

## **GESETZENTWURF**

### **der Landesregierung**

#### **Entwurf eines Dritten Gesetzes zur Änderung des Landesverfassungsschutzgesetzes**

##### **A Problem und Ziel**

Die Tätigkeit des Verfassungsschutzes umfasst in einem hohen Maße die Gewinnung von personenbezogenen Daten und den Umgang mit diesen, um auf dieser Grundlage seine gesetzliche Aufgabe – dem Schutz der freiheitlichen demokratischen Grundordnung, dem Bestand und der Sicherheit des Bundes und der Länder zu dienen – zu erfüllen. Das Landesverfassungsschutzgesetz formuliert einerseits die Grundlagen für das (rechtmäßige) Handeln des Verfassungsschutzes. Andererseits müssen diese Rechtsgrundlagen Grenzen beinhalten, die den Schutz des Einzelnen in seinem Persönlichkeitsrecht im Hinblick auf seine Daten sicherstellen. Beide Rechtsgüter – die Funktionsfähigkeit des Verfassungsschutzes auf der einen und das Recht des Einzelnen an seinen Daten auf der anderen Seite – sind in den Vorschriften in einen angemessenen Ausgleich zu bringen. Verfassungsschutzrecht ist gleichzeitig sowohl Eingriffsrecht als auch Datenschutzrecht.

Staatliche Eingriffe in Rechte einzelner Personen müssen grundsätzlich dem Verhältnismäßigkeitsprinzip genügen. Danach müssen sie geeignet sein, das angestrebte Ziel zu erreichen oder zu fördern, sowie erforderlich in dem Sinne sein, dass kein milderes, den Betroffenen weniger belastendes Mittel zur Verfügung steht, das den Zweck ebenso gut zu fördern vermag. Und der geeignete und erforderliche Eingriff muss verhältnismäßig im engeren Sinne sein. Dies bedeutet, dass der mit dem Eingriff verbundene Schaden nicht im groben Missverhältnis zum angestrebten Zweck stehen darf.

Das Bundesverfassungsgericht hatte in den Jahren 2022 und 2024 Vorschriften in verschiedenen Verfassungsschutzgesetzen auf ihre Verfassungsmäßigkeit zu prüfen. Im Mittelpunkt standen die konkreten Anforderungen des Verhältnismäßigkeitsprinzips an die Tätigkeit des Verfassungsschutzes. Das Gericht formulierte Pflichten des Gesetzgebers, Eingriffsschwellen orientiert am verfassungsschutzspezifischen Aufklärungsbedarf und dem jeweiligen Eingriffsgewicht gesetzlich zu definieren. Als Eingriff wurde dabei nicht nur die spezielle Überwachungsmaßnahme zur Erhebung personenbezogener Daten, sondern prinzipiell auch deren Übermittlung an andere Stellen gesehen.

Unmittelbare Rechtswirkung entfalten die benannten Entscheidungen nur gegenüber den Ländern Bayern und Hessen sowie dem Bund. Das Gericht hat aber über die in den Verfahren jeweils überprüften Rechtsnormen hinausgehende Grundsatzentscheidungen zum Recht des Verfassungsschutzes getroffen, die sich auf alle Verfassungsschutzgesetze in Bund und Ländern auswirken. Filigranere Anforderungen an die Verfassungsmäßigkeit des Handelns von Verfassungsschutzbehörden und für deren Datenübermittlungen an andere Behörden wurden formuliert, die die Gesetzgeber normenklar zu regeln haben.

Welche Folgen aus der Rechtsprechung des Bundesverfassungsgerichts im Hinblick auf den Informationsaustausch zwischen den Sicherheitsbehörden und hier insbesondere zwischen dem Verfassungsschutz und der Polizei resultieren, wird aus dem nachfolgend wiedergegebenen Beschluss der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 27. Januar 2025 zum Tagesordnungspunkt „Innere Sicherheit angesichts der Anschläge von Aschaffenburg, Magdeburg, Mannheim und Solingen“ in Ziffer 8 deutlich:

- „8. Sie nimmt Bezug auf den Beschluss der IMK in ihrer Sitzung vom 12. bis 14. Juni 2017 zu TOP 34 und betont mit Nachdruck, dass eine Intensivierung des Informationsaustauschs zwischen den Sicherheitsbehörden zur effektiven Abwehr von Terrorakten und anderen schwerwiegenden Bedrohungen, die auf eine Destabilisierung des Gemeinwesens zielen oder dazu beitragen, unverzichtbar ist.
- a) Sie stellt fest, dass die Rechtsprechung des Bundesverfassungsgerichts in den vergangenen Jahren der informationellen Zusammenarbeit einen immer engeren Rahmen vorgegeben hat. Vor allem für die Übermittlung nachrichtendienstlich erlangter Informationen an Polizei- und Strafverfolgungsbehörden hat die Rechtsprechung sehr hohe und im internationalen Vergleich einzigartige Hürden aufgestellt. Damit wird eine Zusammenführung der bei verschiedenen Sicherheitsbehörden vorliegenden Informationen zur umfassenden Bewertung der von einzelnen Personen und Gruppierungen ausgehenden Sicherheitsgefährdung erschwert.
  - b) Die IMK weist darauf hin, dass im Grundgesetz die Zusammenarbeit zwischen Nachrichtendiensten und Polizeibehörden des Bundes und der Länder ausdrücklich vorausgesetzt wird.
  - c) Sie spricht sich vor diesem Hintergrund dafür aus, eine Klarstellung durch den verfassungsändernden Gesetzgeber dahingehend zu prüfen, dass diese Zusammenarbeit auch den Informationsaustausch umfasst. Auf diesem Weg könnten die Sicherheitsbehörden von Bund und Ländern auch verfassungsrechtlich verpflichtet werden, zum Schutz von besonders gewichtigen Rechtsgütern, insbesondere von Leib und Leben sowie den Existenzgrundlagen des Staates, eng zusammenzuarbeiten, und die dafür geltenden Anforderungen an den Informationsaustausch konkretisiert werden.“

**B Lösung**

Das Landesverfassungsschutzgesetz wird entsprechend den Ausführungen unter A geändert. Aufgrund der angeführten Entscheidungen ergibt sich folgender gesetzgeberischer Anpassungsbedarf:

- Überarbeitung von Rechtsgrundlagen für Maßnahmen des Verfassungsschutzes,
- Einführung einer unabhängigen Kontrolle von bestimmten Maßnahmen des Verfassungsschutzes,
- Überarbeitung der Rechtsgrundlagen zur Übermittlung von Erkenntnissen des Verfassungsschutzes und
- Regelung des Schutzes des Kernbereichs privater Lebensgestaltung und der Personen, die dem Berufsgeheimnis unterliegen.

Hinzu kommen

- eine Rechtsgrundlage für Auskunftersuchen an das Bundeszentralamt für Steuern,
- Ergänzungen der Vorschriften zur Parlamentarischen Kontrollkommission im Hinblick auf das Format ihrer Sitzungen und die Mitarbeit von Bediensteten der Kommission,
- eine Rechtsgrundlage für Eingaben der Bediensteten des Verfassungsschutzes an die Parlamentarische Kontrollkommission,
- ergänzende Vorschriften zum allgemeinen Datenschutz beim Verfassungsschutz sowie
- Regelungen zur Sicherung von Verschlusssachen beim Verfassungsschutz.

