthalten Bestandsdaten nicht. Insbesondere umfassen sie weder höchstpersönliche Informationen noch ist mit ihnen die Erstellung von Persönlichkeits- oder Bewegungsprofilen möglich.

Gemäß § 113 Abs. 1 Satz 2 TKG in Verbindung mit Absatz 5 Satz 2 erstreckt sich die Auskunftsbefugnis auch auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen geschützt wird (z. B. Pass- und Codewörter, Persönliche Identifikationsnummern [PIN] oder Personal Unblocking Keys [PUK]). Das BVerfG hat dazu allerdings ausgeführt, dass die Sicherheitsbehörden diese nur dann verlangen können, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind (Beschluss vom 24. Januar 2012, 1 BvR 1299/05). Soweit ein Zugriff auf Endgeräte im Rahmen des § 20 Absatz 3 erfolgen soll, müssen daher die dort aufgeführten Voraussetzungen des Artikel 10-Gesetzes erfüllt sein.

Gemäß § 113 Abs. 1 Satz 3 TKG i. V. m. Absatz 5 Satz 3 ist es auch zulässig, die Auskunft anhand einer dynamischen Internetprotokoll-Adresse (IP-Adresse) vorzunehmen. Dazu bedarf es allerdings in einem Zwischenschritt eines Rückgriffs auf Verkehrsdaten, weshalb das BVerfG für diese Fallkonstellation einen Eingriff in Artikel 10 Absatz 1 GG annimmt (Beschluss vom 24. Januar 2012, 1 BvR 1299/05). Für Auskünfte nach Absatz 5 Satz 3 ist daher ein besonderes Verfahren zur Einbeziehung der G10-Kommision in Absatz 9 vorgesehen.

Absatz 5 Satz 4 enthält die der Auskunftspflicht zu Telekommunikations-Bestandsdaten entsprechende Befugnis, Anbieter von Telemedien um Auskunft zu Bestandsdaten zu ersuchen. Die dem § 113 TKG entsprechende Öffnungsklausel ist in § 14 Abs. 2 TMG geregelt. Telemedien sind elektronische Informations- und Kommunikationsdienste, soweit sie nicht der Telekommunikation oder dem Rundfunk zuzuordnen sind. Bei Telemedien steht die Bereitstellung von Informationen im Vordergrund. Dagegen kommt es bei der Telekommunikation nicht auf die Bereitstellung von Informationen an, sondern auf die Bereitstellung von Datenübertragungsmöglichkeiten (z. B. das Telefon). Telemediendienste und Anwendungsfälle sind z. B. Auskünfte über Vertragsdaten bei Internetauktionshäusern und -tauschbörsen, über die Handel und Vertrieb volksverhetzender Propagandamaterialien betrieben wird. Eine Auskunft darüber, ob eine Person bei solchen Unternehmen als sogenannter „Powerseller“ registriert ist, also regelmäßig Waren in größerem Umfang an- und verkauft, kann beispielsweise Rückschlüsse auf die Beschaffung von Finanzmitteln ermöglichen. Weitere Telemedien sind Online-Angebote von Waren oder Dienstleistungen, Internetsuchmaschinen, Telebanking, Online-Computerspiele, Streaming-Plattformen und wohl auch Messenger-Dienste wie WhatsApp oder Skype.

Zu Absatz 6

Mit Absatz 6 Satz 1 wird klargestellt, dass die Verfassungsschutzbehörde ihr Auskunftsverlangen nicht begründen muss, sofern gesetzlich nichts anderes bestimmt ist. Wegen einer fehlenden Begründung darf daher ein Auskunftsverlangen nach den Absätzen 1 bis 5 nicht abgelehnt werden, was dem von der Verfassungsschutzbehörde zu beachtenden Methoden- und ggf. Quellenschutz Rechnung trägt. Dem entsprechend liegt die Verantwortung für die Zulässigkeit des Auskunftsverlangens regelmäßig bei der anfragenden Sicherheitsbehörde, hier der Verfassungsschutzbehörde (vgl. § 25 Abs. 2 Satz 2 und z. B. § 113 Abs. 2 Satz 4 TKG). In der Regel reicht daher bei dem Auskunftsverlangen die Angabe einer gesetzlichen Bestimmung aus, die der Verfassungsschutzbehörde eine Erhebung der angefragten Daten erlaubt (vgl. etwa § 113 Abs. 2 Satz 1 Halbsatz 1 TKG).

Nach Absatz 6 Satz 2 sind die in den Absätzen 1 bis 3 genannten Unternehmen und Dienstleister zur unentgeltlichen Auskunft verpflichtet. Die zur Auskunft verpflichteten Telekommunikations- und Telemedienunternehmen nach Absatz 4 und 5 haben die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Für Auskünfte nach den Absätzen 4 und 5 Satz 3 ist eine Aufwandsentschädigung zu gewähren, die sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes bemisst. Die Auskunftsersuchen nach den Absätzen 1 bis 5 sowie die Auskunft selbst sind durch die zur Auskunft verpflichteten Unternehmen und Dienstleister gegenüber den Betroffenen und Dritten geheim zu halten.

Zu Absatz 7

Die Bestimmung entspricht im Wesentlichen der geltenden Regelung in § 10 a Abs. 5 LVerfSchG. Auskünfte und Erhebungen, welche Rückschlüsse auf höchstpersönliche Informationen sowie Persönlichkeits- und Bewegungsprofile ermöglichen oder Eingriffe in Artikel 10 GG darstellen, sind an das Verfahren in Absatz 7 gebunden. Dies betrifft die Auskünfte nach Absatz 1 Satz 1 (Auskünfte über Kontoinhaltsdaten und Kontobewegungen), Absatz 2 (Auskünfte über Transportverkehrsdaten), Absatz 3 (Auskünfte über den Postverkehr) und Absatz 4 (Auskünfte über Verkehrsdaten der Telekommunikation und Telemedien). Durch das Verfahren ist eine vorherige und unabhängige Kontrolle garantiert. Es bedarf hierzu der Anträge durch die G 10-Aufsichtsbeamtin oder den G 10-Aufsichtsbeamten und der Entscheidung durch die Leitung der Verfassungsschutzbehörde. Die Unterrichtung der G 10-Kommission hat durch die zuständige Ministerin oder den zuständigen Minister vor dem Vollzug zu erfolgen. Bei Gefahr in Verzug kann die Vollziehung auch vor der Unterrichtung erfolgen.

Dem Verfahren nach Absatz 7 nicht unterworfen sind Auskünfte über bloße Bestandsdaten, welche keine besonderen persönlichkeitsrelevanten Rückschlüsse zulassen. Gleiches gilt für die Deanonymisierung nach Absatz 5 Satz 3. Die neu geregelte Befugnis zur Kontostammdatenauskunft (Absatz 1 Satz 2) sowie zur Bestandsdatenauskunft bei Telekommunikations- und Telemedienanbietern (Absatz 5) stellt zwar einen Eingriff in die informationelle Selbstbestimmung dar, jedoch ist dieser verhältnismäßig gering.

Zu Absatz 8

Für die erhobenen personenbezogenen Daten gemäß Absatz 1 Satz 1 (Auskünfte über Kontoinhaltsdaten und Kontobewegungen), Absatz 2 (Auskünfte über Transportverkehrsdaten), Absatz 3 (Auskünfte über den Postverkehr), Absatz 4 (Auskünfte über Verkehrsdaten der Telekommunikation und Telemedien) sowie Absatz 5 Satz 3 (Deanonymisierung der dynamischen IP-Adresse) gelten die besonderen Datenschutzvorschriften des § 4 Artikel 10-Gesetz.

Zu Absatz 9

Wie bereits ausgeführt, geht das BVerfG davon aus, dass die Auskunft über Bestandsdaten der Telekommunikation anhand einer vom Telekommunikationsdiensteanbieter dynamisch vergebenen IP-Adresse einen Eingriff in den Schutzbereich des Artikel 10 Abs. 1 GG darstellt, da hierzu in einem Zwischenschritt ein Rückgriff auf Verkehrsdaten erforderlich ist (Beschluss vom 24. Januar 2012, 1 BvR 1299/05).

Ein diesbezüglicher Eingriff dürfte sich allerdings auf der untersten Stufe bewegen. Von der entsprechenden Auskunft sind keine Inhaltsdaten betroffen und auch die Verkehrsdaten der Kommunikation nur mittelbar. Insbesondere werden die Verkehrsdaten auf der Grundlage des § 113 Abs. 1 TKG nicht an den Bedarfsträger, hier die Verfassungsschutzbehörde, übermittelt. Sie werden lediglich für die Deanonymisierung von IP-Adressen ausgewertet. Dies dürfte regelmäßig automatisiert erfolgen, sodass selbst der Telekommunikationsdiensteanbieter die näheren Umstände der Kommunikationsvorgänge im Zuge der Auswertung nicht persönlich zur Kenntnis nimmt und damit im Übrigen die Vertraulichkeit dieser Informationen gewahrt bleibt.

Insoweit wird für Maßnahmen nach Absatz 5 Satz 3 nicht das formalisierte Antragsverfahren nach Absatz 7 gegenüber der G10-Kommission vorgesehen, da der entsprechende Aufwand – gemessen an der Eingriffsintensität – nicht angemessen wäre. Vielmehr erfolgt in diesen Fällen eine Beteiligung der G10-Kommission durch eine mindestens einmal jährlich stattfindende Unterrichtung über die nach Absatz 5 Satz 3 durchgeführten Maßnahmen (Satz 1) sowie die Befugnis der Kommission, jederzeit Einsicht in alle Unterlagen zu durchgeführten oder laufenden Maßnahmen nach Absatz 5 Satz 3 nehmen und deren Vorlage verlangen zu können (Satz 2).

Die G10-Kommission hat insoweit ein durchgängiges Informations-, Überprüfungs- und Interventionsrecht, dass mit Blick auf die geringe Eingriffstiefe von Maßnahmen nach Absatz 5 Satz 3 den Anforderungen des Artikel 10 Abs. 2 GG genügt.

Zu Absatz 10

Die Bestimmung entspricht der bisherigen Regelung in § 10 a Absatz 8 LVerfSchG und regelt die Berichtspflichten gegenüber dem parlamentarischen Kontrollgremium des Bundes.

Zu § 14 (Funkzellenabfrage)

Zu Absatz 1

Zur Aufgabenerfüllung des Verfassungsschutzes nach § 5 kann es erforderlich sein, sämtliche Telekommunikationsverkehrsdaten, die im Mobilfunknetz in einem bestimmten Bereich zu einer bestimmten Zeit anfallen, zu ermitteln. Zu diesem Zweck können mit der sog. Funkzellenabfrage alle Verkehrsdaten abgefragt werden, die innerhalb der relevanten Zeit über eine oder mehrere Funkzellen abgewickelt worden sind. Die Funkzellenabfrage stellt einen Eingriff in Artikel 10 GG dar, da zum von Artikel 10 GG geschützten Fernmeldegeheimnis auch die Kommunikationsumstände, insbesondere ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist, gehören. Die Maßnahme ist daher nur unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes zulässig. Zudem muss die Erreichung des Zwecks der Maßnahme anderenfalls erheblich erschwert sein. Die grundsätzliche Zulässigkeit einer Maßnahme, bei der unbeteiligte Dritte in nicht vermeidbarer Weise betroffen sind, richtet sich nach § 9 Abs. 1 Satz 2.

Zu Absatz 2

Nach Absatz 2 bedarf die Maßnahme der Anordnung der Leitung der Verfassungsschutzbehörde. Die G 10-Kommission ist grundsätzlich, soweit keine Gefahr im Verzug vorliegt, vorab zu unterrichten.

Zu Absatz 3

Absatz 3 bestimmt die Mindestinhalte der Anordnung. Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um höchstens denselben Zeitraum ist zulässig, soweit die Voraussetzungen nach Absatz 1 weiterhin vorliegen. Hinsichtlich der Verarbeitung der auf diese Weise erhobenen Daten gelten die besonderen Datenschutzvorschriften des § 4 des Artikel 10-Gesetzes entsprechend.

Vor dem Hintergrund der nicht vermeidbaren Erfassung von Daten Unbeteiligter wird geregelt, dass die erhobenen Daten unverzüglich zu löschen sind, soweit sie für die Aufgabenerfüllung der Verfassungsschutzbehörde nicht mehr erforderlich sind. Weiter sind die Betroffenen, soweit keine Löschung erfolgt ist, nach Beendigung der Maßnahme über diese zu benachrichtigen.

Zu Absatz 4

Die Telekommunikationsanbieter haben unverzüglich Auskunft über die angefallenen Verkehrsdaten zu erteilen. Erfasst sind auch solche Daten, die nach der Anordnung angefallen sind. Soweit die Telekommunikationsanbieter für die Möglichkeit einer Auskunftserteilung Vorkehrungen treffen müssen, richtet sich dies nach dem Telekommunikationsgesetz und auf dessen Grundlage erlassener Rechtsvorschriften. Hinsichtlich der Entschädigung gilt § 13 Abs. 6 Satz 4 entsprechend.

Zu § 15 (Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten)

§ 15 regelt die Befugnis zum Einsatz des sog. IMSI-Catchers. Ein solcher ermöglicht es, die auf der Chipkarte eines Mobilfunktelefons gespeicherte Internationale Mobilfunk-Teilnehmerkennung (International Mobile Subscriber Identity, kurz IMSI) auszulesen und den Standort des aktiv geschalteten Mobilfunktelefons innerhalb einer Funkzelle näher zu bestimmen. Darüber hinaus kann auch die Gerätenummer (International Mobile Equipment Identity, kurz IMEI) erhoben werden, was von Bedeutung ist, wenn mehrere oder wechselnde SIM-Karten genutzt werden. Der IMSI-Catcher simuliert dabei gegenüber einem betriebsbereiten Mobiltelefon eine Art mobile Funkzelle, sodass dieses genau wie alle anderen im Einzugsbereich befindlichen betriebsbereiten Mobilfunkgeräte ihre Daten an den IMSI-Catcher senden. Wie das BVerfG klargestellt hat, greift der Einsatz eines IMSI-Catchers nicht in das von Artikel 10 GG 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, Nichtannahmebeschluss vom 22. August 2006, 2 BvR 1345/03 – juris). Vielmehr dient der Einsatz des IMSI-Catchers neben der ungefähren Ortung erst der Vorbereitung von späteren Beschränkungsmaßnahmen

nach dem Artikel 10-Gesetz oder auch von Telekommunikations-Verkehrsdatenauskünften (§ 13 Abs. 4). Der IMSI-Catcher-Einsatz stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Zu Absatz 1

Zur Erfüllung der Aufgaben nach § 5 darf die Verfassungsschutzbehörde unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes technische Mittel zur Ermittlung der Geräte- und Kartennummer oder zu Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes einsetzen. Gleichwohl der Einsatz eines IMSI-Catchers keinen Eingriff in Artikel 10 GG darstellt, so wird der Einsatz dennoch von den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes abhängig gemacht. Diese Gleichsetzung ist in der Praxis gerechtfertigt, da der Einsatz des IMSI-Catchers neben der Ermittlung von Standortdaten vor allem der Vorbereitung einer sich anschließenden Beschränkungsmaßnahme nach dem Artikel 10-Gesetz dient und die Voraussetzungen hierfür erfüllt sein müssen.