**C Alternativen**

Keine. Mit den vorgesehenen Änderungen des Landesverfassungsschutzgesetzes werden hauptsächlich verfassungsrechtliche Vorgaben des Bundesverfassungsgerichts umgesetzt, um einen verfassungskonformen Vollzug des Gesetzes zu gewährleisten.

**D Notwendigkeit (§ 3 Absatz 1 Satz 1 GGO II)**

Die Notwendigkeit der Gesetzesänderungen ergibt sich aus den unter A dargelegten Gründen.

**E Finanzielle Auswirkungen auf die Haushalte des Landes und der Kommunen****1. Haushaltsausgaben ohne Vollzugsaufwand**

Durch die mit diesem Gesetzentwurf vorgesehenen Änderungen entstehen keine weiteren Kosten, da die Anpassungen zu bereits schon bestehenden Eingriffsnormen erfolgen.

## **2. Vollzugsaufwand**

Es werden zusätzliche, nicht konkret bezifferbare personelle Ressourcen gebunden, die jedoch auf die Umsetzung der verfassungsrechtlichen Vorgaben und auf die notwendigen Anpassungen aufgrund der neu geordneten Übermittlungsbefugnisse zurückzuführen sind. Generell gilt, dass der Bedarf personeller Ressourcen durch Organisationsmaßnahmen im Rahmen der vereinbarten Stellenpläne und Personalentwicklungsplanungen kompensiert wird, sodass keine Stellenmehrbedarfe entstehen. Finanzielle Bedarfe werden grundsätzlich im Rahmen bereits veranschlagter Mittel sowie der mittelfristigen Finanzplanung abgedeckt.

### **F Sonstige Kosten**

Es entsteht gegenüber den bisherigen gesetzlichen Regelungslagen kein zusätzlicher Erfüllungsaufwand.

### **G Bürokratiefolgen**

Die Aufnahme gesetzlicher Regelungen zu Mitteilungs- und Dokumentationspflichten führen zu Verwaltungsmehraufwand. Darüber hinaus werden durch den im Gesetz vorgesehenen Verweis auf nähere Ausgestaltungen in Dienstvorschriften weitere untergesetzliche Vorschriften erforderlich.

**DIE MINISTERPRÄSIDENTIN  
DES LANDES  
MECKLENBURG-VORPOMMERN**

Schwerin, den 28. Oktober 2025

An die  
Präsidentin des Landtages  
Mecklenburg-Vorpommern  
Frau Birgit Hesse  
Lennéstraße 1

19053 Schwerin

**Entwurf eines Dritten Gesetzes zur Änderung des Landesverfassungsschutzgesetzes**

Sehr geehrte Frau Präsidentin,

als Anlage übersende ich Ihnen den von der Landesregierung am 28. Oktober 2025 beschlossenen Entwurf des vorbezeichneten Gesetzes mit Begründung.

Ich bitte Sie, die Beschlussfassung des Landtages herbeizuführen.

Federführend ist das Ministerium für Inneres und Bau.

Mit freundlichen Grüßen

**Manuela Schwesig**

## ENTWURF

### eines Dritten Gesetzes zur Änderung des Landesverfassungsschutzgesetzes

Der Landtag hat das folgende Gesetz beschlossen:

#### **Artikel 1** **Änderung des Landesverfassungsschutzgesetzes**

Das Landesverfassungsschutzgesetz vom 11. Juli 2001 (GVOBl. M-V S. 261), das zuletzt durch Artikel 1 des Gesetzes vom 25. Oktober 2022 (GVOBl. M-V S. 547) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 6 wird die folgende Angabe eingefügt:

„§ 6a Beobachtungsbedürftigkeit“.

b) Die Angabe zu § 10a wird durch die folgende Angabe ersetzt:

„§ 10a Schutz des Kernbereichs privater Lebensgestaltung und der Personen,  
die dem Berufsgeheimnis unterliegen

§ 10b Vertrauensleute und verdeckte Bedienstete

§ 10c Observationen

§ 10d Verdecktes Mithören oder Aufzeichnen des nicht öffentlichen Wortes unter  
Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13  
des Grundgesetzes

§ 10e Verdeckte Standortermittlung und Ermittlung der Geräte- und Kartennummer  
mit technischen Mitteln

§ 10f Unabhängige Kontrolle“.

c) Die Angabe zu den §§ 16 und 17 wird durch die folgende Angabe ersetzt:

„§ 16 Verarbeitung personenbezogener Daten von Minderjährigen

§ 17 Speichern, Berichten, Löschen und Verarbeitungseinschränkung  
personenbezogener Daten“.

d) Die Angabe zu § 20 wird durch die folgende Angabe ersetzt:

„§ 20 Zweckbindung, Weiterverarbeitung“.

e) Die Angabe zu § 20a wird durch die folgende Angabe ersetzt:

- „§ 20a Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr
- § 20b Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz
- § 20c Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung
- § 20d Übermittlung an inländische öffentliche Stellen ohne belastende Maßnahmen mit Außenwirkung
- § 20e Übermittlung an inländische nicht öffentliche Stellen
- § 20f Projektbezogene gemeinsame Dateien
- § 20g Minderjährigenschutz bei Inlandsübermittlung“.

f) Die Angabe zu den §§ 22 und 23 wird durch die folgende Angabe ersetzt:

- „§ 22 Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen und Übermittlung zum Schutz der Betroffenen
- § 23 Protokollierung der Übermittlungen und weitere Verfahrensregelungen“.

g) Die Angabe zu § 24a wird durch die folgende Angabe ersetzt:

- „§ 24a Informationsübermittlung durch nicht öffentliche Stellen an die Verfassungsschutzbehörde, Ersuchen an das Bundeszentralamt für Steuern“.

h) Nach der Angabe zu § 29 wird die folgende Angabe eingefügt:

- „§ 29a Eingaben“.

i) Die Angabe zu den §§ 30 bis 32 wird durch die folgende Angabe ersetzt:

- „§ 30 Anwendung des allgemeinen Datenschutzrechts
- § 31 Unabhängige Datenschutzkontrolle
- § 32 Maßnahmen zur Sicherung von Verschlusssachen
- § 33 Durchführung von Maßnahmen zur Sicherung von Verschlusssachen“.

j) Die bisherige Angabe zu § 32 wird die Angabe zu § 34.

2. In § 2 Absatz 1 Satz 2 wird die Angabe „Ministerium für Inneres, Bau und Digitalisierung“ durch die Angabe „für den Verfassungsschutz zuständige Ministerium“ ersetzt.

3. § 5 wird wie folgt geändert:

- a) In Absatz 1 Nummer 4 wird jeweils die Angabe „Abs.“ durch die Angabe „Absatz“ ersetzt.
- b) In Absatz 2 Satz 1 wird nach der Angabe „Länder“ die Angabe „sowie über präventiven Wirtschaftsschutz“ eingefügt.

- c) Nach Absatz 2 wird der folgende Absatz 3 eingefügt:

„(3) Bei der Unterrichtung der Öffentlichkeit über Erkenntnisse der Verfassungsschutzbehörde ist die Übermittlung von personenbezogenen Daten nur zulässig, wenn die Bekanntgabe für das Verständnis des Zusammenhangs erforderlich ist und die Interessen der Allgemeinheit das schutzwürdige Interesse der betroffenen Person überwiegen. Soweit Umfang und Qualität der zu veröffentlichenden personenbezogenen Daten dies im Einzelfall erfordern, sind die betroffene oder eine dritte Person vorab darüber zu informieren.“

- d) Der bisherige Absatz 3 wird zu Absatz 4 und Nummer 1 wird durch die folgende Nummer 1 ersetzt:

„1. bei der Sicherheitsüberprüfung von Personen nach Maßgabe des Sicherheitsüberprüfungsgesetzes vom 22. Januar 1998 (GVOBl. M-V S. 114, 195), das zuletzt durch Artikel 2 des Gesetzes vom 25. April 2016 (GVOBl. M-V S. 203, 206) geändert wurde, sowie bei Überprüfungen von Personen in sonstigen gesetzlich bestimmten Fällen,“.