Zu Absatz 2

Personenbezogene Daten unbeteiligter Dritter dürfen nur bei technischer Unvermeidbarkeit erhoben werden. Über den Datenabgleich zur Ermittlung der Geräte- oder Kartennummer oder des Standortes eines mobilen Telekommunikationsendgerätes hinaus, dürfen diese Daten nicht verwendet werden. Ein solcher Datenabgleich zur Ermittlung der gesuchten Kennungen kann erforderlich sein, wenn sich in der simulierten Funkzelle mehrere Mobilfunkteilnehmer befinden. Dann sind zur Bestimmung des gesuchten Mobiltelefons mehrere Messungen an verschiedenen Orten erforderlich, wobei nach einem statistischen Auswerteprinzip die jeweiligen IMSI/IMEI ermittelt oder eingegrenzt werden (BVerfG, Nichtannahmebeschluss vom 22. August 2006, 2 BvR 1345/03 – juris).

Zu Absatz 3

Mit Absatz 3 wird das in § 14 näher ausgeführte Verfahren zur Anordnung der Maßnahme für entsprechend anwendbar erklärt.

Zu § 16 (Inbesitznahme von Sachen)

Gemäß § 16 darf die Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben nach § 5 vorübergehend Sachen zur Datenerhebung heimlich in Besitz nehmen. Hierunter fällt vornehmlich die Inbesitznahme von Datenträgern (konventionelle Unterlagen ebenso wie elektronische Speicherung) zu deren Auslesung. Die Befugnis umfasst auch die Benutzung der Sache, insbesondere die Inbetriebnahme, sofern diese für die Datenerhebung bzw. Auslesung erforderlich ist. Die Regelung beschränkt das Besitzrecht des Besitzers, womit ein Eingriff gerechtfertigt werden kann. Eine Veränderung, insbesondere elektronischer Unterlagen, ist jedoch von der Maßnahme nicht umfasst. Maßnahmen nach § 16 können dann zur Aufgabenerfüllung der Verfassungsschutzbehörde notwendig sein, wenn z. B. relevante Personen im Sinne des § 9 Abs. 3 auf Grund einer Ausschreibung der Verfassungsschutzbehörde bei der Einreise nach Deutschland festgestellt werden. Insoweit kann es erforderlich sein, mit sich geführte Unterlagen der Person zu sichten.

Zu § 17 (Einsatz technischer Mittel zur akustischen Überwachung außerhalb von Wohnungen)

Zu Absatz 1

Absatz 1 sieht den Einsatz technischer Mittel zur akustischen Überwachung außerhalb der Wohnung vor. Keine Wohnung i. S. d. Artikel 13 GG sind z. B. Autos (soweit nicht zu Wohnzwecken geeignet und genutzt), umfriedete Flächen, die nicht im Zusammenhang mit Wohnzwecken stehen oder der Öffentlichkeit zugängliche Räume. Verfassungsrechtlich sind solche Maßnahmen als Eingriff in das Recht auf informationelle Selbstbestimmung in seiner Ausprägung als Recht am eigenen Wort zu beurteilen (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG). Auf Grund der Eingriffsintensität müssen tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 genannten Schutzgüter vorliegen. Des Weiteren muss die Maßnahme zur Aufgabenerfüllung erforderlich sein sowie die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert sein.

Zu Absatz 2

Nach Absatz 2 bedarf die Maßnahme der Anordnung der Leitung der Verfassungsschutzbehörde. Hierdurch wird sichergestellt, dass mit Blick auf das besondere Gewicht der Maßnahme für Betroffene die Entscheidung hierüber auf einer entsprechend hohen Ebene getroffen wird. Vor dem Vollzug der Maßnahme ist die nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildete Kommission zu unterrichten. In Eilfällen ist die Unterrichtung nachzuholen.

Zu § 18 (Einsatz technischer Mittel zur Wohnraumüberwachung)

Die Befugnis zum Einsatz technischer Mittel zur optischen und akustischen Wohnraumüberwachung ist bereits nach der bisherigen Rechtslage vorgesehen (§§ 10 b und 10 c LVerfSchG). Nach dem Urteil des BVerfG zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) bedarf es der Anpassung dieser Vorschriften. Das BVerfG hat die konkrete Ausgestaltung der polizeilichen Ermächtigungen im BKA-Gesetz zum Einsatz heimlicher Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus für teilweise unverhältnismäßig und damit verfassungswidrig angesehen. Es hat ausgeführt, dass Eingriffsbefugnisse, die wie die Wohnraumüberwachung oder die Onlinedurchsuchung tief in die Privatsphäre eingreifen, als Ausfluss des Verhältnismäßigkeitsgrundsatzes besonders strengen Vorgaben an ihre Ausgestaltung unterliegen. Darüber hinaus hat es den Schutz des Kernbereichs privater Lebensgestaltung fortgeschrieben sowie die in der Rechtsprechung der letzten Jahre entwickelten Kriterien für die Zulässigkeit heimlicher Überwachungsmaßnahmen im Vorfeld von Terrorgefahren präzisiert. Obwohl die Entscheidung des BVerfG zu polizeilichen Befugnissen ergangen ist, so ist es dennoch sachgerecht und folgerichtig, die wesentlichen Vorgaben des BVerfG, soweit diese nicht mit bereichsspezifischen Grundlinien des Nachrichtendienstrechts kollidieren, zu übernehmen.

Zu Absatz 1

Absatz 1 Satz 1 entspricht der bisherigen Rechtslage in § 10 b Abs. 1 Satz 1 LVerfSchG. Danach darf die Verfassungsschutz-

behörde im Rahmen ihrer Beobachtungsaufgaben zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder Lebensgefahr, technische Mittel zur optischen oder akustischen Überwachung von Wohnungen einsetzen.

Nach Absatz 1 Satz 2 ist eine Wohnraumüberwachung zukünftig auch zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums die in Satz 1 genannten Rechtsgüter schädigen wird. Mit dieser Änderung werden die durch das BVerfG entwickelten Prognosekriterien aufgenommen und umgesetzt. Mit dieser Prognosemöglichkeit, die nicht an ein konkretes Schadensereignis, sondern an das individuelle Verhalten einer Person anknüpft, will das BVerfG den Besonderheiten bei Terrorgefahren Rechnung tragen. Oftmals liegen den Sicherheitsbehörden der Polizei und des Verfassungsschutzes nur Erkenntnisse darüber vor, dass bestimmte Personen Attentate in Deutschland planen; das drohende Schadensereignis selbst kann aber noch nicht konkret beschrieben werden. Anders formuliert: Die vorhandenen Tatsachen lassen noch nicht den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zu. In diesen Fällen kann die Prognose statt auf das Ergebnis eines Schadensverlaufs auch auf das Verhalten eines Schädigers – hier eines Terroristen – gerichtet werden. Polizeiliche Überwachungsmaßnahmen sind dann bereits zulässig, wenn Tatsachen die Annahme rechtfertigen, dass eine Person mit hinreichender Wahrscheinlichkeit terroristische Straftaten begehen wird. Für den Verfassungsschutz gelten die bundesverfassungsgerichtlich zugestandenen Befugnisse im Vorfeld konkreter Terrorgefahren uneingeschränkt und erst recht. Dem Wesen einer nachrichtendienstlichen Gefahrenerforschungsbehörde entsprechend besteht die Hauptaufgabe des Verfassungsschutzes in der verdeckten Vorfeldaufklärung extremistischer und terroristischer Bestrebungen.

Zu Absatz 2

Die Bestimmung entspricht mit redaktionellen Änderungen der bisherigen Regelung in § 10 b Abs. 1 Satz 2 LVerfSchG und regelt den Einsatz technischer Mittel zur Wohnraumüberwachung ausschließlich zum Schutz der für den Verfassungsschutz tätigen Personen, z. B. bei heimlichen Quellentreffen in Wohnungen. Die Anordnung erfolgt durch die Leitung der Verfassungsschutzbehörde und bedarf einer richterlichen Bestätigung nur, wenn die aus der Maßnahme erlangten Erkenntnisse verwertet werden sollen (vgl. § 19 Abs. 2).

Zu Absatz 3

Nach Absatz 3 darf die Maßnahme nur in Wohnungen von Personen durchgeführt werden, gegen die aufgrund tatsächlicher Anhaltspunkte der Verdacht von Bestrebungen oder Tätigkeiten nach § 5 besteht. Die Vorschrift dient der Anpassung an die Vorgaben des BVerfG im Urteil zum BKA-Gesetz, wonach sich besonders eingriffsintensive Maßnahmen wie die Wohnraumüberwachung nur unmittelbar gegen diejenigen als Zielpersonen richten dürfen, die für die Gefahr verantwortlich sind (BVerfG, a. a. O., Rn. 114 f.). Die zielgerichtete Überwachung von Kontakt- und Begleitpersonen (vgl. bisherige Regelung in § 10 b Abs. 2 Satz 2 LVerfSchG) ist dagegen unzulässig und wird dem entsprechend gestrichen. Das BVerfG hat es allerdings für verfassungsrechtlich zulässig erachtet, wenn von einer Wohnraumüberwachung auch Dritte betroffen sind. So kann die Überwachung der Wohnung von Dritten erlaubt werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass sich die verantwortliche Person während der Überwachung dort aufhält, für die Ermittlungen relevante Gespräche führen wird und eine Überwachung seiner Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht (BVerfG, a. a. O., Rn. 115). Damit übereinstimmend wird in Absatz 3 Satz 2 die Überwachung der Wohnung einer dritten Person geregelt, wenn Tatsachen die Annahme rechtfertigen, dass sich die Zielperson dort aufhält und die Überwachung der Wohnung allein dieser Person zur Erforschung des Sachverhalts nicht Erfolg versprechend erscheint.

Zu Absatz 4

Die Anordnung der Wohnraumüberwachung nach Absatz 1 erfolgt gemäß Artikel 13 Abs. 4 GG durch ein Gericht. Die Eilanordnungskompetenz bei Gefahr im Verzug gemäß der bisherigen Regelung in § 10 b Abs. 4 Satz 2 LVerfSchG wird gestrichen. In einer dafür bedingten „Ad-hoc“-Lage lassen die komplexen und zeitintensiven Planungs- und Umsetzungserfordernisse der tatsächlichen Durchführung einer Wohnraumüberwachung die richterliche Entscheidung nicht unaufschiebbar werden. Im Übrigen kann eine gerichtliche Entscheidung in der Praxis sehr zeitnah eingeholt werden.

Zu Absatz 5

Die Bestimmung entspricht der bisherigen Regelung in § 10 b Abs. 5 LVerfSchG und regelt die formellen Anforderungen der Anordnung sowie die Befristung der Maßnahme auf einen Monat sowie die Verlängerungsmöglichkeit um den gleichen Zeitraum.

Zu Absatz 6

Die Bestimmung entspricht im Wesentlichen der bisherigen Regelung in § 10 b Abs. 6 LVerfSchG zum Kernbereichsschutz. In Satz 4 wird bezüglich der Verwertung von Daten auf das Artikel 10-Gesetz verwiesen. An die Stelle des Gerichts tritt in dieser Hinsicht die G 10-Kommission als die für den Verfassungsschutz vorgesehene unabhängige Kontrollinstanz. Eine unabhängige Sichtung von Aufzeichnungen aus einer Wohnraumüberwachung vor der Verwendung der Daten dient der verfahrensrechtlichen Absicherung des Kernbereichsschutzes der persönlichen Lebensführung auf der Auswertungsebene. Diese Sichtung erfolgt für den Bereich des Verfassungsschutzes über die Verweisung auf § 2 Abs. 3 des Landesgesetzes zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses durch die G 10-Kommission.

Zu Absatz 7

Absatz 7 entspricht im Wesentlichen dem bisherigen § 10 b Abs. 7 LVerfSchG. In Absatz 7 Satz 3 werden allerdings entsprechend den bereits zu Absatz 3 gemachten Ausführungen Kontakt- und Begleitpersonen nicht mehr mit aufgeführt. Eingriffe in das nach §§ 53 und 53 a StPO geschützte Vertrauensverhältnis sind danach auch dann nicht zulässig, wenn sich die zeugnisverweigerungsberechtigte Berufsgeheimnisträgerin/Berufshelferin oder der zeugnisverweigerungsberechtigte Berufsgeheimnisträger/Berufshelfer als Kontakt- oder Begleitpersonen erweist.

§ 19 (Besondere Bestimmungen für Maßnahmen nach § 18)

Zu Absatz 1

Die Bestimmung entspricht mit redaktionellen Änderungen der bisherigen Regelung in § 10 c Abs. 1 LVerfSchG zum Kernbereichsschutz auf der Auswertungsebene.

Zu Absatz 2

Die Regelung entspricht dem bisherigen § 10 c Abs. 2 LVerfSchG.

Zu Absatz 3 und 4

Die Bestimmungen entsprechen mit redaktionellen Änderungen den bisherigen Regelungen zu den Kennzeichnungspflichten in § 10 c Abs. 4 und 5 LVerfSchG.

Zu Absatz 5

Die Regelung stellt eine besondere Datenübermittlungsvorschrift dar. Die bisherige Bestimmung des § 10 c Abs. 6 LVerfSchG bedarf der Anpassung aufgrund der Vorgaben des BVerfG im Urteil zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09). Bei der besonders eingriffsintensiven Überwachungsmaßnahme der Wohnraumüberwachung gilt eine besonders enge Bindung jeder weiteren Nutzung der bei einer solchen Maßnahme gewonnenen personenbezogenen Daten an die Voraussetzungen und Zwecke der Datenerhebung. Eine zweckändernde Datenverwendung muss sich am Grundsatz der hypothetischen Datenneuerhebung orientieren. Danach gilt, dass die Verarbeitung der erhobenen Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen muss, die verfassungsrechtlich die Neuerhebung der Daten mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Bei der Übermittlung zu Zwecken der Gefahrenabwehr nach Absatz 5 Satz 1 Nummer 1 sowie zu Zwecken der Strafverfolgung nach Absatz 5 Satz 1 Nummer 2 ist zukünftig § 26 Abs. 2 Satz 3 zu beachten, wonach die Übermittlung an die Strafverfolgungs- bzw. Gefahrenabwehrbehörden nur zulässig ist, wenn der mit der Verarbeitung der übermittelten Daten beim Datenempfänger verfolgte Zweck die Neuerhebung durch die empfangende Stelle mit vergleichbaren Mitteln rechtfertigen würde. Im Einzelfall müssen sich Ermittlungsansätze zur Verfolgung dieser Straftaten oder zur Abwehr der Gefahren ergeben. Dabei ist jedoch zu beachten, dass personenbezogene Daten aus einer optischen Wohnraumüberwachung gemäß Artikel 13 Abs. 3 Satz 1 GG nicht zu Zwecken der Strafverfolgung erhoben und folglich auch nicht zu diesen Zwecken übermittelt werden dürfen.

Die gegenüber dem bisherigen § 10 c Abs. 6 LVerfSchG abweichende Verweisung in Bezug auf den Straftatenkatalog folgt einer Änderung der StPO.

Zu Absatz 6 und 7

Die Bestimmungen entsprechen mit redaktionellen Änderungen den bisherigen Regelungen in § 10 c Abs. 7 und 8 LVerfSchG zu verbundenen Akten und besonderen Löschungspflichten.

Zu Absatz 8

Der in der bisher geltenden Regelung (§ 10 c Abs. 9 LVerfSchG) enthaltene Verweis auf den bisherigen § 10 Abs. 5 LVerfSchG zu den Benachrichtigungspflichten wird durch den inhaltlich gleichlautenden Text ersetzt.

Zu Absatz 9

Für die gerichtliche Entscheidung ist zukünftig das Oberverwaltungsgericht Rheinland-Pfalz zuständig. Eine Zuständigkeit des Amtsgerichts ist nicht mehr vorgesehen. Mit der Regelung wird die bereits für die Polizei normierte Zuständigkeit des Oberverwaltungsgerichts Rheinland-Pfalz für die Anordnung der Wohnraumüberwachung (vgl. § 29 Abs. 7 des Polizei- und Ordnungsbehördengesetzes) auch für den Verfassungsschutz übernommen.

Zu § 20 (Erhebung und Verarbeitung von Daten aus digitalen Medien)

Die Bedeutung des Internets hat für die Kommunikation von Extremisten und Terroristen in den vergangenen Jahren stetig zugenommen. Es konnte insbesondere im Bereich des Islamismus festgestellt werden, dass die neuen Medien als Plattform für die Radikalisierung und Rekrutierung von häufig noch jungen Menschen genutzt werden. Insoweit obliegt dem Verfassungsschutz die Aufgabe, extremistische Bestrebungen in digitalen Medien zu beobachten und aufzuklären. Die Regelung bietet hierfür eine entsprechende Rechtsgrundlage.

Zu Absatz 1

Nach der Rechtsprechung des Bundesverfassungsgerichts (Urteil des BVerfG v. 27. Februar 2008, 1 BvR 370/07, 595/05, Rn. 305 ff. – juris), ist eine Kenntnisnahme öffentlich zugänglicher Informationen dem Staat grundsätzlich nicht verwehrt. Demnach liege kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebe, die sich an jedermann oder zumindest an einen nicht weiter abgrenzbaren Personenkreis richte. Ein Eingriff in das Recht auf informationelle Selbstbestimmung könne allerdings dann gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen werden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergebe.

Weiter führt das Gericht in seinem Urteil aus, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung nicht schon dann vorliege, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begebe, wohl aber, wenn sie dabei schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutze, um persönliche Daten zu erhalten, die sie ansonsten nicht erhalten würde. Eine reine Internetaufklärung stelle jedoch in der Regel keinen Grundrechtseingriff dar. Dies gelte selbst dann, wenn bestimmte Personen über einen längeren Zeitraum an der Kommunikation teilnehmen und sich auf diese Weise eine Art „elektronische Gemeinschaft“ gebildet habe. Auch im Rahmen einer solchen Beziehung sei jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kenne oder deren Angaben über sich nicht überprüfen könne.

Soweit eine Internetaufklärung einen Grundrechtseingriff darstellt, zum Beispiel weil allgemein zugängliche Inhalte ge-

zielt zusammengetragen, gespeichert und zusammen mit anderen Daten systematisch ausgewertet werden, ergibt sich die Ermächtigungsgrundlage hierfür bereits aus der allgemeinen Befugnisnorm des § 9. Insoweit ist Absatz 1 rein deklaratorischer Natur. Die Regelung soll vornehmlich in Bezug auf die folgenden Absätze 2 und 3 die verschiedenen Stufen der Eingriffsintensität systematisch darstellen.

Zu Absatz 2

Rechtsgrundlage für Eingriffe nach Absatz 2 bildet ebenfalls § 9. Im Unterschied zu Absatz 1 sind diese jedoch nur zur Aufgabenerfüllung nach § 5 zulässig. Zudem liegt bei Maßnahmen dieser Art, die mit Hilfe einer Legende unter Ausnutzung schutzwürdigen Vertrauens des Betroffenen in die Identität und Motivation des Kommunikationspartners durchgeführt werden, wie oben dargestellt, stets ein Eingriff in Artikel 1 i. V. m. Artikel 2 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung vor. Insoweit besteht eine höhere Schutzbedürftigkeit der Betroffenen als bei Maßnahmen nach Absatz 1, die sich auf eine reine Internetrecherche oder ein bloßes Zusammentragen von Informationen (ohne dass schutzwürdiges Vertrauen tangiert ist) beschränken. Um diesem nicht unerheblichen Eingriff in die Grundrechte der Betroffenen Rechnung zu tragen, bedarf es neben der obligatorischen Beachtung des Verhältnismäßigkeitsgrundsatzes (§ 8 Abs. 1) der Anordnung der Maßnahme durch die Leitung der Verfassungsschutzbehörde. Wann schutzwürdiges Vertrauen im Sinne der Vorschrift tangiert ist, ist im Einzelfall nach Art und Umfang der Kommunikation zu entscheiden. Voraussetzung ist jedoch zumindest, dass ein intensiver und dauerhafter Kommunikationsprozess stattfindet. Schutzwürdiges Vertrauen kann daher z. B. dann betroffen sein, wenn Tarnpersonalien – wie in einem Post-ID-Verfahren – vorgegeben werden oder bei der Legendenbildung der Name eines existierenden Extremisten verwendet wird.

Zu Absatz 3

Nach Absatz 3 ist ein verdeckter Zugriff auf zugangsgesicherte Inhalte und sonstige Informations- und Kommunikationsinhalte in digitalen Medien auf dem hierfür technisch vorgesehenen Weg, ohne selbst Kommunikationsadressat oder von den an der Kommunikation teilnehmenden Personen oder anderen Berechtigten hierzu autorisiert zu sein, nur unter den Voraussetzungen und nach dem Verfahren des Artikel 10-Gesetzes zulässig. Dies entspricht insoweit den Vorgaben des BVerfG, das für einen derartig schwerwiegenden Grundrechtseingriff die Normierung einer qualifizierten materiellen Eingriffsschwelle voraussetzt (Urteil des BVerfG vom 27. Februar 2008, 1 BvR 370/07, 595/05, Rn. 298 – juris). Das Gericht führte in seinem Urteil weiterhin aus, dass kein Eingriff in Artikel 10 GG vorliege, wenn etwa ein Teilnehmer eines Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt habe und die Behörde in der Folge diesen Zugang nutze (Urteil des BVerfG vom 27. Februar 2008, 1 BvR 370/07, 595/05, Rn. 293 – juris).

Zu § 21 (Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums)

Öffentliche Veranstaltungsorte sowie öffentliche Plätze und Infrastruktureinrichtungen werden zunehmend mit öffentlichen Videoüberwachungsanlagen ausgerüstet. Die Wirksamkeit von Videoüberwachungsmaßnahmen zu präventiven und repressiven Zwecken wird dabei unterschiedlich beurteilt. Gleichwohl ist in Zeiten einer abstrakt hohen Gefährdungslage durch terroristische Anschläge eine Zunahme von Videoüberwachung an öffentlichen Orten und auf Veranstaltungen mit großem potenziellen Schadensrisiko, wie z. B. bei Volksfesten, Umzügen und Sport- oder Musikveranstaltungen aber auch Infrastruktureinrichtungen wie Bahnhöfen und Flughäfen zu verzeichnen. Dabei ist stets das Recht auf informationelle Selbstbestimmung der Besucherinnen und Besucher, Teilnehmerinnen und Teilnehmer oder Kundinnen und Kunden gegen das Sicherheitsbedürfnis vor terroristischen Gefahren und des Schutzes von Leib und Leben abzuwägen. Die islamistischen Terroranschläge der Vergangenheit haben gezeigt, dass die Täter gezielt den öffentlichen Raum für ihre Anschlagsziele auswählen, um möglichst großen Schaden anzurichten. Dabei werden sog. weiche Ziele, d. h. große Menschenansammlungen plötzlich und aus dem nichts heraus mit einfachen Tatmitteln, aber auch mit Kriegswaffen angegriffen. Die Wehrlosigkeit und Panik wird ausgenutzt, um möglichst viele Menschenleben zu beenden.

Die Auswertung der Videoüberwachung kann neben Zwecken der Strafverfolgung und Gefahrenabwehr nicht zuletzt auch dem positiven Sicherheitsempfinden der Bürgerinnen und Bürger dienen. Den Verfassungsschutzbehörden können Video- und Tonaufnahmen darüber hinaus Aufschluss über komplexe Zusammenhänge terroristischer Tatbegehungen und weitere für die nachrichtendienstliche Analyse tragende Erkenntnisse geben. Mit der Anknüpfung an die Aufgabenerfüllung nach § 5 bei der Verarbeitung personenbezogener Daten aus Videoüberwachungen wird die Nutzung zu einem anderen gesetzlich geregelten Zweck im Sinne des § 21 Abs. 3 LDSG geregelt.

Zu Absatz 1

Zur Aufgabenerfüllung nach § 5 darf die Verfassungsschutzbehörde auf verfügbare Einrichtungen zur Videobeobachtung von öffentlich zugänglichen Räumen zugreifen. Öffentlich zugängliche Räume sind örtliche Bereiche, die von jedermann betreten werden können oder bei denen die Zugänglichkeit anhand von allgemeinen Merkmalen bestimmt wird, die von jedermann erfüllt werden können. Beispielhaft sind Konzerte aber auch Bahnhöfe oder Flughäfen zu nennen. Auf eine häusliche Bedachung kommt es nicht an.

Die Mehrzahl der Videoüberwachungen im öffentlichen Raum findet durch ständig oder temporär verfügbare Einrichtungen zur Videobeobachtung in Form des Monitoring statt, das heißt es werden keine Aufzeichnungen gefertigt, sondern die Überwachung erfolgt „live“ durch laufende Beobachtung des Videobildes. Absatz 1 Satz 1 ermöglicht es der Verfassungsschutzbehörde, bei dem Monitoring zugegen zu sein. Ein Erfordernis hierfür kann sich im Rahmen einer besonderen Sicherheitslage ergeben oder aber bei Örtlichkeiten im öffentlich zugänglichen Raum, die sich im Rahmen von Observationen durch eigene Kräfte unbemerkt oder über einen längeren Zeitraum nur schwer überwachen lassen.

Mit Satz 2 werden die Betreiber von Einrichtungen zur Videobeobachtung verpflichtet, den Zutritt zu den entsprechenden Räumlichkeiten zu gewähren und die Mitbenutzung der Videobeobachtungsanlage zu dulden. Insoweit besteht eine Mitwirkungsverpflichtung der Betreiber bzw. der über die entsprechenden Räumlichkeiten verfügungsberechtigten Personen.

Zu Absatz 2

Zur Aufgabenerfüllung nach § 5 darf die Verfassungsschutzbehörde auf gespeicherte Bild- und Tonaufzeichnungen von Videoüberwachungen öffentlich zugänglicher Räume zugreifen (Satz 1). Das Videografieren mit eigenen Mitteln ist nicht von der Regelung umfasst. Für den Zugriff müssen tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 genannten Schutzgüter vorliegen. Der Begriff der schwerwiegenden Gefahr verweist auf eine erhöhte Intensität der Rechtsgutsbedrohung. Durch das Erfordernis tatsächlicher Anhaltspunkte für eine schwerwiegende Gefahr wird zudem die tatsächliche Grundlage des Eingriffs qualifiziert. Es reicht nicht aus, dass die geregelte Datenerhebung allgemein für die Aufgabenerfüllung der Verfassungsschutzbehörde nützlich ist. Vielmehr müssen Anhaltspunkte für einen Zustand bestehen, in dem die Schutzgüter in § 5 konkret bedroht sind.

Gemäß Satz 2 haben die Betreiber die relevanten Daten auf Verlangen unverzüglich und unentgeltlich zur Verfügung zu stellen. Es besteht insoweit eine Mitwirkungsverpflichtung. Dabei hat die Verfassungsschutzbehörde, soweit möglich, die angeforderten Bild- und Tonaufzeichnungen nach Datum, Ort und Zeit einzugrenzen und dem Betreiber mitzuteilen (Satz 3).

Zu Absatz 3

Die Bestimmung sieht eine unverzügliche Rückgabe-, Löschungs- oder Vernichtungsverpflichtung der Verfassungsschutzbehörde vor, wenn überlassene Bild- und Tonaufzeichnungen nicht mehr zur Aufgabenerfüllung erforderlich sind und die Voraussetzungen in Absatz 1 nicht mehr vorliegen. Damit wird die Datenverarbeitung auf das erforderliche Maß beschränkt.

Zu § 22 (Amtshilfe bei Tarnmaßnahmen)

Die Bestimmung entspricht der bisherigen Regelung in § 10 Abs. 3 LVerfSchG. Tarnmaßnahmen beinhalten unabdingbare Hilfsmittel wie Tarnpapiere und -kennzeichen, die erst den Einsatz anderer nachrichtendienstlicher Mittel ermöglichen, aber nicht primär der Informationsbeschaffung dienen. Es handelt sich insbesondere um Führer- und Fahrzeugscheine, Personalausweise, Reisepässe und vergleichbare Urkunden mit Tarnangaben zur Person. Soweit die Verfassungsschutzbehörde diese Hilfsmittel nicht selbst herstellt, wird mit der Bestimmung geregelt, dass zuständige andere öffentliche Stellen Hilfe zu leisten haben. Da ein zeitlicher Verzug den Aufgaben des Verfassungsschutzes hinderlich sein kann, hat diese Hilfe unverzüglich, d. h. ohne schuldhafte Verzögerung zu erfolgen.

Bezüglich der Erstattung der Kosten der Amtshilfe gilt § 1 Abs. 1 des Landesverwaltungsverfahrensgesetzes vom 23. Dezember 1976 (GVBl. S. 308), zuletzt geändert durch § 48 des Gesetzes vom 22. Dezember 2015 (GVBl. S. 487), BS 2010-3, in Verbindung mit § 8 des Verwaltungsverfahrensgesetzes in der Fassung vom 23. Januar 2003 (BGBl. I S. 102) in der jeweils geltenden Fassung.

Zu § 23 (Verarbeitung personenbezogener Daten)

Mit der Überschrift zu Teil 4 „Datenverarbeitung“ wird in Anlehnung an die Begrifflichkeiten im neuen Landesdatenschutzgesetz in erster Linie auf die Erhebung, Speicherung, Übermittlung und Nutzung personenbezogener Daten abgestellt. Die Begriffsbestimmung findet sich in § 27 Nr. 2 LDSG, welcher gemäß § 39 Satz 2 für entsprechend anwendbar erklärt wird.

Zu Absatz 1

Absatz 1 Satz 1 Nr. 1 regelt die Verarbeitung personenbezogener Daten bei Ausübung der Hauptaufgabe der Verfassungsschutzbehörde, nämlich der Beobachtung von Bestrebungen oder Tätigkeiten nach § 5. Voraussetzung ist das Vorliegen tatsächlicher Anhaltspunkte für einen Verdacht in diese Richtung. Satz 1 Nummer 2 regelt die Verarbeitung personenbezogener Daten insbesondere im Zusammenhang mit Maßnahmen der Nachrichtenbeschaffung inklusive der Einschätzung von Gefahren, die für Einzelne von den beobachteten Bestrebungen oder Tätigkeiten ausgehen und knüpft die Befugnis zur Verarbeitung insoweit an den allgemeinen Erforderlichkeitsgrundsatz an.