- e) Der bisherige Absatz 4 wird zu Absatz 5.

4. § 6 wird wie folgt geändert:

- a) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Für einen Personenzusammenschluss handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. Bestrebungen im Sinne des § 5 Absatz 1 können auch von Einzelpersonen ausgehen, die nicht in einem oder für einen Personenzusammenschluss handeln. In diesem Fall gilt Satz 1 mit der Maßgabe, dass die Verhaltensweise der Einzelperson darauf gerichtet sein muss, die dort genannten Ziele zu verwirklichen.“

- b) Absatz 4 wird gestrichen.

- c) Absatz 5 wird zu Absatz 4 und in Satz 1 wird die Angabe „Abs.“ durch die Angabe „Absatz“ ersetzt.

- d) Absatz 6 wird gestrichen.

5. Nach § 6 wird der folgende § 6a eingefügt:

**„§ 6a  
Beobachtungsbedürftigkeit**

(1) Beobachtungsbedürftig im Sinne dieses Gesetzes sind Bestrebungen gemäß § 5 Absatz 1 Nummer 1, 3 und 4.



(2) Erheblich beobachtungsbedürftig im Sinne dieses Gesetzes sind Tätigkeiten nach § 5 Absatz 1 Nummer 2 oder solche Bestrebungen, die allgemein, insbesondere nach Verhaltens- oder Wirkungsweise, geeignet sind, die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes erheblich im Sinne von Absatz 4 Satz 2 zu beeinträchtigen.

(3) Die Eignung im Sinne von Absatz 2 ist anzunehmen, wenn die Bestrebungen zur Zielverfolgung

1. Gewalt anwenden, androhen, fördern oder befürworten,
2. zu Hass oder Willkürmaßnahmen anstacheln oder
3. andere Straftaten begehen oder darauf gerichtet sind.

Eine Eignung liegt in der Regel auch vor, wenn die Bestrebungen zur Zielerreichung

1. verdeckt vorgehen, insbesondere Ziele, Organisation, Finanzierung, Beteiligte, Zusammenarbeit oder Umfang verschleiern, oder
2. erhebliche gesellschaftliche Bedeutung besitzen, insbesondere unter Berücksichtigung der Anzahl der Beteiligten, deren Mobilisierungsfähigkeit, der Finanzkraft sowie der Aktionsfähigkeit.

Die Eignung kann auch anzunehmen sein, wenn Bestrebungen zur Zielerreichung in erheblichem Umfang gesellschaftlichen Einfluss auszuüben suchen, insbesondere durch

1. Vertretung in Ämtern und Mandaten,
2. wirkungsbreite Publikationen, Bündnisse, Unterstützerstrukturen,
3. systematische Desinformationen in öffentlichen Prozessen politischer Willensbildung oder zur Verächtlichmachung der freiheitlichen demokratischen Grundordnung, auch durch systematische Verunglimpfung ihrer Institutionen und Repräsentanten, oder
4. Herbeiführung einer Atmosphäre der Angst oder Bedrohung zur Förderung ihrer Zielverfolgung.

(4) Voraussetzung für die Einstufung ist, dass hinreichende tatsächliche Anhaltspunkte für die Sachverhalte nach den Absätzen 1 bis 3 vorliegen. Die Beobachtungsbedürftigkeit steigt umso stärker, je deutlicher tatsächliche Anhaltspunkte vorliegen, die es möglich erscheinen lassen, dass die Schutzgüter des Verfassungsschutzes konkret bedroht sind und dass das gegen sie gerichtete Handeln erfolgreich sein kann. Die Beobachtungsbedürftigkeit ist jährlich zu überprüfen. Sie entfällt, wenn nach 5 Jahren kein die Einstufung begründender Sachverhalt hinreichend festgestellt ist oder eine 5 Jahre zurückliegende Feststellung sich zwischenzeitlich nicht neuerlich bestätigt hat.“

6. § 7 Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) Die Verfassungsschutzbehörde darf Informationen einschließlich personenbezogener Daten verarbeiten, soweit sie zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich sind. Voraussetzung für die Sammlung von Informationen im Sinne des § 5 Absatz 1 ist das Vorliegen tatsächlicher Anhaltspunkte, die, insgesamt betrachtet und unter Einbeziehung nachrichtendienstlicher Erfahrungen, den Verdacht einer der in § 5 Absatz 1 genannten Bestrebungen oder Tätigkeiten rechtfertigen. Art und Umfang des Umgangs mit Informationen richten sich nach den Vorschriften dieses Gesetzes. Im Übrigen findet das allgemeine Datenschutzrecht nach Maßgabe des § 30 Anwendung.“

7. § 9 Absatz 1 und 2 wird durch die folgenden Absätze 1 und 2 ersetzt:

„(1) Die Verfassungsschutzbehörde darf personenbezogene Daten der betroffenen Person auch ohne deren Kenntnis bei ihr und bei Dritten erheben, wenn

1. tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten gemäß § 5 Absatz 1 vorliegen,
2. dies für die Erforschung und Bewertung von gewalttätigen Bestrebungen nach § 5 Absatz 1 Nummer 3 oder Tätigkeiten nach § 5 Absatz 1 Nummer 2 erforderlich ist oder
3. dies zur Schaffung oder Erhaltung nachrichtendienstlicher Zugänge über Bestrebungen oder Tätigkeiten nach § 5 Absatz 1 erforderlich ist.

Die Verarbeitung der Daten ist auch zulässig, wenn die betroffene Person eingewilligt hat; sie ist über die Freiwilligkeit der Mitwirkung und den Verwendungszweck zu informieren. Die Informationspflicht umfasst bei einer beabsichtigten Übermittlung auch die empfangende Stelle der Daten.

(2) Personenbezogene Daten von Dritten dürfen ohne deren Kenntnis nur erhoben werden, wenn

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

Daten Dritter dürfen auch erhoben werden, wenn sie mit zur Aufgabenerfüllung erforderlichen Informationen untrennbar verbunden sind. Daten, die für das Verständnis der zu speichernden Informationen nicht erforderlich sind, sind unverzüglich zu löschen. Dies gilt nicht, wenn die Löschung nicht oder nur mit unververtretbarem Aufwand möglich ist. In diesem Fall ist die Verarbeitung der Daten gemäß § 17 Absatz 4 und 5 einzuschränken; diese Daten dürfen nicht mehr genutzt werden.“

8. § 10 wird durch den folgenden § 10 ersetzt:

#### **„§ 10**

#### **Informationsbeschaffung mit nachrichtendienstlichen Mitteln**

(1) Die Verfassungsschutzbehörde darf zur verdeckten Informationsbeschaffung, insbesondere zur verdeckten Erhebung personenbezogener Daten, folgende nachrichtendienstliche Mittel anwenden:

1. Inanspruchnahme von Vertrauensleuten nach Maßgabe des § 10b, sonstigen Informanten und Gewährspersonen,
2. Einsatz von verdeckten Bediensteten nach Maßgabe des § 10b,
3. Observationen nach Maßgabe des § 10c,
4. Bildaufzeichnungen (Fotografieren, Filmen und Videografieren) außerhalb des Schutzbereiches des Artikels 13 des Grundgesetzes,
5. verdeckte Ermittlungen und Befragungen,

6. verdecktes Mithören ohne Inanspruchnahme technischer Mittel,
7. verdecktes Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13 des Grundgesetzes nach Maßgabe des § 10d,
8. Beobachtung des Funkverkehrs auf nicht für den allgemeinen Empfang bestimmten Kanälen,
9. Verwendung fingierter biografischer, beruflicher oder gewerblicher Angaben (Legenden),
10. Beschaffung, Herstellung und Verwendung von Tarnpapieren und Tarnkennzeichen,
11. Überwachung des Brief-, Post- und Fernmeldeverkehrs nach Maßgabe des aufgrund von Artikel 10 Absatz 2 Satz 1 des Grundgesetzes erlassenen Bundesgesetzes,
12. verdecktes Beobachten und sonstiges Aufklären des Internets, ohne dass der Schutzbereich des Artikels 10 des Grundgesetzes (Brief-, Post- und Fernmeldegeheimnis) berührt ist, unter einer Legende und unter Ausnutzung eines schutzwürdigen Vertrauens der betroffenen oder einer dritten Person in die Identität und Motivation des Kommunikationspartners,
13. verdeckte Standortermittlung und Ermittlung der Geräte- und Kartennummer mit technischen Mitteln nach Maßgabe des § 10e.

(2) Die Mittel nach Absatz 1 dürfen, soweit nicht anders geregelt, nur angewendet werden, wenn

1. die Voraussetzungen des § 9 Absatz 1 Nummer 1, 2 oder 3 vorliegen,
2. sich ihr Einsatz gegen Dritte richtet, deren Einbeziehung in eine solche Maßnahme unumgänglich ist, um auf diese Weise Erkenntnisse über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen zu gewinnen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 5 Absatz 1 Nummer 1 und 3 genannten Schutzgüter gerichtet sind oder
3. dies zur Abschirmung der Bediensteten, Einrichtungen, Gegenstände und Nachrichtenzugänge des Verfassungsschutzes gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist.

Die Mittel nach Absatz 1 Satz 1 Nummer 9 und 10 dürfen auch für Vertrauensleute angewendet werden, wenn dies zur Erfüllung eines dienstlichen Auftrags oder zu ihrem Schutz erforderlich ist.

(3) Die Anwendung nachrichtendienstlicher Mittel gemäß Absatz 1 ist unzulässig, wenn die Informationsbeschaffung auf andere, die betroffene Person weniger beeinträchtigende Weise möglich ist. Eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Daten aus allgemein zugänglichen Quellen oder durch Übermittlung nach § 24 gewonnen werden können. Die Anwendung nachrichtendienstlicher Mittel darf nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Bei Maßnahmen nach Absatz 1 Nummer 1, 2, 3, 7 und 13 ist die Beobachtungsbedürftigkeit im Sinne von § 6a in Verbindung mit den § 10b Absatz 4, § 10c Absatz 2, § 10d Absatz 1 und § 10e Absatz 2 zu beachten.

(3a) Die Verfassungsschutzbehörde darf die mit nachrichtendienstlichen Mitteln erhobenen Daten nur für die in § 9 Absatz 1 genannten Zwecke nutzen. Daten, die für diese Zwecke nicht erforderlich sind, sind unverzüglich zu löschen. Sind diese Daten mit anderen, für die in § 9 Absatz 1 genannten Zwecke erforderlichen Daten derart verbunden, dass sie nicht oder nur mit einem unverhältnismäßig großen Aufwand getrennt werden können, so ist die Verarbeitung dieser Daten einzuschränken; sie dürfen nicht mehr genutzt werden.

(4) Wirkt die Verfassungsschutzbehörde an Sicherheitsüberprüfungen im Sinne des § 5 Absatz 3 Nummer 1 mit, so darf sie nur das nachrichtendienstliche Mittel der Tarnung von Bediensteten anwenden.

(5) Die Behörden des Landes sowie die Kommunalbehörden sind verpflichtet, der Verfassungsschutzbehörde Hilfe für Tarnungsmaßnahmen zu leisten.“

9. § 10a wird durch den folgenden § 10a ersetzt:

**„§ 10a  
Schutz des Kernbereichs privater Lebensgestaltung und der Personen,  
die dem Berufsgeheimnis unterliegen**

(1) Die Anwendung nachrichtendienstlicher Mittel ist unzulässig, soweit hinreichend gewichtige tatsächliche Anhaltspunkte vorliegen, dass durch sie allein Erkenntnisse gewonnen werden würden

1. aus dem Kernbereich privater Lebensgestaltung oder
2. über die eine Rechtsanwältin, ein Rechtsanwalt, ein Kammerrechtsbeistand, eine der in § 53 Absatz 1 Satz 1 Nummer 1, 2 oder 4 der Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nummer 351) geändert worden ist, genannten Personen oder eine diesen nach § 53a Absatz 1 Satz 1 der Strafprozessordnung gleichstehende Person das Zeugnis verweigern dürfte.

Treten die Voraussetzungen des Satzes 1 während der Anwendung nachrichtendienstlicher Mittel ein, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung von Leib und Leben oder Enttarnung eingesetzter Personen möglich ist und solange anzunehmen ist, dass diese Voraussetzungen vorliegen. Bestehen Zweifel, ob oder wie lange die Voraussetzungen des Satzes 1 vorliegen, darf ausschließlich eine automatische Aufzeichnung durchgeführt werden. In diesen Zweifelsfällen ist unverzüglich eine Entscheidung der Kommission nach § 10f über die Verwertbarkeit herbeizuführen. Soweit bei der Anwendung nachrichtendienstlicher Mittel Erkenntnisse im Sinne von Satz 1 gewonnen wurden, sind sie unverzüglich zu löschen. Eine Fortsetzung der Maßnahme in Fällen des Satzes 2 und die Löschung der Erkenntnisse nach Satz 5 sind zu dokumentieren.

(2) Erfolgen Maßnahmen bei anderen als den in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten zeugnisverweigerungsberechtigten Berufsgeheimnisträgern oder diesen nach § 53a Absatz 1 Satz 1 der Strafprozessordnung gleichstehenden Personen nicht zur Aufklärung von deren eigenen Bestrebungen oder Tätigkeiten, sind das öffentliche Interesse an den von diesen wahrgenommenen Aufgaben und das Interesse an der Geheimhaltung der ihnen anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken.“

10. Nach § 10a wird der folgende § 10b eingefügt:

**„§ 10b  
Vertrauensleute und verdeckte Bedienstete**

(1) Die Verfassungsschutzbehörde darf

1. Privatpersonen, deren planmäßige, dauerhafte Zusammenarbeit mit ihr Dritten nicht bekannt ist (Vertrauensleute), und
2. eigene Bedienstete unter einer ihnen verliehenen und auf Dauer angelegten Legende (verdeckte Bedienstete)

zur Aufklärung von Bestrebungen unter den Voraussetzungen des § 10 Absatz 2 und 3 einsetzen. Die Maßnahme setzt voraus, dass tatsächliche Anhaltspunkte für eine beobachtungsbedürftige Bestrebung und die Erforderlichkeit der Aufklärung vorliegen, wobei ein erhöhtes Eingriffsgewicht bei der Herstellung und Nutzung von Vertrauensbeziehungen einen erheblichen Beobachtungsbedarf und Aufklärungsgewinn erfordert.

(1a) Eine Maßnahme nach Absatz 1 darf sich gezielt nur gegen eine Person richten, von der aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie entweder

1. an der Bestrebung oder Tätigkeit beteiligt ist oder
2. mit einer Person nach Nummer 1 in Kontakt steht und
  - a) von der Bestrebung oder Tätigkeit Kenntnis hat oder die Person nach Nummer 1 sich ihrer zur Förderung der Bestrebung oder Tätigkeit bedient und
  - b) eine Maßnahme gegen die Person nach Nummer 1 allein nicht zur Erforschung des Sachverhalts ausreicht.

(2) Vertrauensleute und verdeckte Bedienstete dürfen weder zur Gründung von Bestrebungen nach § 5 Absatz 1 Nummer 1, 3 oder 4 noch zur steuernden Einflussnahme auf derartige Bestrebungen eingesetzt werden. Sie dürfen in solchen Personenzusammenschlüssen oder für solche Personenzusammenschlüsse, einschließlich strafbarer Vereinigungen, tätig werden, um deren Bestrebungen aufzuklären. Im Übrigen ist im Einsatz eine Beteiligung an Bestrebungen nur zulässig, wenn sie

1. nicht in Individualrechte eingreift,
2. von den an den Bestrebungen Beteiligten derart erwartet wird, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist, und
3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.

Sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass Vertrauensleute oder verdeckte Bedienstete rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht haben, soll der Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden. Über Ausnahmen nach Satz 4 entscheidet die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung.

(3) Über die Verpflichtung von Vertrauensleuten entscheidet die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung. Als Vertrauensleute dürfen Personen nicht angeworben und eingesetzt werden, die

1. nicht voll geschäftsfähig, insbesondere minderjährig sind,
2. von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden,
3. an einem Aussteigerprogramm teilnehmen,
4. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind,
5. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landtags oder eines Landesparlaments oder Beschäftigte eines solchen Mitglieds sind oder
6. berechtigt sind, in Strafsachen aus beruflichen Gründen das Zeugnis zu verweigern (§§ 53 und 53a der Strafprozessordnung), wenn sie zur Beschaffung von Informationen über Sachverhalte eingesetzt werden sollen, auf die sich ihr Zeugnisverweigerungsrecht bezieht; Informationen, die diese Personen unter Verletzung des § 203 des Strafgesetzbuches rechtswidrig an die Verfassungsschutzbehörde weiterzugeben beabsichtigen, dürfen von dieser nicht entgegengenommen werden.

Die Leitung der Verfassungsschutzabteilung kann eine Ausnahme von Nummer 4 zulassen, wenn die Verurteilung nicht als 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 Absatz 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 ausreichend gewichtig beigetragen hat. Auch im Weiteren ist die Qualität der gelieferten Informationen fortlaufend zu bewerten. Das für den Verfassungsschutz zuständige Ministerium trägt der Parlamentarischen Kontrollkommission mindestens einmal im Jahr einen Lagebericht zum Einsatz von Vertrauensleuten vor.

(4) Der Einsatz von Vertrauensleuten und verdeckten Bediensteten für eine Dauer von länger als sechs Monaten oder gegen Personen nach Absatz 1a Nummer 2 ist nur zulässig, wenn dieser zur Aufklärung erheblich beobachtungsbedürftiger Bestrebungen oder Tätigkeiten gemäß § 5 Absatz 1 in Verbindung mit § 6a Absatz 2 und 3 unerlässlich ist. Er unterliegt der unabhängigen Kontrolle nach § 10f. Der Einsatz ist auf höchstens zwölf Monate zu befristen. Verlängerungen um jeweils nicht mehr als zwölf Monate sind zulässig, soweit die Voraussetzungen der Maßnahme fortbestehen. Auch ein Einsatz, der nicht länger als sechs Monate dauert, ist nur zur Aufklärung von erheblich beobachtungsbedürftigen Bestrebungen zulässig, wenn er auf die Herstellung und Nutzung von Vertrauensbeziehungen angelegt ist.

(5) Zum Absehen von der Verfolgung von im Einsatz begangenen Vergehen oder der Rücknahme einer bereits erhobenen Klage und der Verfahrenseinstellung durch die Staatsanwaltschaft findet § 9a Absatz 3 des Bundesverfassungsschutzgesetzes Anwendung.“

11. Nach § 10b werden die folgenden §§ 10c bis 10f eingefügt:

**„§ 10c  
Observationen**

(1) Die Verfassungsschutzbehörde darf außerhalb des Schutzbereichs von Artikel 10 und 13 des Grundgesetzes verdeckt mit oder ohne Inanspruchnahme technischer Mittel planmäßig beobachten, sofern dies zur Aufklärung von Bestrebungen oder Tätigkeiten nach § 5 Absatz 1 im Einzelfall geboten ist. Eine Maßnahme darf sich gezielt nur gegen eine Person richten, von der aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie entweder

1. an der Bestrebung oder Tätigkeit beteiligt ist oder
2. mit einer beteiligten Person nach Nummer 1 in Kontakt steht und
  - a) von der Bestrebung oder Tätigkeit Kenntnis hat oder die Person nach Nummer 1 sich ihrer zur Förderung der Bestrebung oder Tätigkeit bedient und
  - b) eine Maßnahme gegen die beteiligte Person nach Nummer 1 allein nicht zur Erforschung des Sachverhalts ausreicht.

(2) Die Observation einer Person durchgehend länger als 48 Stunden oder mehr als vier Tage innerhalb einer Woche ist nur zulässig, soweit sie zur Beobachtung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit erforderlich ist. Die Maßnahme ist auf höchstens drei Monate zu befristen. Verlängerungen um jeweils nicht mehr als drei weitere Monate sind zulässig, soweit die Voraussetzungen der Maßnahme fortbestehen.

(3) Maßnahmen nach Absatz 2 unterfallen der unabhängigen Kontrolle nach § 10f.

(4) Maßnahmen nach den Absätzen 1 und 2 sind der betroffenen Person nach Maßgabe des § 11 mitzuteilen.

**§ 10d  
Verdecktes Mithören oder Aufzeichnen des nicht öffentlichen Wortes  
unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13  
des Grundgesetzes**

(1) Das verdeckte Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13 des Grundgesetzes durchgehend länger als 48 Stunden oder an mehr als vier Tagen innerhalb einer Woche ist nur zulässig, soweit es zur Beobachtung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit erforderlich ist. Werden die zeitlichen Grenzen des Satzes 1 nicht überschritten, muss eine erheblich beobachtungsbedürftige Bestrebung oder Tätigkeit ebenfalls vorliegen, wenn die Maßnahme aufgrund ihrer Eingriffstiefe mit einer Maßnahme nach Satz 1 gleichzustellen ist.

(2) Maßnahmen nach Absatz 1 unterfallen der unabhängigen Kontrolle nach § 10f.

(3) Maßnahmen nach Absatz 1 sind der betroffenen Person nach ihrer Einstellung gemäß § 11 mitzuteilen.

(4) Für die Verarbeitung der aus einer Maßnahme nach § 10 Absatz 1 Nummer 7 gewonnenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden, soweit in diesem Gesetz keine abweichenden Regelungen getroffen werden.