Nummer 3 regelt die Verarbeitung personenbezogener Daten bei der Durchführung von und Mitwirkung bei Sicherheitsüberprüfungen sowie den Überprüfungen nach § 6 Abs. 2 (Erkenntnisabfragen).

Nach Absatz 1 Satz 1 Nr. 4 dürfen Daten auch zur Gewinnung, Erhaltung oder Überprüfung nachrichtendienstlicher Zugänge zu Bestrebungen oder Tätigkeiten nach § 5 verarbeitet werden. Dieses ist wieder an den Erforderlichkeitsgrundsatz geknüpft.

Gemäß Absatz 1 Satz 1 Nr. 5 dürfen Daten verarbeitet werden, um entweder Mitarbeiterinnen und Mitarbeiter, Vertrauenspersonen oder die Verfassungsschutzbehörde als Einrichtung sowie Gegenstände und Nachrichtenzugänge vor Enttarnung, Spionage oder Gewalt durch Dritte zu schützen. Die Abschirmung des Personals, der Arbeitsweise sowie der behördlichen Einrichtungen kennzeichnet den Verfassungsschutz als Nachrichtendienst.

Gemäß Absatz 1 Satz 1 Nr. 6 können Daten auch mit Einwilligung der oder des Betroffenen verarbeitet werden. Damit wird ein allgemeiner Grundsatz des Datenschutzrechts in das Gesetz aufgenommen. Die Regelung korrespondiert insoweit mit § 6 Abs. 2. Relevant werden die Bestimmungen insbesondere bei Überprüfungen (Erkenntnisabfragen) im Rahmen eines Akkreditierungsverfahrens, z. B. hinsichtlich des Personals, welches bei Großveranstaltungen zum Einsatz kommen soll.

Absatz 1 Satz 2 regelt die Belegbarkeit von in Auswertungsdateien (z. B. NADIS) gespeicherten personenbezogenen Daten. Diese müssen zusätzlich in Akten oder auf anderen Datenträgern vorgehalten werden.

Absatz 1 Satz 3 regelt, dass personenbezogene Daten, die für Zwecke der Erfüllung der Aufgaben nach § 5 erhoben wurden, auch für Zwecke der Sicherheitsüberprüfungen nach § 6 verwendet werden dürfen.

Absatz 1 Satz 4 stellt im Übrigen klar, dass die Verarbeitung von personenbezogenen Daten derselben Aufgabe und dem Schutz derselben Rechtsgüter dienen muss, welche Gründe der Erhebung waren (Grundsatz der Zweckbindung).

Die Verarbeitung von personenbezogenen Daten aus der besonders eingriffsintensiven Maßnahme der Wohnraumüberwachung (§ 18) ist nur bei Tatsachen für eine im Einzelfall bestehende dringende Gefahr für die öffentliche Sicherheit, ins-

besondere einer gemeinen Gefahr oder einer Lebensgefahr oder eine Gefahrenlage im Sinne des § 18 Abs. 1 Satz 2 zulässig (Absatz 1 Satz 5). Damit wird den besonderen Anforderungen des BVerfG im Urteil zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 283) an die Zweckbindung für Daten Rechnung getragen. Aufgrund des besonderen Eingriffsgewichts der Datenerhebungen bei der Wohnraumüberwachung gilt hier eine besonders enge Bindung jeder weiteren Nutzung der bei diesen Maßnahmen gewonnenen Daten an die Voraussetzungen und Zwecke ihrer Datenerhebung.

Zu Absatz 2

Absatz 2 entspricht im Wesentlichen mit redaktionellen Änderungen dem bisherigen § 11 Abs. 2 LVerfSchG. Absatz 2 Satz 2 verweist auf Absatz 1 Satz 4 und 5, sodass klarstellend der Grundsatz der Zweckbindung sowie auch die besonders enge Bindung jeder weiteren Nutzung der bei der Wohnraumüberwachung gewonnenen Daten an die Voraussetzungen und Zwecke ihrer Datenerhebung gelten. Der Begriff „sperren“ ist durch „einschränken“ ersetzt worden und entspricht somit der harmonisierten Begriffsbestimmung im Datenschutzrecht.

Zu Absatz 3

Die Regelung entspricht der bisherigen Bestimmung in § 11 Abs. 3 LVerfSchG.

Zu Absatz 4

Die Bestimmung dient der Umsetzung der Vorgaben des BVerfG in dem Urteil zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 283). Zwar ist die Rechtsprechung zum BKA-Gesetz, mithin einem Polizeigesetz ergangen, gleichwohl können grundsätzliche Aussagen für die Datenverarbeitung durch die Sicherheitsbehörden von Polizei und Verfassungsschutz abgeleitet werden. So hat das BVerfG in der Entscheidung seine Rechtsprechung zu den Grundsätzen der Zweckbindung und Zweckänderung fortentwickelt. Die Verhältnismäßigkeitsanforderungen für jede zweckändernde Datenverwendung müssen sich am Grundsatz der hypothetischen Datenneuerhebung orientieren. Danach gilt, dass eine neue Nutzung der erhobenen Daten dem Schutz von Rechtsgütern eines solchen Gewichts dienen muss, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen können (BVerfG, Urteil vom 20. April 2016, a. a. O, Rn. 288). Der Verweis in Absatz 4 Satz 2 auf Absatz 1 Satz 5 macht dabei wiederrum die besonderen Anforderungen an die zweckändernde Nutzung von Daten aus Maßnahmen der Wohnraumüberwachung zur Bedingung. Ihre Zweckänderung ist danach nur bei dem Vorliegen von Tatsachen für im Einzelfall bestehende dringende Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr oder eine Gefahrenlage im Sinne des § 18 Abs. 1 Satz 2, zulässig.

Mit Blick auf den besonderen Aufgabenzuschnitt der Verfassungsschutzbehörden ist bei der Anwendung von Absatz 4 allerdings zu berücksichtigen, dass es sich bei der wiederholenden Verarbeitung von Daten im Zusammenhang mit den Beobachtungsaufgaben nach § 5 nicht um Zweckänderungen handelt. Hierzu erfolgt nach § 5 gerade eine gezielte und planmäßige Sammlung und Auswertung sach- und personenbezogener Daten. Beides ist grundsätzlich nicht an konkrete verfahrensbezogene Ermittlungen geknüpft, sondern dient u. a. der laufenden Fortschreibung von Lagebildern bezogen auf Bestrebungen und Tätigkeiten nach § 5. Dies gilt sowohl für die sich wiederholende Verarbeitung der Daten innerhalb der Verfassungsschutzbehörde als auch beispielsweise bei entsprechenden Datenübermittlungen innerhalb des Verfassungsschutzverbundes, zu denen die Verfassungsschutzbehörden im Wege der Zusammenarbeit nach § 6 BVerfSchG durch Bundesrecht verpflichtet sind.

Zu Absatz 5

Die Bestimmung entspricht mit redaktionellen Änderungen der bisherigen Regelung in § 11 Absatz 5 LVerfSchG.

Zu § 24 (Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten)

Zu Absatz 1 bis 3

Die Absätze 1 bis 3 entsprechen mit redaktionellen Änderungen der bisherigen Rechtslage in § 12 Abs.1 bis 3 LVerfSchG. In Anlehnung an die Begrifflichkeiten im neuen Landesdatenschutzgesetz wird für das Sperren personenbezogener Daten der Begriff „Einschränkung der Verarbeitung“ verwendet. Mit dem Verweis in Absatz 2 Satz 4 auf Absatz 5 Satz 1 wird klargestellt, dass für personenbezogene Daten in Akten, die der Anbietungspflicht nach § 7 des Landesarchivgesetzes (LArchG) vom 5. Oktober 1990 (GVBl. S. 277), zuletzt geändert durch Gesetz vom 27. November 2015 (GVBl. S. 383), BS 224-10, unterliegen, die Verarbeitung bis zur Anbietung einzuschränken ist (vgl. Absatz 2 Satz 6).

Zu Absatz 4

Im Rahmen der Datenverarbeitung bedürfen Minderjährige eines besonderen Schutzes, der vor allem die Adoleszenzphase berücksichtigt. Hierzu gehört die Bewältigung alterstypischer Entwicklungsaufgaben, wie familiäre Ablösung, soziale Neuorientierung und die Entwicklung einer eigenen (auch politischen) Identität. Die Gefahr von Etikettierungen durch die Vorhaltung von Daten ist aus diesem Grund zu vermeiden. In der Vergangenheit wurden jedoch zunehmend Fälle bekannt, in denen sich bereits unter 14-jährige Personen innerhalb kürzester Zeit radikalisierten. Bei der Aufdeckung und Verhinderung terroristischer Anschläge kommt der Tätigkeit des Verfassungsschutzes eine zentrale Bedeutung zu. Im Unterschied zur Strafmündigkeit spielt die Einsichtsfähigkeit für die Frage der Gefahrenabwehr keine Rolle, sodass starre Altersgrenzen dem Auftrag des Verfassungsschutzes als Frühwarnsystem der Demokratie nicht gerecht werden. Um beiden Aspekten Rechnung zu tragen sieht Satz 1 vor, dass Daten von unter 14-jährigen Personen, welche in Dateien oder in zu ihrer Person geführten Akten gespeichert sind, grundsätzlich nach zwei Jahren zu löschen sind, es sei denn, dass weitere Erkenntnisse nach § 5 angefallen sind. Hiermit wird deutlich, dass in der Regel nicht davon ausgegangen wird, dass sich das verfassungsschutzrelevante Verhalten in allen Fällen zu einer dauerhaften verfassungsfeindlichen Einstellung im Sinne des § 5 verfestigt.

Zwischen dem 14. und 18. Lebensjahr sind nach Satz 2 die zu den Minderjährigen gespeicherten Daten 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 nach § 5 angefal-

len sind. Auch in diesem Lebensaltersabschnitt wird dem Minderjährigenschutz durch enge Überprüfungs- und Löschfristen Rechnung getragen.

Nach Satz 3 dürfen personenbezogene Daten über das Verhalten von Minderjährigen vor Vollendung des 16. Lebensjahres nach den Bestimmungen dieses Gesetzes nicht an ausländische oder über- oder zwischenstaatliche Stellen übermittelt werden. Wegen der international unterschiedlichen Altersgrenzen und der schwierigeren Eindämmung von Übermittlungsfolgen im internationalen Informationsaustausch ist es ausnahmslos untersagt, personenbezogene Daten über noch nicht 16-jährige Personen an außerdeutsche Stellen zu übermitteln. § 26 Abs. 5 ist insoweit nicht anwendbar.

Zu Absatz 5

Akten, auch solche die nach gesetzlichen oder sonstigen Vorschriften geheim zu halten sind, sind in der Regel spätestens dreißig Jahre nach ihrer Entstehung gemäß § 7 Abs. 1 und 2 LArchG der Landesarchivverwaltung zwecks öffentlicher Nutzung anzubieten. Gemäß § 3 Abs. 3 Satz 4 LArchG dürfen Unterlagen, die aufgrund von Rechtsvorschriften geheim zu halten sind, 60 Jahre nach ihrer Entstehung genutzt werden. Damit sind auch ursprünglich geheim zu haltende Aktenbestände grundsätzlich der Öffentlichkeit zugänglich. Die Sperrfrist kann gemäß § 3 Abs. 3 Satz 5 LArchG um höchstens 20 Jahre verlängert werden, wenn dies unter Anlegung strengster Maßstäbe im öffentlichen Interesse geboten ist. Eine solche starre Beschränkung der Verlängerung der Sperrfrist verbietet sich aber, wenn dies im öffentlichen Interesse geboten ist. So kann es beispielhaft geboten sein, bestimmte Daten weitere 21 Jahre der öffentlichen Nutzung vorzuenthalten bzw. weiterhin geheim zu halten. Die Regelung in Absatz 5 sieht daher eine besondere und restriktiv anzuwendende Erklärungsbefugnis der für den Verfassungsschutz zuständigen Ministerin oder des für den Verfassungsschutz zuständigen Ministers vor, dass das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten würde. Die Entscheidung zur Aufhebung der Beschränkung der Sperrfrist ergeht im Einvernehmen mit der für das Archivwesen zuständigen Ministerin oder dem für das Archivwesen zuständigen Minister.

Zu § 25 (Informationsübermittlung an die Verfassungsschutzbehörde)

Zu Absatz 1

Absatz 1 sieht vor, dass die öffentlichen Stellen des Landes und der kommunalen Gebietskörperschaften an die Verfassungsschutzbehörde von sich aus, d. h. ohne Ersuchen derselben Informationen übermitteln, soweit nach ihrer Beurteilung tatsächliche Anhaltspunkte dafür bestehen, dass die Informationen für die Erfüllung der Aufgaben nach § 5 erforderlich sind. Die Unterscheidung in der bisherigen Regelung des § 13 Abs. 1 LVerfSchG, wonach eine Übermittlungspflicht der Behörden und Einrichtungen nur bei Bestrebungen und Tätigkeiten gemäß § 5 Satz 1 Nummer 1 und 4 LVerfSchG mit Gewaltbezug sowie § 5 Satz 1 Nr. 2 und 3 LVerfSchG besteht, die Übermittlung im Übrigen bei Bestrebungen und Tätigkeiten gemäß § 5 Satz 1 Nr. 1 und 4 LVerfSchG ohne Gewaltbezug aber im jeweiligen Ermessen der Behörden oder Einrichtungen steht, wird aufgegeben.

Die Beobachtung extremistischer Bestrebungen mit oder ohne Gewaltbezug steht im besonderen öffentlichen Interesse. Die Verwaltungen des Landes und der kommunalen Gebietskörperschaften sind daher verpflichtet, bei entsprechenden Anhaltspunkten die diesbezüglichen Informationen zu übermitteln. Die fachliche Einschätzung der etwaigen Anwendung von Gewalt oder darauf bezogener Vorbereitungen durch Bestrebungen gemäß § 5 Satz 1 Nr. 1 und 4 LVerfSchG ist durch die Verfassungsschutzbehörde zu beurteilen; sie ist für die Pflicht zur Informationsübermittlung durch die anderen öffentlichen Stellen des Landes und der kommunalen Gebietskörperschaften ohne Belang.

Zu Absatz 2

Die Bestimmung entspricht im Wesentlichen der bisherigen Regelung in § 13 Abs. 2 LVerfSchG. Es wird ergänzend eingefügt, dass die ersuchten Behörden und Einrichtungen in Angelegenheiten des Verfassungsschutzes unverzüglich und unentgeltlich zur Übermittlung der ersuchten Informationen verpflichtet sind (Satz 4).

Zu Absatz 3 und 4

Die Bestimmungen entsprechen mit redaktionellen Änderungen der bisherigen Regelung in § 13 Abs. 3 und 4 LVerfSchG.

Zu Absatz 5

Die Verfassungsschutzbehörde darf automatisierte Abrufverfahren anstatt eines Verlangens nach Absatz 2 und § 18 Abs. 3 Satz 2 BVerfSchG nutzen, wenn dies ausdrücklich gesetzlich geregelt ist. Die Einrichtung eines automatisierten Abrufverfahrens ist durch die Leitung der Verfassungsschutzbehörde anzuordnen. Gründe für einen Abruf sind nach Maßgabe der den Abruf zulassenden Rechtsvorschriften zu dokumentieren.