#### **§ 10e Verdeckte Standortermittlung und Ermittlung der Geräte- und Kartennummer mit technischen Mitteln**

(1) Der Einsatz von technischen Mitteln

1. zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder anderer Gegenstände und

2. zur Ermittlung der Geräte- und Kartennummern

ist außerhalb des Schutzbereiches von Artikel 10 Absatz 1 des Grundgesetzes zulässig, wenn die Ermittlung ansonsten aussichtslos oder wesentlich erschwert wäre. Für die Verarbeitung der Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden, soweit in diesem Gesetz keine abweichenden Regelungen getroffen werden.

(2) Technische Mittel nach Absatz 1 Nummer 1, die nicht lediglich im Zusammenhang mit anderen operativen Maßnahmen zu deren Ermöglichung eingesetzt werden, insbesondere für Zwecke von Observationsmaßnahmen nach § 10c zur Bestimmung von Standortdaten, sondern sich eignen, um anhand der Standortdaten die Bewegungen des Mobiltelefons oder eines anderen Gegenstandes nachzuverfolgen (Bewegungsprofil), dürfen wegen der damit verbundenen potenziell hohen Persönlichkeitsrelevanz nur eingesetzt werden, soweit dies zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit im Einzelfall geboten ist. Maßnahmen nach Satz 1 unterfallen der unabhängigen Kontrolle nach § 10f.

(3) Ein Bewegungsprofil im Sinne von Absatz 2 Satz 1 und das einhergehende erhöhte Eingriffsgewicht kann vorliegen, wenn die Standortermittlung erfolgt

1. durch punktuelle Maßnahmen über einen längeren Zeitraum,

2. in sehr enger zeitlicher Taktung über einen kürzeren Zeitraum oder

3. im engen Zeittakt über einen längeren Zeitraum.

Erfolgt eine punktuelle Standortfeststellung nur einmalig, liegt kein Bewegungsprofil vor, sodass keine erhebliche Beobachtungsbedürftigkeit als Voraussetzung für die Maßnahme erforderlich ist.

Von persönlichkeitsrelevanten Erkenntnissen eines Bewegungsprofils ist in der Regel auszugehen, wenn die Standortermittlung erfolgt

1. durchgehend länger als zwei Wochen,

2. durchgehend an 21 Tagen in einem Monat oder

3. länger als einen Monat.

(4) Maßnahmen nach Absatz 1 Nummer 1 und Absatz 2 dürfen sich nur gegen eine Person richten, von der aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass

1. sie an einer Bestrebung oder Tätigkeit nach § 5 Absatz 1 beteiligt ist oder

2. deren Anschluss durch die beteiligte Person nach Nummer 1 benutzt wird.



Personenbezogene Daten einer dritten Person dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zweckes nach Absatz 1 unvermeidbar ist. Sie unterliegen einem absoluten Verwendungsverbot und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

### **§ 10f Unabhängige Kontrolle**

(1) Die unabhängige Kontrolle im Sinne dieses Gesetzes wird von der G10-Kommission ausgeübt. Diese hat sich eigenverantwortlich ein Urteil darüber zu bilden, ob die Anordnungen gemäß § 10b Absatz 4, § 10c Absatz 2, § 10d Absatz 1 und § 10e Absatz 2 den gesetzlichen Voraussetzungen entsprechen, und entscheidet von Amts wegen über deren Zulässigkeit und Notwendigkeit. Anordnungen, die die G10-Kommission für unzulässig oder nicht notwendig hält, hat die Verfassungsschutzbehörde unverzüglich aufzuheben.

(2) Die Kontrolle von Maßnahmen, die der unabhängigen Kontrolle unterliegen, sind von der Leitung der Verfassungsschutzabteilung oder ihrer Stellvertretung zu beantragen. Der Antrag ist schriftlich zu stellen und hinreichend substantiiert zu begründen.

(3) Der Antrag hat alle beurteilungsrelevanten Tatsachen zu beinhalten. Es sind insbesondere Art, Umfang und Dauer der Maßnahme anzugeben sowie bei gezielt gegen bestimmte Personen gerichteten Maßnahmen die Personen, gegen die sich die Maßnahmen richtet. Soweit dies ohne Beeinträchtigung der Erfordernisse gemäß den Sätzen 1 und 2 möglich ist, sind Informationen, die nicht der alleinigen Verfügungsbefugnis der Verfassungsschutzbehörde unterliegen, nicht anzugeben. Gleiches gilt, wenn dies aus zwingenden Gründen des Nachrichtenzugangs, des Schutzes von Persönlichkeitsrechten oder der exekutiven Eigenverantwortung erforderlich ist.

(4) Zuständig für die Anordnungen ist die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung. Anordnungen sind auf höchstens ein Jahr zu befristen. Für Verlängerungen gelten die Sätze 1 und 2 sowie die Absätze 1 bis 3 entsprechend.

(5) § 2 Absatz 1 Satz 2 und 5 sowie Absatz 3 und 4 des Gesetzes zur Ausführung des Artikel 10-Gesetzes gelten entsprechend. Darüber hinaus findet das Gesetz zur Ausführung des Artikel 10-Gesetzes keine Anwendung.

(6) Die Kommissionsmitglieder und ihr Personal sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit im Rahmen der unabhängigen Kontrolle bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus der Kommission und nach der Beendigung der Tätigkeit des Personals. Das Personal ist konkret für diese Aufgabe zu bestimmen und einer erweiterten Sicherheitsüberprüfung gemäß § 10 des Sicherheitsüberprüfungsgesetzes zu unterziehen. Eine Vertretung außerhalb dieses Personenkreises ist nicht möglich. Näheres zu den Aufgaben und Befugnissen des Personals regelt die Geschäftsordnung der Kommission.“

## 12. § 11 wird wie folgt geändert:

- a) In Satz 1 wird die Angabe „Betroffenen Personen sind Maßnahmen nach § 10 Abs. 6 Satz 1 nach ihrer Beendigung mitzuteilen,“ durch die Angabe „Den Einsatz nachrichtendienstlicher Mittel teilt die Verfassungsschutzbehörde nach Beendigung den betroffenen Personen mit, soweit dies in diesem Gesetz bestimmt ist und“ ersetzt.
- b) In Satz 2 wird die Angabe „unterbleibt die Mitteilung so lange“ durch die Angabe „ist die Mitteilung so lange zurückzustellen“ ersetzt.
- c) Satz 3 wird durch die folgenden Sätze ersetzt:

„Für die Entscheidung nach Satz 2 ist die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung zuständig. Erfolgt die nach den Sätzen 2 und 3 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Zustimmung der Kommission gemäß § 10f. Diese Kommission bestimmt die Dauer der weiteren Zurückstellung. Einer Mitteilung bedarf es nicht, wenn die Kommission einstimmig festgestellt hat, dass

- 1. eine der Voraussetzungen in Satz 2 auch nach fünf Jahren nach Beendigung der Maßnahme noch vorliegt,
- 2. sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegt und
- 3. die Voraussetzungen für eine Löschung bei der erhebenden Stelle vorliegen.