Zu Absatz 6

Der Verfassungsschutz erhält eine Rechtsgrundlage für die Ausschreibung von Zielpersonen sowie die von ihr benutzen oder eingesetzten Kraftfahrzeuge in dem polizeilichen Informationssystem (POLIS). Die Ausschreibung muss zur Aufgabenerfüllung nach § 5 erforderlich sein. Die Mitteilung über das Antreffen einer Person oder das Feststellen eines Kraftfahrzeuges dient dem zusätzlichen Erkenntnisgewinn des Verfassungsschutzes über mögliche Reise- und Bewegungsmuster sowie sonstige Umstände des polizeilichen Antreffens verfassungsschutzrelevanter Personen. Beispielhaft findet im Bereich des Rechtsextremismus eine starke Mobilisierung im Zusammenhang mit rechtsradikalen Rockkonzerten statt, bei deren Anfahrt das relevante Personenpotenzial durch die Polizei kontrolliert wird. Unter Beachtung des organisatorischen und befugnisrechtlichen Trennungsgebots wird durch die Ausschreibung keine polizeiliche Aufgabenwahrnehmung veranlasst (Satz 2). Polizeiliche Maßnahmen dürfen aufgrund der Tatsache der Ausschreibung nicht erfolgen. Die Kontrollmitteilung setzt vielmehr eine für polizeiliche Aufgaben durchgeführte Kontrolle voraus und stellt aus polizeilicher Sicht einen reinen Zufallstreffer dar. Somit wird dem nachrichtendienstlichen Erkenntnisbedarf lediglich bei Gelegenheit polizeilicher Aufgabenwahrnehmung Rechnung getragen, ohne dass polizeiliche Befugnisse für nachrichtendienstliche Aufgaben ausgeübt werden.

Zu Absatz 7

Absatz 7 stellt klar, dass Übermittlungsvorschriften nach anderen Gesetzen unberührt bleiben. Soweit Informationen von Bundesbehörden, bundesunmittelbaren juristischen Personen des öffentlichen Rechts, Staatsanwaltschaften und Polizeien des Bundes und anderer Länder betroffen sind, ist § 18 BVerfSchG maßgebend.

Zu § 26 (Informationsübermittlung durch die Verfassungsschutzbehörde)

Unter den Bedingungen informationeller Trennung sind Übermittlungsvorschriften das Bindeglied zwischen informationellen und aktionellen staatlichen Eingriffen. Datenübermittlungen des Verfassungsschutzes an die zu staatlichen Zwangsmaßnahmen befugten Polizeibehörden waren Gegenstand der Rechtsprechung des BVerfG zur Antiterrordatei (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07) sowie auch zum BKA-Gesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09). Dabei wurde der Grundsatz der informationellen Trennung (vgl. dazu BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 123) und der Grundsatz der hypothetischen Datenneuerhebung durch das BVerfG entwickelt und für den Datenaustausch der Sicherheitsbehörden zur verfassungsrechtlichen Bedingung gemacht.

Das BVerfG hat die Erhebung personenbezogener Daten durch Polizeibehörden und Nachrichtendienste im Rahmen ihrer unterschiedlichen Aufgabenwahrnehmung und Zweckrichtung hervorgehoben und den zwischenbehördlichen Datenaustausch für ein mögliches operatives Tätigwerden grundsätzlich von einem herausragenden öffentlichen Interesse abhängig gemacht. In der Praxis dürfen nachrichtendienstliche Erhebungen personenbezogener Daten mit niedrigschwelligeren Eingriffsbefugnissen nicht durch Übermittlungsvorschriften in polizeilichen Zwangsmaßnahmen münden, wenn die Polizei nicht ihrerseits durch eigene Befugnisse dazu ermächtigt und in der Lage ist, diese Daten ebenso (hypothetisch) zu erheben. Es darf durch die Übermittlung zu keiner Umgehung höherer Eingriffsschwellen im Rahmen polizeilicher Befugnisse kommen.

Zu Absatz 1

Absatz 1 gestattet die Übermittlung personenbezogener Daten an solche öffentlichen Stellen, die für die Sicherung der Schutzgüter zuständig sind, deren Bewahrung auch der Verfassungsschutzbehörde obliegt. Diese erfüllt dadurch ihre Aufgabe, den zuständigen Stellen zu ermöglichen, rechtzeitig die erforderlichen Maßnahmen zu treffen. Für Aufgaben im Sinne von § 6 kommen als Empfänger insbesondere solche Stellen in Betracht, die eine Sicherheitsüberprüfung durchzuführen haben. Ebenso ist die Übermittlung im Rahmen der sonstigen gesetzlich oder mit Einwilligung vorgesehenen Überprüfungen zulässig (§ 6 Abs. 2).

Absatz 1 entspricht bis auf den letzten Halbsatz im Wesentlichen dem bisherigen § 14 Abs. 1 LVerfSchG. Die Ergänzung ist dem Umstand geschuldet, dass der Datenempfänger nach anderen Rechtsvorschriften gegebenenfalls befugt sein kann, die übermittelten personenbezogenen Daten für andere Zwecke, als für die sie übermittelt wurden, zu verwenden (vgl. Artikel 6 Abs. 4 EU-Datenschutzgrundverordnung; § 7 Abs. 1 LDSG). Dies soll allerdings dann nicht gelten, wenn die Verfassungsschutzbehörde im Zuge der Übermittlung ausdrücklich auf eine bestimmte Verarbeitungsbeschränkung hinweist, was beispielsweise aus Gründen des Quellen- oder Methodenschutzes geboten sein kann.

Zu Absatz 2

Absatz 2 regelt die Übermittlung personenbezogener Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden.

Nummer 1 lässt eine Übermittlung personenbezogener Daten an die Stationierungskräfte zu und verweist auf bestehende völkerrechtliche Verpflichtungen. Rechtsgrundlage für die Übermittlung ist Artikel 3 des Zusatzabkommens vom 3. August 1959 in der durch die Abkommen vom 21. Oktober 1971, 18. Mai 1981 und 18. März 1993 geänderten Fassung zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen (im Folgenden als „Zusatzabkommen“ bezeichnet). Die dort zuletzt vereinbarte Ergänzung von Artikel 3 Abs. 3 des Zusatzabkommens stellt eine wesentliche Weiterentwicklung hinsichtlich des wirksamen Schutzes des Rechts auf informationelle Selbstbestimmung dar; Buchstabe a Satz 2 enthält das Gebot der Zweckbindung bei Übermittlung personenbezogener Daten, sodass nicht stärker in das Persönlichkeitsrecht des oder der Betroffenen eingegriffen wird, als der Vertragszweck dies erfordert. Eine eigene „Ordre-public“ Klausel in Buchstabe b befreit die Vertragspartner von der allgemeinen Unterstützungsplicht, wenn durch die Unterstützungsmaßnahme gegen nationales Recht verstoßen würde. Im Übrigen verweist Artikel 3 Abs. 1 des Zusatzabkommens auf die Verpflichtung der Vertragsparteien zur gegenseitigen Unterstützung und zur Zusammenarbeit und erläutert in Absatz 2 Buchstabe a diese Zusammenarbeit, die sich u. a. auf die Förderung und Wahrnehmung der Sicherheit der Bundesrepublik, der Entsendestaaten und der Truppen bezieht und sich namentlich auf die Sammlung, den Austausch und den Schutz aller Nachrichten, die für diesen Zweck von Bedeutung sind, erstreckt.

Nummer 2 und 3 regelt die Übermittlung personenbezogener Daten an die Strafverfolgungs- und Polizeibehörden, welche mit nachrichtendienstlichen Mitteln erhoben wurden. Diese Behörden haben vergleichbare Erhebungsbefugnisse wie die Verfassungsschutzbehörde und mittelbar oder unmittelbar Exekutiv-/ bzw. Zwangsbefugnisse, sodass bei der Zweckänderung durch eine Datenübermittlung die Grundsätze der informationellen Trennung sowie der hypothetischen Datenneuerhebung Beachtung finden müssen. Werden personenbezogene Daten mit nachrichtendienstlichen Mitteln erhoben, so dürfen die Erhebungsvorschriften der Strafverfolgungs- und polizeilichen Gefahrenabwehrbehörden nicht durch Übermittlungsvorschriften unterlaufen werden. Die Übermittlung muss einem überragenden öffentlichen Interesse dienen. Die Aufklärung der Straftaten in Nummer 2, mithin Katalogstraftaten nach § 100 a StPO und § 131 StGB, Straftaten der organisierte Kriminalität, Staatsschutzdelikte nach §§ 74 a und 120 des Gerichtsverfassungsgesetzes (GVG), sonstige Straftaten mit verfassungsfeindlichen Zielen, Motiven oder durch verfassungsfeindliche Organisationen aber auch die effektive Abwehr von erheblichen Gefahren (i. e. gefährdete hochrangige Rechtsgüter z. B. Leben, Gesundheit, Bestand des Staates oder eine Vielzahl von betroffenen Opfern) sowie die vorbeugende Bekämpfung der Straftaten in § 28 Abs. 3 POG stehen grundsätzlich in einem überragenden öffentlichen

Interesse. Die Übermittlung ist jedoch im Einzelfall nur zulässig, wenn der mit der Verarbeitung der übermittelten Daten verfolgte Zweck eine Neuerhebung durch die empfangende Stelle mit vergleichbaren Mitteln rechtfertigen würde (Satz 3). Es sind folglich die rechtlichen Voraussetzungen zu prüfen, ob die empfangende Stelle die übermittelten Daten im Rahmen ihrer Aufgaben der Gefahrenabwehr oder Strafverfolgung selber hätte (verdeckt) erheben können.

Nummer 4 regelt die Übermittlung an andere öffentliche Stellen, wozu insbesondere auch Ordnungsbehörden zählen können, wenn die empfangende Stelle die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für erhebliche Zwecke der öffentlichen Sicherheit (z. B. gewaltbereite Reichsbürger bzw. Selbstverwalter) benötigt. Eine vergleichbare Regelung findet sich in § 19 Abs. 1 Satz 3 BVerfSchG.

Zu Absatz 3

Absatz 3 erlaubt die Übermittlung personenbezogener Daten, welche nicht mit nachrichtendienstlichen Mitteln erhoben wurden, soweit die Daten für die Aufgabenerfüllung der empfangenden Stelle erforderlich sind. Die Gefahr, dass personenbezogene Daten, die mit niedrigen Eingriffsschwellen erhoben wurden, in staatlichen Zwangsmaßnahmen münden, besteht hier nicht. In das Gesetz neu aufgenommen wird eine Datenübermittlungsvorschrift zum Schutz von Mitarbeiterinnen und Mitarbeitern öffentlicher Stellen, unabhängig davon, ob die personenbezogenen Daten mit nachrichtendienstlichen Mittel erhoben wurden (Absatz 2 Satz 2) oder nicht (Absatz 3 Alternative 2). Mit dieser Neuregelung sollen geeignete Schutzmaßnahmen für Mitarbeiterinnen und Mitarbeiter im öffentlichen Dienst vor Gefahren für Leib oder Leben ermöglicht werden, wenn dem Verfassungsschutz entsprechende Erkenntnisse, z. B. über extremistische und gewaltbereite Waffenbesitzer (z. B. Reichsbürger bzw. Selbstverwalter) vorliegen. Die Übermittlung solcher Daten dient dem Schutz von Mitarbeiterinnen und Mitarbeitern öffentlicher Stellen, z. B. den Finanzverwaltungen, der Justiz oder den Polizei- und Ordnungsbehörden bei der eigenen Aufgabenwahrnehmung gegenüber einem solchen Personenspektrum.

Zu Absatz 4

Absatz 4 verweist auf die Mitwirkungsaufgabe in § 6 Abs. 2 und erlaubt es der Verfassungsschutzbehörde in diesem Zusammenhang, Auskunft einschließlich personenbezogener Daten aus vorhandenen Datenbeständen über gerichtsverwertbare Tatsachen zu geben.

Zu Absatz 5

Die Bestimmung entspricht der bisherigen Regelung in § 14 Abs. 5 LVerfSchG.

Zu Absatz 6

Die Bestimmung entspricht im Wesentlichen der bisherigen Regelung in § 14 Abs. 6 LVerfSchG. In Anlehnung an den Wortlaut gemäß § 19 Abs. 4 Satz 1 BVerfSchG dürfen jedoch nunmehr personenbezogene Daten an nichtöffentliche Stellen übermittelt werden, wenn dies zu einem der in Nummer 1 bis 4 genannten Gründe erforderlich ist. Das in der bisherigen Regelung normierte Übermittlungsverbot mit Ausnahmevorbehalt wird insoweit aufgehoben und durch eine verhältnismäßige Übermittlungsbefugnis ersetzt.

Zu Absatz 7

Die Bestimmung entspricht der bisherigen Regelung in § 7 Abs. 3 LVerfSchG.

Zu Absatz 8

Absatz 8 stellt klar, dass Informationsübermittlungen durch die Verfassungsschutzbehörde nach anderen Gesetzen, z. B. § 21 BVerfSchG, unberührt bleibt.

Zu § 27 (Übermittlungsverbote)

Die Bestimmung entspricht mit redaktionellen Änderungen der bisherigen Regelung in § 15 LVerfSchG. In Nummer 1 wird lediglich ergänzend klargestellt, dass für die übermittelnde Stelle erkennbar sein muss, dass die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen. Insofern wird der Wortlaut des § 23 Nummer 1 BVerfSchG übernommen. Bezüglich Nummer 2 wird die Regelung durch die Dienstanweisung zum Übermittlungsverbot entsprechend § 15 Nr. 2 Landesverfassungsschutzgesetz vom 13. März 2013 ergänzt. Nach Nummer 2 der Dienstanweisung ist ein Übermittlungsverbot regelmäßig dann nachrangig, wenn aus Sicht des Verfassungsschutzes im Einzelfall tatsächliche Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit bestehen, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt oder tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand als Täter oder Teilnehmer eine in § 100 c Abs. 2 StPO bezeichnete besonders schwere Straftat (jetzt nunmehr § 100 b Abs. 2 StPO) begangen hat oder sonstige erhebliche öffentliche Belange, z. B. im Rahmen der gesetzlichen Beteiligung des Verfassungsschutzes an Überprüfungen im Einbürgerungs- und anderen Verfahren, nicht gewahrt werden können. Insoweit wird die in Nummer 2 zu treffende Abwägungsentscheidung durch die Dienstanweisung konkretisiert.

Zu § 28 (Besondere Pflichten bei der Übermittlung personenbezogener Daten)

Die Bestimmung entspricht mit redaktionellen Änderungen der bisherigen Regelung in § 16 LVerfSchG.

Zu § 29 (Auskunft an Betroffene)

Die Bestimmung entspricht der bisherigen Regelung in § 18 LVerfSchG.

Zu § 30 (Datenschutzkontrolle)

Zu Absatz 1

Mit Absatz 1 wird die Befugnis der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit zur Kontrolle der Einhaltung aller datenschutzrechtlichen Bestimmungen aus diesem Gesetz sowie allen anderen bereichsspezifisch für den Verfassungsschutz geltenden Bestimmungen über die Verarbeitung personenbezogener Daten geregelt. Die Befugnis findet ihre Grenzen, wenn entweder der Parlamentarischen Kontrollkommission oder der nach dem Landesgesetz zur parlamentarischen Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gebildeten Kommission die datenschutzrechtliche Kontrolle obliegt, es sei denn, die Kommission hat die oder den Landesbeauftragten beauftragt, die Einhaltung datenschutzrechtlicher

Bestimmungen bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten

Zu Absatz 2

Die Bestimmung entspricht der bisherigen Regelung in § 19 LVerfSchG.

Zu Absatz 3

Die Einhaltung der Kontrolle datenschutzrechtlicher Bestimmungen bei der Verfassungsschutzbehörde setzt voraus, dass das hierfür von der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit eingesetzte Personal ihrer oder seiner Behörde vorab nach den Bestimmungen des Landessicherheitsüberprüfungsgesetzes sicherheitsüberprüft wird. Da sich die betreffenden Personen mit der Befugnis nach Absatz 1 und 2 Zugang zu einer Vielzahl von mit dem Verschlusssachengrad geheim eingestuften Verschlusssachen verschaffen können, ist eine Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 12 des Landessicherheitsüberprüfungsgesetzes (Ü3) erforderlich.

Zu Teil 5 (Parlamentarische Kontrolle)

Die innere Sicherheit des Landes und die Sicherheit der Bevölkerung sind zu verteidigen, so der Grundgedanke der wehrhaften Demokratie, wie er in der Verfassung für Rheinland-Pfalz und im Grundgesetz für die Bundesrepublik Deutschland verankert ist. Eine maßgebliche Rolle spielt hierbei die Verfassungsschutzbehörde Rheinland-Pfalz. Sie gewinnt und bewertet Informationen über extremistische und sicherheitsgefährdende Bestrebungen.

So wesentlich der Verfassungsschutz für die freiheitlich-demokratische Grundordnung ist, so entscheidend ist seine wirksame Kontrolle. Denn bei der Sammlung von Informationen kann die Verfassungsschutzbehörde erheblich in Grundrechte eingreifen, etwa Auskünfte über Konten, Telekommunikation oder Flugverbindungen einholen oder Wohnungen mit technischen Mitteln überwachen. Die Maßnahmen finden im Verborgenen, ohne Wissen der Betroffenen statt. Eine gerichtliche Kontrolle kann daher in der Regel nicht erfolgen. Aus demselben Grund scheidet eine Kontrolle durch die Öffentlichkeit aus. Der parlamentarischen Kontrolle kommt daher entscheidende Bedeutung zu.

Entscheidend ist die parlamentarische Kontrolle auch insofern, als sie die gesellschaftliche Akzeptanz des Verfassungsschutzes fördert. Die Verfassungsschutzbehörde ist wegen ihrer herausragenden Bedeutung für die Sicherung der freiheitlich-demokratischen Grundordnung auf eine hohe Akzeptanz angewiesen. Vertrauen in die Lauterkeit und Gesetzmäßigkeit ihrer meist klandestinen Tätigkeit kann aber nur entstehen, wenn eine effektive und transparente Kontrolle stattfindet.

Der Verfassungsschutz kann nicht wirksam durch das Parlament als Ganzes kontrolliert werden. Zu viele Informationen müssten aus Gründen des Geheimschutzes zurückgehalten werden. Im Jahre 1978 wurde deshalb eine Parlamentarische Kontrollkommission eingerichtet, deren Mitglieder zur Geheimhaltung verpflichtet sind (Artikel 1 Nr. 3 des Landesgesetzes zur Änderung des Landesgesetzes über den Verfassungsschutz Rheinland-Pfalz vom 21. Dezember 1978, GVBl. S. 769). Die parlamentarische Kontrolle konnte so in einen Bereich erstreckt werden, der dem Parlament ansonsten verschlossen wäre.

Der vorliegende Entwurf einer Gesetzänderung sorgt dafür, dass die Parlamentarische Kontrollkommission ihrer Aufgabe weiterhin gewachsen ist. Die letzte grundlegende Modernisierung der parlamentarischen Kontrolle des Verfassungsschutzes erfolgte in den Jahren 1998 (Landesverfassungsschutzgesetz [LVerfSchG] vom 6. Juli 1998 [GVBl. S. 184], zuletzt geändert durch Artikel 3 des Gesetzes vom 22. Dezember 2015 [GVBl. S. 461], BS 12-2) und 2002 (Neufassung des Ausführungsgesetzes zu Artikel 10 GG und zur Fortentwicklung verfassungsschutzrechtlicher Vorschriften vom 16. Dezember 2002 [GVBl. S. 477]).

Stellung, Befugnisse und Ausstattung der Parlamentarischen Kontrollgremien und -kommissionen wurden auf Bundesebene und in den Ländern fortentwickelt. Neue Kontrollinstrumente wurden entwickelt und haben sich bewährt. Insoweit besteht Anpassungsbedarf.

Im Einzelnen sieht das Gesetz folgende Änderungen vor:

Die Tätigkeit der Verfassungsschutzbehörde ist umfangreicher und komplexer geworden. Insbesondere technische Zusammenhänge können ohne besonderen Sachverstand nicht nachvollzogen werden.

- Die Mitglieder der Parlamentarischen Kontrollkommission erhalten daher erstmals das Recht, eine sachverständige Person zu beauftragen. Nur so können sie zeitnah und fachlich fundiert auf komplexe Sachverhalte reagieren. Die Hinzuziehung von Sachverständigen hat sich auf Bundesebene bewährt (§ 34 Abs. 4).
- Die Zuarbeit durch eine Geschäftsstelle wird gesetzlich verankert. Sie bringt den hohen Stellenwert der Arbeit der Kontrollkommission zum Ausdruck und trägt dem gestiegenen Arbeitsaufwand Rechnung (§ 36).

Der Zugang zu Informationen wird verbessert:

- Die Mitglieder der Parlamentarischen Kontrollkomission erhalten mehr Selbstinformationsrechte. Mit deren Hilfe können sie sich Informationen selbst unmittelbar verschaffen und sind nicht auf mittelbare Unterrichtung durch die Landesregierung angewiesen. Zusätzlich zur Einsicht in Akten, Schriftstücke oder Dateien (§ 34 Abs. 1) wird das Recht gesetzlich verankert, jederzeit unangemeldet Zutritt zu den Räumlichkeiten der Verfassungsschutzbehörde zu verlangen (§ 34 Abs. 2) und Angehörige der Verfassungsschutzbehörde sowie das für die Tätigkeit der Verfassungsschutzbehörde zuständige Regierungsmitglied unmittelbar zu befragen (§ 34 Abs. 3).
- Angehörige der Verfassungsschutzbehörde erhalten die Möglichkeit, Eingaben direkt an die Parlamentarische Kontrollkommission zu richten, ohne die Behördenleitung zu informieren (§ 37). Hinweise aus den Nachrichtendiensten gehören auf Bundesebene zu den wichtigsten Informationsquellen für die Parlamentarische Kontrolle. Durch die Möglichkeit direkter Kontaktaufnahme und ein flankierendes Maßregelungs- und Benachteiligungsverbot werden solche Mitteilungen begünstigt.

- Die Pflicht der Landesregierung, die Parlamentarische Kontrollkommission zu unterrichten, wird konkretisiert. Für Vorgänge von besonderer Bedeutung wird die unverzügliche Unterrichtung neu aufgenommen. Das Kontrollrecht wird auf sonstige Vorgänge erstreckt. Über sie hat die Landesregierung auf Verlangen zu unterrichten (§ 33 Abs. 1).
- Der neue § 35 schafft Klarheit bezüglich der Grenzen der Auskunftspflichten. Ihre Einhaltung wird durch die Pflicht für die Landesregierung, die Verweigerung zu begründen, für die Parlamentarische Kontrollkommission überprüfbar.

Die Kontrollintensität wird erhöht. Es findet eine kontinuierliche und dauerhafte Kontrolle statt. Die Parlamentarische Kontrollkommission tritt mindestens alle drei Monate zusammen. Auf Verlangen eines Mitglieds der Kommission oder der Verfassungsschutzbehörde beruft die Vorsitzende oder der Vorsitzende sie unverzüglich ein (§ 32 Abs. 1). So wird ein regelmäßiger Informationsaustausch gewährleistet, bei Bedarf ein sofortiger.

Wesentlich für die Akzeptanz der Arbeit der Verfassungsschutzbehörde sind Transparenz und demokratische Rückkopplung der Kontrolle.

- Die Parlamentarische Kontrollkommission erhält die Möglichkeit, Vorgänge öffentlich zu bewerten (§ 32 Abs. 3). Soweit dies für die Bewertung unerlässlich ist, kann sie auch den zugrunde liegenden Sachverhalt öffentlich darstellen (§ 32 Abs. 4).
- Die unverzichtbare Rückkopplung zum Plenum als dem originären Ort demokratischer Kontrolle erfolgt durch Berichte mindestens in der Mitte und am Ende der Wahlperiode (§ 38).

Zu § 31 (Parlamentarische Kontrollkommission)

Zu Absatz 1

Die Vorschrift übernimmt mit redaktionellen Änderungen die bisherige Regelung (§ 20 Abs. 1). Sie unterstreicht, dass Adressatin der parlamentarischen Kontrolle nicht die Verfassungsschutzbehörde selbst ist, sondern die Landesregierung. Innerhalb der Landesregierung ist die Staatsministerin oder der Staatsminister verantwortlich, dem die Verfassungsschutzbehörde unterstellt ist.

Entsprechend dem Grundprinzip der repräsentativen Demokratie bleibt das Plenum der Ort der Willensbildung des Parlaments und der Kontrolle der Exekutive. Die Parlamentarische Kontrollkommission soll die Kontrolle durch das Plenum effektivieren, nicht ersetzen. Auch Kontrollbefugnisse der Ausschüsse bleiben erhalten. Die Kontrolle von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses ist der Kommission nach Artikel 10 GG vorbehalten.

Zu Absatz 2

Die Vorschrift des Absatz 2 gibt die bisher in § 20 Abs. 2 Satz 1 und Abs. 4 enthaltenen Regelungen wieder und ergänzt diese. Nur Abgeordnete können danach Mitglieder der Parlamentarischen Kontrollkommission werden. Scheidet eine Abgeordnete oder ein Abgeordneter aus dem Landtag aus, so endet kraft Gesetzes auch ihre oder seine Mitgliedschaft in der Parlamentarischen Kontrollkommission. Gleiches gilt, wenn sie oder er aus der Fraktion ausscheidet, der sie oder er im Zeitpunkt ihrer oder seiner Wahl angehört hat. Ebenso verliert die Mitgliedschaft in der Parlamentarischen Kontrollkommission, wer Mitglied der Landesregierung wird. Kontrollierender und Kontrollierter müssen personenverschieden sein. Für die Wahl eines neuen Mitglieds gelten die Regeln nach Satz 1.

Das Verfahren zur Bestimmung der Zahl der Mitglieder und die Zusammensetzung der Parlamentarischen Kontrollkommission wird entsprechend der bundesrechtlichen Regelung in § 2 Abs. 3 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz – PKGrG) vom 29. Juli 2009 (BGBl. I S. 2346), zuletzt geändert durch Artikel 13 des Gesetzes zur Änderung des VersorgungsrücklageG und weiterer dienstrechtlicher Vorschriften vom 5. Januar 2017 (BGBl. I S. 17), geändert (Begründung vgl. Bundestagsdrucksache 16/12411, S. 9 und Bundestagsdrucksache 08/1599, S. 7).

Die Arbeit der Parlamentarischen Kontrollkommission unterliegt ihrerseits keiner parlamentarischen Kontrolle. Die Abgeordneten, die nicht der Parlamentarischen Kontrollkommission angehören, müssen daher in besonderem Maße auf die fachliche Kompetenz und die Integrität der Mitglieder der Parlamentarischen Kontrollkommission vertrauen können. Dies wird durch ihre Wahl sichergestellt.

Zu Absatz 3

Nach dem Grundsatz der Diskontinuität endet mit einer Wahlperiode die Tätigkeit aller Gremien des Landtags. Die Tätigkeit der Verfassungsschutzbehörde bedarf jedoch kontinuierlicher Kontrolle. Daher nimmt die Parlamentarische Kontrollkommission ihre Aufgaben wahr, bis der nachfolgende Landtag Mitglieder für eine neue Parlamentarische Kontrollkommission gewählt hat.

Zu Absatz 4

Absatz 4 gibt die bisherige Regelung aus § 20 Abs. 2 Satz 2 wieder. Die Parlamentarische Kontrollkommission stellt in der konstituierenden Sitzung ihre Arbeits- und Funktionsfähigkeit her, indem sie eine Vorsitzende oder einen Vorsitzenden und eine Stellvertreterin oder einen Stellvertreter wählt und sich eine Geschäftsordnung gibt. Die Mitglieder der Parlamentarischen Kontrollkommission können dabei als Ausdruck ihrer Geschäftsordnungsautonomie innerhalb des gesetzlich vorgegebenen Rahmens ihre Arbeitsweise und innere Organisation selbst bestimmen.

Zu § 32 (Beratungen)

Neben Regelungen zum Zusammentritt der Kommission (Abs. 1) sucht die Vorschrift einen Ausgleich zwischen dem notwendigen Geheimschutz nachrichtendienstlicher Tätigkeit und der Transparenz und Öffentlichkeit parlamentarischer Kontrolle (Abs. 2 bis 4).

Zu Absatz 1

Die Vorschrift übernimmt die bisherige Regelung aus § 21 Abs. 2 Satz 1 und ergänzt diese. Die Parlamentarische Kontrollkommission wird einberufen, wenn eines ihrer Mitglieder dies verlangt. Zukünftig kann auch die Verfassungsschutzbehörde die Einberufung verlangen. Sie kann so die Parlamentarische Kontrollkommission aktiv informieren.

Die Einberufung der Kommission obliegt der Vorsitzenden oder dem Vorsitzenden, wie die neue Regelung klarstellt.

Der neu eingefügte Satz 1 sieht vor, dass die Parlamentarische Kontrollkommission mindestens alle drei Monate zusammentritt, auch ohne dass ein Mitglied der Kommission oder die Verfassungsschutzbehörde dies verlangt. Die Vorschrift greift die bisherige parlamentarische Praxis einer mitlaufenden, die Tätigkeit der Verfassungsschutzbehörde begleitenden Kontrolle auf. Sie stellt sicher, dass die Parlamentarische Kontrollkommission kontinuierlich durch die Regierung informiert wird.

Zu Absatz 2

Die Regelung des bisherigen § 20 Abs. 3 zur Geheimhaltungspflicht wird übernommen und um die Geheimhaltungspflicht des Personals der Geschäftsstelle ergänzt. Die Vorschrift schafft die Voraussetzungen für eine weitreichende parlamentarische Kontrolle des Verfassungsschutzes. Erst die Pflicht der Mitglieder und des Personals der Parlamentarischen Kontrollkommission, sämtliche Informationen geheim zu halten, ermöglicht der Landesregierung, die Parlamentarische Kontrollkommission umfassend und detailliert zu unterrichten.

Zu Absatz 3

Absatz 3 räumt der Parlamentarischen Kontrollkommission erstmals die Möglichkeit ein, die Tätigkeit der Verfassungsschutzbehörde öffentlich zu bewerten. Diese auf Bundesebene seit dem Jahr 1992 bestehende Möglichkeit hat sich als effektives Kontrollinstrument erwiesen. Parlamentarische Kontrolle zielt auf Öffentlichkeit. Öffentlichkeit ist ihr wichtigstes Instrument. Öffentlichkeit fördert auch die demokratische Rückkopplung. Wenn die Tätigkeit der Parlamentarischen Kontrollkommission öffentlich wahrnehmbar ist, kann sie vertrauensbildend wirken.