Die Frist von fünf Jahren beginnt mit der Erhebung der personenbezogenen Daten. Wurden personenbezogene Daten übermittelt, erfolgt die Mitteilung im Benehmen mit der empfangenden Stelle.“

## 13. § 12 wird wie folgt geändert:

- a) In Absatz 1 Nummer 2 wird die Angabe „Abs.“ durch die Angabe „Absatz“ und die Angabe „Nr.“ durch die Angabe „Nummer“ ersetzt.
- b) In Absatz 3 Satz 3 wird die Angabe „sind diese Daten zu sperren“ durch die Angabe „ist die Verarbeitung dieser Daten einzuschränken“ ersetzt.

## 14. § 14 Absatz 2 wird durch die folgenden Absätze 2 und 3 ersetzt:

„(2) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist vor Erlass und Änderung der Dateianordnung anzuhören. Die Verfassungsschutzabteilung führt ein Verzeichnis der geltenden Dateianordnungen.

(3) Die Speicherung personenbezogener Daten ist auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit der Weiterführung der automatisierten Dateien durch die Verfassungsschutzbehörde zu überprüfen.“

15. § 16 wird durch den folgenden § 16 ersetzt:

**„§ 16  
Verarbeitung personenbezogener Daten von Minderjährigen**

(1) Personenbezogene Daten von Minderjährigen unter 14 Jahren dürfen unter den Voraussetzungen von § 15 in Verbindung mit § 9 nur verarbeitet werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie eine der in § 3 Absatz 1 des Artikel 10-Gesetzes genannten Straftaten planen, begehen oder begangen haben.

(2) Personenbezogene Daten über Minderjährige nach Absatz 1 sind jährlich auf die Erforderlichkeit der Verarbeitung zu überprüfen und spätestens nach zwei Jahren zu löschen, es sei denn, dass weitere Erkenntnisse nach § 5 Absatz 1 angefallen sind. Personenbezogene Daten über Minderjährige ab Vollendung des 14. Lebensjahres sind nach zwei Jahren auf die Erforderlichkeit der Verarbeitung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, dass nach Eintritt der Volljährigkeit weitere Erkenntnisse nach § 5 Absatz 1 angefallen sind.“

16. § 17 wird wie folgt geändert:

a) Die Überschrift wird durch die folgende Überschrift ersetzt:

**„§ 17  
Speichern, Berichtigen, Löschen und Verarbeitungseinschränkung personenbezogener Daten“.**

b) Die Absätze 3 bis 5 werden durch die folgenden Absätze 3 bis 5 ersetzt:

„(3) Personenbezogene Daten in Dateien sind zu löschen, wenn ihre Erhebung oder Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Bei jeder Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens aber nach fünf Jahren, sind die in Dateien gespeicherten personenbezogenen Daten auf ihre Erforderlichkeit zu überprüfen. Soweit die Daten Bestrebungen nach § 5 Absatz 1 Nummer 1 betreffen, sind sie spätestens zehn Jahre, soweit sie Bestrebungen nach § 5 Absatz 1 Nummer 3 oder 4 betreffen, spätestens 15 Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung trifft im Einzelfall ausnahmsweise eine andere Entscheidung.

(4) Die Verarbeitung personenbezogener Daten in Dateien ist einzuschränken, soweit durch ihre Löschung schutzwürdige Belange der betroffenen Person oder von Dritten beeinträchtigt würden. Ein schutzwürdiges Interesse liegt auch vor, wenn die betroffene Person einen Antrag nach § 26 Absatz 1 Satz 1 gestellt hat. Anstelle der Löschung tritt auch dann eine Verarbeitungseinschränkung, wenn die nach Absatz 3 zu löschenden Daten mit anderen Daten derart verbunden sind, dass sie nicht oder nur mit einem unverhältnismäßig großen Aufwand getrennt werden können. Die Daten, deren Verarbeitung eingeschränkt ist, dürfen ohne Einwilligung der betroffenen Person nicht mehr genutzt werden.

(5) Eine Akte ist zu vernichten, wenn sie insgesamt zur Aufgabenerfüllung der Verfassungsschutzbehörde nicht oder nicht mehr erforderlich ist. Die Erforderlichkeit ist bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren, zu prüfen. Eine Vernichtung unterbleibt, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden. Dies ist auch dann gegeben, wenn eine betroffene Person einen Antrag nach § 26 Absatz 1 Satz 1 gestellt hat. In diesen Fällen ist die Verarbeitung der in der Akte gespeicherten personenbezogenen Daten einzuschränken und mit einem entsprechenden Vermerk zu versehen. Sie dürfen nur für den Zweck der Wahrung schutzwürdiger Interessen des Betroffenen verwendet werden oder wenn es zur Abwehr einer erheblichen Gefahr unerlässlich ist. Eine Vernichtung der Akte erfolgt nicht, wenn sie nach den Vorschriften des Landesarchivgesetzes dem Landesarchiv zur Übernahme anzubieten und zu übergeben ist.“

17. Die §§ 20 bis 23 werden durch die folgenden §§ 20 bis 23 ersetzt:

**„§ 20  
Zweckbindung, Weiterverarbeitung**

(1) Die Verfassungsschutzbehörde darf personenbezogene Daten auch über den für die Datenerhebung maßgebenden Anlass hinaus zum Zweck der Aufgabenerfüllung des Verfassungsschutzes im Sinne des § 5 nutzen. Die Übermittlung personenbezogener Daten an eine andere Stelle stellt eine Nutzung für andere Zwecke dar und ist nur nach Maßgabe der §§ 20a bis 20e, § 20g, §§ 21 und 22 zulässig.

(2) Die empfangende Stelle prüft, ob die nach den §§ 20a bis 20e, § 20g, §§ 21 und 22 übermittelten personenbezogenen Daten für die Erfüllung ihrer Aufgaben erforderlich sind. Ergibt die Prüfung, dass die Daten nicht erforderlich sind, hat sie sie zu löschen. Die Löschung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unververtretbarem Aufwand möglich ist. Die empfangende Stelle darf diese weiteren Daten jedoch nicht nutzen.

(3) Die empfangende Stelle darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur verarbeiten

1. zu dem Zweck, zu dem sie ihr übermittelt wurden, oder
2. zu einem anderen Zweck, wenn sie ihr auch zu diesem Zweck übermittelt werden dürften unter der Voraussetzung, dass die Verfassungsschutzbehörde der Verarbeitung zu dem abgeänderten Zweck für den Einzelfall oder eine Reihe gleichgelagerter Fälle zustimmt.

Die Verfassungsschutzbehörde hat die empfangende Stelle auf den Zweck der Übermittlung und die Zweckbindung nach Satz 1 hinzuweisen. Dies gilt nicht für Übermittlungen im Rahmen verdeckter Ermittlungen. Die empfangende Stelle ist verpflichtet, der Verfassungsschutzbehörde auf deren Verlangen Auskunft über die weitere Verarbeitung zu geben.

(4) Hat die Übermittlung personenbezogener Daten in einem Verfahren zur vorbeugenden Personenüberprüfung nachteilige Folgen für die betroffene Person, so schließt das Auskunftsrecht der betroffenen Person auch das Recht auf Auskunft ein, dass die Folge durch eine Übermittlung der Verfassungsschutzbehörde veranlasst ist.

**§ 20a****Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr**

(1) Die Verfassungsschutzbehörde darf mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, soweit dies im Einzelfall aufgrund tatsächlicher Anhaltspunkte zur Abwehr einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist. Im Falle einer unmittelbar bevorstehenden Gefahr oder einer im Einzelfall bestehenden Gefahr, die von einer Bestrebung oder Tätigkeit nach § 5 Absatz 1 ausgeht, ist die Verfassungsschutzbehörde zur Übermittlung verpflichtet.