Öffentlich bewertet werden dürfen nur konkrete („bestimmte“) Vorgänge. Anlassunabhängige allgemeine Bewertungen sind nicht zulässig. Es muss ein erhebliches öffentliches Interesse an der Veröffentlichung naheliegen. Dieses kann insbesondere in der Gewährleistung effektiver Kontrolle oder der Herstellung erforderlicher Transparenz der Tätigkeit des Verfassungsschutzes sowie der Kontrollkommission liegen. Die Mitglieder der Parlamentarischen Kontrollkommission haben eine Prognose hierüber zu treffen. Bei der Auslegung des Begriffs des erheblichen öffentlichen Interesses kommt ihnen ein Beurteilungsspielraum zu. Dabei haben sie den Ausnahmecharakter der Vorschrift zu berücksichtigen. Die widerstreitenden Interessen der Veröffentlichung und Geheimhaltung sind im Einzelfall nach Verhältnismäßigkeitsgesichtspunkten gegeneinander abzuwägen.

Die Veröffentlichung der Bewertung darf nur erfolgen, wenn eine Mehrheit von zwei Dritteln der Mitglieder eingewilligt hat. Vor der Veröffentlichung muss die Landesregierung angehört werden. Der Bericht wird grundsätzlich als Drucksache veröffentlicht.

Satz 2 der Regelung stärkt die Minderheitenrechte in der Kommission. Er erlaubt Kommissionsmitgliedern, die die Bewertung nicht stützen, eine abweichende Bewertung zu veröffentlichen. Die Verfasserin oder der Verfasser eines Sondervotums hat deren Inhalt selbst zu verantworten und die Anforderungen zu beachten, die für den vergleichbaren Fall von Sondervoten in Untersuchungsausschüssen geregelt sind. Im Streitfall hat die Parlamentarische Kontrollkommission über deren Einhaltung zu befinden. Deshalb sind ihr Sondervoten vor der Veröffentlichung vorzulegen. Die Veröffentlichung erfolgt ausschließlich durch die Kommission und nicht etwa durch die Abgeordneten selbst.

Zu Absatz 4

Der Bewertung oder dem Sondervotum kann unter bestimmten Voraussetzungen eine Sachverhaltsdarstellung vorangestellt werden. Ihr Inhalt wird so für die Öffentlichkeit besser verständlich.

Zur Wahrung des notwendigen Geheimschutzes in diesem sensiblen Bereich darf eine Veröffentlichung insoweit jedoch nur erfolgen, wenn sie für die Bewertung oder das Sondervotum unerlässlich ist und weder zwingende Gründe des Nachrichtenzugangs entgegenstehen noch der Schutz von Persönlichkeitsrechten Dritter. Auch der Kernbereich exekutiver Eigenverantwortung darf nicht betroffen sein. Der ausdrückliche Verweis auf die in § 35 normierten Grenzen der Parlamentarischen Kontrolle betont ihren hohen Stellenwert im Rahmen der Entscheidung über eine Sachverhaltsdarstellung.

Zu § 33 (Unterrichtungspflicht der Landesregierung)

Für eine effektive Kontrolle ist die Parlamentarische Kontrollkommission auf die Unterrichtung durch die Landesregierung angewiesen. Die Vorschrift entwickelt die bisherige Regelung in § 21 fort. Sie erweitert und konkretisiert die Fremdinformationsrechte der Parlamentarischen Kontrollkommission gegenüber der Landesregierung.

Zu Absatz 1

Absatz 1 unterscheidet in Anlehnung an § 4 PKGrG verschiedene Unterrichtungspflichten:

Über die allgemeine Tätigkeit der Verfassungsschutzbehörde hat die Landesregierung umfassend zu unterrichten. Darunter fallen regelmäßige, typische Arbeitsabläufe der Verfassungsschutzbehörde und deren Ergebnisse. Die Parlamentarische Kontrollkommission soll ein möglichst vollständiges Bild über die allgemeine Tätigkeit der Nachrichtendienste erlangen, da nur auf der Basis umfassender Informationen eine Kontrolle der Regierung möglich ist. Die Unterrichtung hat im Abstand von höchstens sechs Monaten zu erfolgen. Dies entspricht der bisherigen Praxis. Die Formulierung wurde den Regelungen über besondere Auskunftsverlangen in § 8 b Abs. 10 Satz 1 i. V. m. Abs. 3 BVerfSchG angeglichen.

Über Geschehnisse von besonderer Bedeutung hat die Landesregierung unverzüglich, also so zeitnah wie möglich zu unterrichten. Gemeint sind Geschehnisse, die außerhalb der Regel liegen und deren Kenntnis für eine effektive Kontrolle erforderlich ist. Entsprechend der Legaldefinition in § 4 PKGrG betrifft dies insbesondere wesentliche Änderungen im Lagebild der äußeren und inneren Sicherheit, behördeninterne Vorgänge mit erheblichen Auswirkungen auf die Aufgabenerfüllung und Einzelvorkommnisse, die Gegenstand politischer Diskussionen oder öffentlicher Berichterstattung sind. In der Regel erfolgt die Unterrichtung in Abstimmung mit der oder dem Vorsitzenden.

Über sonstige Vorgänge hat die Landesregierung auf Verlangen eines Mitglieds der Parlamentarischen Kontrollkommis-

sion zu unterrichten. Die Pflicht bezieht sich auf Sachverhalte jeder Art, sofern ihre Kenntnis für die Ausübung wirksamer Kontrolle erforderlich ist. Das Verlangen bedarf keines Mehrheitsbeschlusses des Parlamentarischen Kontrollgremiums. Es kann von jedem Mitglied geäußert werden. So wird die Kontrollfunktion insgesamt gestärkt. Das Verlangen ist an die Vorsitzende oder den Vorsitzenden der Parlamentarischen Kontrollkommission zu richten.

Zu Absatz 2

Die Landesregierung unterrichtet die Parlamentarische Kontrollkommission über die Einholung von Auskünften nach § 13 Abs. 1 bis 4 (zum Beispiel bei Kreditinstituten, Verkehrsunternehmen, Erbringern von und Mitwirkenden an Telekommunikationsdiensten und Telemediendiensten). Gemäß § 8 b Abs. 10 Satz 1 BVerfSchG dürfen die Verfassungsschutzbehörden der Länder besondere Auskünfte bei den in § 13 Abs. 1, 2 und 4 genannten Unternehmen nur einholen, wenn eine § 8 b Abs. 3 BVerfSchG gleichwertige Kontrolle durch den Landesgesetzgeber vorgesehen ist. Dies setzt voraus, dass die Regierung die Parlamentarische Kontrollkommission im Abstand von höchstens sechs Monaten über solche Anordnungen informiert. Dabei hat sie insbesondere einen Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben. Die Landesregierung hat die Parlamentarische Kontrollkommission auch über die Einholung von Auskünften bei Erbringern von und Mitwirkenden an Postdienstleistungen zu unterrichten. Die Maßnahme ist in ihrer Art und Schwere vergleichbar mit den in § 13 Abs. 1, 2 und 4 genannten Auskünften.

Durch einen Verweis auf § 12 wird klargestellt, dass der Parlamentarischen Kontrollkommission auch die parlamentarische Kontrolle von Maßnahmen zur Überwachung des Brief-, Post- und Fernmeldeverkehrs obliegt.

Zu Absatz 3

Absatz 3 stellt klar, dass die Landesregierung auch über den Einsatz technischer Mittel unterrichten muss, die die Verfassungsschutzbehörde bei der Wohnraumüberwachung einsetzt, beispielsweise durch Einbau von Videokameras oder Abhörgeräten oder durch die Verwendung von Richtmikrofonen.

Artikel 13 Abs. 6 GG unterstellt diese Überwachungsmaßnahmen der parlamentarischen Kontrolle, weil sie besonders stark in das Grundrecht auf Unverletzlichkeit der Wohnung (Artikel 13 GG, Artikel 7 der Verfassung für Rheinland-Pfalz) eingreifen. Die Kontrolle bezieht sich dabei nicht auf die Rechtmäßigkeit einzelner Maßnahmen zur Wohnraumüberwachung – diese sind der Justiz vorbehalten, sondern auf die Frage, ob die Regelungen über den Einsatz besonderer technischer Mittel zur Überwachung von Wohnungen die Gefahrenabwehr verbessern und ob ausreichende gesetzgeberische Maßnahmen zum Grundrechtsschutz getroffen sind („Normeffizienz“). Hilfreiche Angaben in dem Bericht können dementsprechend solche über die Zahl der angeordneten Maßnahmen und deren Art (optisch oder akustisch), ihren Grund und ihr Ergebnis sein, aber auch zu ihrer Intensität, insbesondere ihrer Dauer.

Der Bericht ist entsprechend Artikel 13 Abs. 6 Satz 1 i. V. m. Satz 3 GG an das Landtagsplenum zu richten. Auf der Grundlage dieses Berichts übt gemäß Artikel 13 Abs. 6 Satz 1 i. V. m. Satz 2 GG die parlamentarische Kontrollkommission die Kontrolle aus.

Zu Absatz 4

Der Verweis auf an anderer Stelle im Gesetz geregelte Unterrichtungspflichten, wie in §§ 9 Abs. 2 Satz 3, 10 Abs. 5 und 11 Abs. 1 i. V. m. 10 Abs. 5, dient der Übersichtlichkeit.

Zu § 34 (Besondere Kontrollbefugnisse)

Die Selbstinformationsrechte der Parlamentarischen Kontrollkommission werden erheblich erweitert: neben das bereits bisher bestehende Einsichtsrecht in Akten, Dateien und sonstige Unterlagen (Abs. 1) tritt die Möglichkeit, eine sachverständige Person zu beauftragen (Abs. 4). Das Recht auf jederzeitigen Zutritt zur Verfassungsschutzbehörde (Abs. 2) und das Recht zur Befragung von Angehörigen der Verfassungsschutzbehörde und des für die Tätigkeit der Verfassungsschutzbehörde zuständigen Regierungsmitglieds (Abs. 3) werden gesetzlich verankert. Die Grenzen sind in § 35 geregelt.

Die Selbstinformationsrechte stehen nicht nur der Parlamentarischen Kontrollkommission als Ganzer zu, sondern jedem einzelnen Mitglied. Die Ausübung der Rechte hängt damit nicht von einem Mehrheitsbeschluss ab, sondern kann individuell geltend gemacht werden. Hierdurch wird die Kontrollfunktion insgesamt gestärkt.

Zu Absatz 1

Die Mitglieder der Parlamentarischen Kontrollkommission können Einsicht in Akten, Schriftstücke und Dateien verlangen. Die Einsichtnahme findet in den Räumlichkeiten der Verfassungsschutzbehörde statt. Ein Recht auf Herausgabe der Akten, Schriftstücke und Dateien an die Parlamentarische Kontrollkommission besteht nicht.

Zu Absatz 2

Das Recht, jederzeit unangemeldet die Verfassungsschutzbehörde zu betreten wird gesetzlich verankert. Es erleichtert die Einsichtnahme in Akten, Schriftstücke und Dateien.

Zu Absatz 3

Gesetzlich verankert wird auch das Recht, Angehörige der Verfassungsschutzbehörde und das für die Tätigkeit der Verfassungsschutzbehörde zuständige Regierungsmitglied zu befragen. Die Mitglieder der Parlamentarischen Kontrollkommission können auf diese Weise in direkten Kontakt zu den an zu überprüfenden Maßnahmen Beteiligten treten und sind nicht auf die nur mittelbaren Berichte der Landesregierung angewiesen.

Zu Absatz 4

Die Vorschrift gibt der Parlamentarischen Kontrollkommission erstmals die Möglichkeit, eine sachverständige Person zu beauftragen. Die schnelle und fachgerechte Bewertung von Vorgängen ist entscheidend für eine effektive Kontrolle. Der Rückgriff auf externen Sachverstand versetzt die Mitglieder der Parlamentarischen Kontrollkommission hierzu jederzeit in die Lage. Die Zunahme der netzgestützten Kommunikation im Rahmen der digitalen Entwicklung ermöglicht weitreichende Überwachungsmaßnahmen, die ohne

informationstechnische Kenntnisse nicht zu verstehen sind. Ihre Kontrolle erfordert ein immer spezielleres technisches Verständnis. Die oder der Sachverständige kann bei komplexen Sachverhalten die Vorarbeit übernehmen, unter anderem Material beschaffen und sichten und die zu beurteilenden Sachverhalte in tatsächlicher und rechtlicher Hinsicht aufbereiten. Auf der Grundlage solcher Vorermittlungen kann die Parlamentarische Kontrollkommission ihre Kontrolltätigkeit gezielter und zügiger durchführen. Der Einsatz von Sachverständigen hat sich auf Bundesebene seit dem Jahr 1999 bewährt.

Beauftragt die Parlamentarische Kontrollkommission eine sachverständige Person, so behält sie die Verfahrensherrschaft und bedient sich ihrer lediglich zur Unterstützung. Sie legt den Untersuchungsgegenstand selbst fest. Satz 1 fordert zu diesem Zweck die bestimmte Bezeichnung der Untersuchung. Der Auftrag muss eine ausreichende tatsächliche Grundlage aufweisen und von anderen Sachverhalten hinsichtlich Tatsachengrundlage und Fragestellung abgrenzbar sein. Allgemein gehaltene Formulierungen wie „Missstände“ reichen nicht aus. Vielmehr muss der konkrete Anlass für die Untersuchung benannt werden. Nur so ist erkennbar, wie weit die besonderen Kontrollbefugnisse aus § 34 im Einzelfall reichen.

Die Beauftragung bedarf einer Mehrheit von zwei Dritteln der Mitglieder der Parlamentarischen Kontrollkommission und der vorherigen Anhörung der Landesregierung.

Die sachverständige Person darf die Maßnahmen aus § 34 Abs. 1 und 2 und § 34 Abs. 3 Alternative 1 in den von § 35 gezogenen Grenzen ausüben und unterliegt der Geheimhaltungsverpflichtung aus § 32 Abs. 2. Soweit im Zuge der Untersuchung vorgesehen ist, dass als Verschlusssache eingestufte Tatsachen, Gegenstände oder Erkenntnisse von der sachverständigen Person zur Kenntnis genommen werden, ist zum Ausschluss von Sicherheitsrisiken vorab eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 12 des Landessicherheitsüberprüfungsgesetzes vom 8. März 2000 (GVBl. S. 70, BS 12-3) in der jeweils geltenden Fassung durchzuführen.

Die sachverständige Person hat der Parlamentarischen Kontrollkommission über das Ergebnis der Untersuchungen zu berichten.

Zu § 35 (Umfang der Unterrichtungspflicht)

Die Vorschrift zieht der parlamentarischen Kontrolle notwendige Grenzen. Sie liegen dort, wo der Verfassungsschutzbehörde die Verfügungsbefugnis über die begehrten Informationen fehlt (Abs. 1) oder ihre Weitergabe verfassungsrechtlich geschützte Güter verletzen würde (Abs. 2). Wie bereits dargestellt, gelten die Grenzen für die Unterrichtungspflicht der Regierung nach § 33 ebenso wie für die Selbstinformationsrechte der Parlamentarischen Kontrollkommission nach § 34.

Zu Absatz 1

Die Landesregierung darf nur Informationen weitergeben, die ihrer Verfügungsberechtigung unterliegen. Ausländische Behörden übermitteln Informationen in der Regel auf der Grundlage völkerrechtlicher Vereinbarungen, in denen festgelegt ist, unter welchen Voraussetzungen Personen Zugang zu den Informationen erhalten und welche Schutzmaßnahmen zur Geheimhaltung zu ergreifen sind.

Eine Weitergabe außerhalb der festgelegten Grenzen kann die Sicherheit des Partnerstaats gefährden und zur Verweigerung weiterer Zusammenarbeit führen. Die Zusammenarbeit der Nachrichtendienste dient dem Staatswohl. Ihr kommt Verfassungsrang zu. Vor dem Hintergrund des internationalen Terrorismus und der Gefährdung durch Cyberattacken wird sie durch das Bundesministerium des Inneren derzeit als von „überragender Bedeutung“ eingestuft (Verfassungsschutzberichte des Bundesministeriums des Inneren der Jahre 2014 bis 2016).

Zu Absatz 2

Parlamentarische Kontrolle kann im gewaltenteilenden Staat nicht unbegrenzt sein, sondern unterliegt wie die Tätigkeit aller Staatsgewalten verfassungsrechtlichen Schranken. Absatz 2 enthält eine Aufzählung der in Artikel 89 a der Verfassung für Rheinland-Pfalz niedergelegten und aus dem Grundgesetz abzuleitenden (BVerfG, Beschluss vom 13. Oktober 2016, 2 BvE 2/15, und Beschluss vom 17. Juni 2009, 2 BvE 3/07 u. a.) Informationsschranken. Die Formulierung der Vorschrift entspricht § 6 Abs. 2 PKGrG.

Der Informationspflicht können zwingende Gründe des Nachrichtenzugangs entgegenstehen. Dies ist der Fall, wenn durch die Weitergabe von Informationen die künftige Informationsbeschaffung in Frage gestellt ist. Beispielhaft seien Informationen von Vertrauenspersonen genannt. Durch die Offenlegung können Mitarbeiterinnen und Mitarbeiter oder Dritte erheblich in Gefahr geraten. Sie kann zur Verweigerung weiterer Zusammenarbeit führen. Wichtige Informationsquellen können damit verloren gehen.

Die Unterrichtung soll auch aus Gründen des Schutzes von Persönlichkeitsrechten Dritter unterbleiben. In Betracht kommen die Persönlichkeitsrechte von Mitarbeiterinnen und Mitarbeitern, insbesondere Agentinnen oder Agenten, V-Leuten und Informantinnen oder Informanten sowie die Persönlichkeitsrechte einzelner Bürgerinnen und Bürger. Beispielhaft ist das Recht auf informationelle Selbstbestimmung zu nennen.

Schließlich kann einer Unterrichtung entgegenstehen, dass sie den Kernbereich exekutiver Eigenverantwortung betrifft. Aus dem Gewaltenteilungsgrundsatz ergibt sich, dass Informationen dem Parlament und damit auch der Parlamentarischen Kontrollkommission nicht zustehen, wenn ihre Mitteilung Einfluss auf Entscheidungen haben kann, die allein von der Regierung zu treffen sind. Entscheidungen, die dem Kernbereich exekutiver Eigenverantwortung angehören, sind aus diesem Grund der parlamentarischen Kontrolle entzogen. Dies betrifft unter anderem laufende Verhandlungen und Entscheidungsvorbereitungen, darunter Meinungsbildungs- und Abstimmungsprozesse zwischen Landesregierung und Verfassungsschutzbehörde.

Bei der Prüfung der Voraussetzungen des Informationsanspruchs hat die Landesregierung im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen, ob die Informationen auf weniger einschneidende Weise als durch ihre vollständige Verweigerung geschützt werden können. Sie hat weiter abzuwägen, ob das Geheimhaltungsinteresse im konkreten Fall das Informationsinteresse der Parlamentarischen Kontrollkommission überwiegt. Die betroffenen Verfassungsgüter sind im Wege praktischer Konkordanz zum Ausgleich zu bringen.

Auf die Rechtsprechung des Bundesverfassungsgerichts zu den einzelnen Verweigerungsgründen im Hinblick auf den Parlamentarischen Untersuchungsausschuss wird Bezug genommen (s. o.). Sie sind als verfassungsrechtliche Schranken der parlamentarischen Kontrolle auf sämtliche Formen parlamentarischer Kontrolle übertragbar, gelten mithin entsprechend auch für die Parlamentarische Kontrollkommission.

Die Landesregierung hat die Verweigerung gegenüber der Parlamentarischen Kontrollkommission zu begründen. Sie muss eine konkrete und individuelle, der jeweiligen Problemlage angemessene Begründung liefern, die erkennen lässt, welche Belange abgewogen wurden und letztlich zur Versagung der Information geführt haben. Nur auf diese Weise kann die Parlamentarische Kontrollkommission überprüfen, ob die Informationen ihr zu Recht vorenthalten wurden und ihr Kontrollrecht wirksam ausüben. Andernfalls stünde die Informationsübermittlung zur Disposition der Landesregierung.

Ausdrücklich klargestellt wird, dass die Einschränkungen des Informationsanspruchs nicht nur die Unterrichtungspflicht aus § 33 betreffen, sondern auch die besonderen Kontrollbefugnisse aus § 34 Abs. 1 und Abs. 3. Sie können nicht weiter reichen als die Unterrichtungspflicht der Landesregierung. Für die Befugnis aus § 34 Abs. 1 ergibt sich dies außerdem durch die einleitende Formulierung „im Rahmen ihrer Kontrollrechte“, für die Befugnis aus § 34 Abs. 4 ist es in Satz 3 desselben Absatzes festgelegt.

Zu § 36 (Geschäftsstelle)

Der Parlamentarischen Kontrollkommission wird eine Geschäftsstelle zugeordnet. Sie unterstützt die Kommissionsmitglieder bei ihrer Arbeit. Die Anforderungen an die Kontrolltätigkeit der Kommission sind qualitativ und quantitativ gestiegen. Die bisher bestehende Parlamentspraxis wird gesetzlich festgeschrieben. Um eine effektive Kontrolle sicherzustellen, verankert die neue Vorschrift die Einrichtung und die Aufgaben der Geschäftsstelle im Gesetz.

Die Beschäftigten der Geschäftsstelle gehören der Parlamentsverwaltung an. Die Leitung übernimmt eine Beamtin oder ein Beamter, die oder der die Befähigung zum Richteramt besitzt. Die Vorschrift greift einen Gedanken auf, der bereits in die G 10-Gesetze des Bundes und des Landes Rheinland-Pfalz Eingang gefunden hat und auf die Rechtsprechung des Bundesverfassungsgerichts zurückgeht. Für die parlamentarische Kontrolle der Verfassungsschutzbehörden bei Beschränkung des Brief-, Post- und Fernmeldegeheimnisses hat das Bundesverfassungsgericht mit Urteil vom 14. Juli 1999 (1 BvR 2226/94 u. a.) betont, dass die zuständige G 10-Kommission personell so auszustatten ist, dass sie eine intensive und effektive Kontrolle zu leisten vermag.

Angesichts dessen, dass die Beschäftigten der Geschäftsstelle gleichzeitig in der Parlamentsverwaltung tätig sind, wird klarstellend aufgenommen, dass sie nur der Parlamentarischen Kontrollkommission unterstellt sind.

Zum Ausschluss von Sicherheitsrisiken ist für das Personal der Geschäftsstelle vor der Aufnahme seiner Tätigkeit eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 12 des Landessicherheitsüberprüfungsgesetzes vom 8. März 2000 (GVBl. S. 70, BS 12-3) in der jeweils geltenden Fassung durchzuführen.

Zu § 37 (Eingaben)

Zu Absatz 1

Die Vorschrift entspricht § 8 Abs. 1 des PKGrG. Angehörige der Verfassungsschutzbehörde können sich nunmehr direkt und vertrauensvoll an die Parlamentarische Kontrollkommission wenden, um auf mögliche dienstliche Missstände hinzuweisen. Auf Bundesebene hat sich dieser Weg als wichtige Informationsquelle herausgestellt. Missstände können mithilfe eines solchen „Frühwarnsystems“ unter Umständen zeitnah behoben werden.

Die Eingabe muss einen Bezug zur eigentlichen nachrichtendienstlichen Tätigkeit aufweisen. Eingaben im eigenen Interesse der oder des Angehörigen der Behörde oder im Interesse anderer Angehöriger, wie etwa Streit um die interne Besetzung von Dienstposten oder Personalvertretungsangelegenheiten werden ausdrücklich ausgenommen.

Satz 1 der Vorschrift sieht in Übereinstimmung mit der Neuregelung auf Bundesebene vor, dass Eingaben direkt an die Parlamentarische Kontrollkommission gerichtet werden können, ohne dass die Leitung der Behörde informiert wird.

Zusätzlich wird in Satz 2 das Verbot verankert, Angehörige der Verfassungsschutzbehörde wegen ihrer Eingabe dienstlich zu maßregeln oder sonst zu benachteiligen. Die Eingaben erfolgen im dienstlichen Interesse. Die oder der Beschäftigte ist deshalb vor Sanktionen zu schützen. Dieser Rechtsgedanke findet sich auch in anderen Vorschriften, etwa in § 20 Satz 2 des Landesgesetzes über den Bürgerbeauftragten des Landes Rheinland-Pfalz und den Beauftragten für die Landespolizei, § 7 Satz 2 des Gesetzes über den Wehrbeauftragten des Deutschen Bundestages, § 84 Abs. 3 des Betriebsverfassungsgesetzes und § 612 a des Bürgerlichen Gesetzbuches. Die Grenze des Maßregelungs- und Benachteiligungsverbots bilden Dienstvergehen oder Straftaten.

Die Parlamentarische Kontrollkommission übermittelt nach Satz 3 die Eingabe an die Landesregierung, damit diese eine Stellungnahme abgeben kann. Die vertrauliche Behandlung der Eingaben durch die Parlamentarische Kontrollkommission stellt dabei den Regelfall dar. Den Namen der hinweisgebenden Person teilt die Parlamentarische Kontrollkommission gemäß Satz 4 nur mit, wenn dies für die Aufklärung des Sachverhalts erforderlich ist.

Zu Absatz 2

Absatz 2 stellt sicher, dass die Parlamentarische Kontrollkommission Kenntnis von Bürgereingaben an den Landtag erhält, sofern diese hinreichend konkrete Vorwürfe bezüglich der Tätigkeit der Verfassungsschutzbehörde enthalten.

Zu § 38 (Bericht)

Die Vorschrift führt regelmäßige Berichte der parlamentarischen Kontrollkommission gegenüber dem Plenum ein. Wie zu § 32 ausgeführt, steht die parlamentarische Kontrolle der Exekutive entsprechend dem Grundsatz der parlamentarischen Demokratie originär dem Parlament als Ganzem zu. Die Parlamentarische Kontrollkommission soll die Kontrolle durch das Plenum effektivieren, nicht ersetzen. Die regelmäßigen Berichte gewährleisten die notwendige demokratische Rückkopplung.

Die Verpflichtung zur jährlichen Berichterstattung über die Einholung von Auskünften nach § 13 beruht auf § 8 b Abs. 10 Satz 1 BVerfSchG. Nach dieser Vorschrift stehen die Befugnisse zur Einholung von besonderen Auskünften den Verfassungsschutzbehörden der Länder nur zu, wenn eine § 8 b Abs. 3 BVerfSchG gleichwertige parlamentarische Kontrolle gewährleistet ist. Diese setzt jährliche Berichte über die Durchführung sowie Art, Umfang und Anordnungsgründe der Maßnahmen voraus.

Der Verweis auf § 32 Abs. 2 macht deutlich, dass nur insoweit zu berichten ist, als keine Geheimhaltungspflicht besteht.

Zu § 39 (Geltung des Landesdatenschutzgesetzes)

Die Bestimmung stellt klar, dass das LVerfSchG als bereichsspezifisches Spezialgesetz das Landesdatenschutzgesetz verdrängt. Das LDSG dient gemäß § 1 Abs. 1 und 2 der ergänzenden Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (EU-Datenschutzgrundverordnung) sowie der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (EU-Datenschutzrichtlinie).

Die Europäische Union hat jedoch gemäß Artikel 4 Abs. 2 Satz 3 EU-Vertrag keine Regelungskompetenz für den Bereich des Verfassungsschutzes, sodass abschließende bereichsspezifische Spezialregelungen im LVerfSchG unionrechtskonform möglich sind. Für das LDSG sowie die Datenschutzgrundverordnung besteht dagegen kein Raum, sodass die Anwendung des LDSG gemäß Satz 1 ausgeschlossen ist. Soweit aber einige im LDSG getroffenen Regelungen auch im Aufgabenbereich des § 5 und § 6 angemessen sind, gelten diese nach Satz 2 entsprechend. Im Einzelnen sind dies § 14 (Landesbeauftragte oder Landesbeauftragter für den Datenschutz und die Informationsfreiheit), § 15 (Aufgaben und Organisation), § 27 LDSG (Begriffsbestimmungen), § 33 Absatz 1 bis Absatz 4 LDSG (Einwilligung), § 34 LDSG (Verarbeitung auf Weisung des Verantwortlichen), § 35 LDSG (Datengeheimnis), §§ 37 bis 39 LDSG teilweise (Datenschutzbeauftragte öffentlicher Stellen), § 42 Absatz 1 (Befugnis zur Beanstandung), § 51 LDSG (Auftragsverarbeitung) und § 53 LDSG (Anforderungen an die Sicherheit der Datenverarbeitung).

Zu § 40 (Einschränkung von Grundrechten)

Die Bestimmung zitiert das durch dieses Gesetz eingeschränkte Grundrecht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes bzw. Artikel 4 a der Verfassung für Rheinland-Pfalz) und das Grundrecht aus Artikel 13 GG bzw. Artikel 7 der Verfassung für Rheinland-Pfalz sowie das Grundrecht aus Artikel 10 GG bzw. Artikel 14 der Verfassung für Rheinland-Pfalz.

Zu § 41 (Änderung des Landessicherheitsüberprüfungsgesetzes)

Mit dieser Bestimmung wird das Landessicherheitsüberprüfungsgesetz als Folge der Neufassung des Landesverfassungsschutzgesetzes redaktionell angepasst.

Zu § 42 (Änderung des Polizei- und Ordnungsbehördengesetzes)

Mit dieser Bestimmung wird das Polizei- und Ordnungsbehördengesetz als Folge der Neufassung des Landesverfassungsschutzgesetzes redaktionell angepasst.

Zu § 43 (Inkrafttreten)

Diese Bestimmung regelt das Inkrafttreten der Neufassung des Landesverfassungsschutzgesetzes am Tage nach der Verkündung; das bisherige Landesverfassungsschutzgesetz tritt gleichzeitig außer Kraft.

Für die Fraktion der SPD:
Martin Haller

Für die Fraktion der FDP:
Marco Weber

Für die Fraktion BÜNDNIS 90/DIE GRÜNEN:
Pia Schellhammer