(2) Eine konkretisierte Gefahr nach Absatz 1 Satz 1 liegt vor, wenn sich der zum Schaden führende Kausalverlauf zwar noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits bestimmte Tatsachen im Einzelfall auf die Entstehung einer konkreten Gefahr für ein besonders gewichtiges Rechtsgut hinweisen.

(3) Besonders gewichtige Rechtsgüter nach Absatz 1 Satz 1 sind

1. die freiheitliche demokratische Grundordnung, einschließlich des Gedankens der Völkerverständigung und des friedlichen Zusammenlebens der Völker,
2. der Bestand und die Sicherheit des Bundes, der Länder sowie überstaatlicher und internationaler Organisationen, denen die Bundesrepublik Deutschland angehört,
3. sonstige Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, Sachen von bedeutendem Wert und bedeutende Vermögenswerte, deren Erhaltung im besonderen öffentlichen Interesse geboten ist,
4. das Leben sowie bei einer erheblichen Gefährdung im Einzelfall die körperliche Integrität und die Freiheit einer Person.

**§ 20b****Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz**

(1) Die Verfassungsschutzbehörde darf mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz der in § 20a Absatz 3 genannten Rechtsgüter erforderlich ist zur

1. Überprüfung der Verfassungstreue von Bewerbenden und Beschäftigten des öffentlichen Dienstes,
2. Vorbereitung oder Durchführung einer Maßnahme nach dem Vereinsgesetz,
3. Vorbereitung oder Stellung eines Antrags nach Artikel 18 Satz 2 des Grundgesetzes,
4. Vorbereitung oder Stellung eines Antrags nach Artikel 21 Absatz 4 des Grundgesetzes,
5. Durchführung von Personenüberprüfungen,
  - a) die gesetzlich vorgesehen sind, insbesondere nach dem Waffenrecht, Jagdrecht, Sprengstoffrecht, Atomrecht, Luftsicherheitsrecht, Außenwirtschaftsrecht, Sicherheitsgewerberecht, Aufenthaltsrecht oder Staatsangehörigkeitsrecht oder den Sicherheitsüberprüfungsgesetzen,
  - b) die gesetzliche Aufgaben des Objekt- oder Personenschutzes betreffen,
6. Vorbereitung oder Durchführung der Aufhebung eines begünstigenden Verwaltungsakts, der aufgrund einer Überprüfung im Sinne von Nummer 5 erlassen wurde,

7. Wahrnehmung von gesetzlichen Befugnissen der empfangenden Stelle beim aufsichtlichen Schutz vor missbräuchlicher Nutzung von Einrichtungen und Dienstleistungen der Unternehmen im Finanzsektor in Bezug auf Terrorismusfinanzierung,
8. Vorbereitung oder Durchführung der Strafvollstreckung, einschließlich der Vollzugsplanung, gegen die unmittelbar betroffene Person oder zur Gewährleistung der Sicherheit des Vollzugs freiheitsentziehender Maßnahmen gegen Gefährdungen durch diese Person,
9. Durchsetzung von im Bereich der Gemeinsamen Außen- und Sicherheitspolitik der Europäischen Union beschlossenen wirtschaftlichen Sanktionsmaßnahmen.

(2) Die Verfassungsschutzbehörde darf personenbezogene Daten, die sie mit nachrichtendienstlichen Mitteln erhoben hat, an eine inländische öffentliche Stelle zur Vorbereitung, Durchführung oder Überprüfung einer begünstigenden Maßnahme übermitteln, wenn dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz der in § 20a Absatz 3 genannten Rechtsgüter erforderlich ist.

### **§ 20c**

#### **Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung**

(1) Die Verfassungsschutzbehörde darf mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an eine zuständige inländische Strafverfolgungsbehörde übermitteln, wenn bestimmte Tatsachen den Verdacht einer besonders schweren Straftat begründen und soweit die Daten zur Verfolgung dieser Straftat erforderlich sind.

(2) Eine besonders schwere Straftat im Sinne des Absatzes 1 ist eine Straftat, die

1. in § 100b Absatz 2 der Strafprozessordnung aufgeführt ist,
2. im Höchstmaß mit Freiheitsstrafe von mehr als fünf Jahren bedroht ist, oder
3. im Höchstmaß mit Freiheitsstrafe von mindestens fünf Jahren bedroht ist, wenn der Straftatbestand dem Schutz eines der in § 20a Absatz 3 genannten Rechtsgüter dient und die Straftat aufgrund der tatbestandlich umschriebenen Begehungsformen und Tatfolgen besonders schwer wiegt.

Maßgeblich ist die Strafdrohung des gesetzlichen Tatbestands im Zeitpunkt der Übermittlung. Dasselbe gilt für Regelbeispiele für besonders schwere oder minder schwere Fälle, sofern bestimmte Tatsachen den Verdacht begründen, dass das Regelbeispiel erfüllt ist.

**§ 20d****Übermittlung an inländische öffentliche Stellen ohne belastende Maßnahmen mit Außenwirkung**

(1) Die Verfassungsschutzbehörde darf mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, wenn dies aufgrund tatsächlicher Anhaltspunkte zur eigenen Aufklärung einer beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 5 Absatz 1, insbesondere zur Vorbereitung oder Konkretisierung eines Auskunftsersuchens, erforderlich ist. Darf die Verfassungsschutzbehörde eine Maßnahme nach § 10 sowie den §§ 10a bis 10e, §§ 24a und 24b nur zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit einsetzen, so darf sie die durch den Einsatz dieses Mittels erhobenen personenbezogenen Daten nach Satz 1 nur zur Aufklärung einer ebenso beobachtungsbedürftigen Bestrebung oder Tätigkeit übermitteln.

(2) Die Verfassungsschutzbehörde darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz der Rechtsgüter nach § 20a Absatz 3 vor Bestrebungen oder Tätigkeiten nach § 5 Absatz 1 für Aufgaben erforderlich ist, die die empfangende Stelle ohne unmittelbar außenwirksame Maßnahmen zulasten der betroffenen Person wahrnimmt. Dies gilt insbesondere für die

1. Erforschung und Bewertung dieser Bedrohungen,
2. Verbesserung der Fachkompetenz und Organisation bei der Erforschung dieser Bedrohungen.

Liegen die Voraussetzungen nach den §§ 20a und 20b nicht vor, darf die empfangende Stelle die übermittelten Daten nicht für Maßnahmen nutzen, die die betroffene Person mit unmittelbarer Außenwirkung belasten.

**§ 20e****Übermittlung an inländische nicht öffentliche Stellen**

Eine Übermittlung personenbezogener Daten an inländische nicht öffentliche Stellen ist unzulässig, es sei denn, es bestehen im Einzelfall tatsächliche Anhaltspunkte, dass dies zum Schutz der Rechtsgüter nach § 20a Absatz 3 erforderlich ist zur

1. eigenen Aufklärung einer beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 5 Absatz 1, insbesondere zur Vorbereitung oder Konkretisierung eines Auskunftsersuchens,
2. Abwendung einer zumindest konkretisierten Gefahr für ein Rechtsgut nach § 20a Absatz 3 oder
3. Erreichung eines der folgenden Zwecke:
  - a) Schutz lebenswichtiger und verteidigungsrelevanter Einrichtungen und kritischer Infrastrukturen,
  - b) Schutz der Sicherheit in der Informationstechnik gegen erhebliche Gefährdungen,
  - c) Schutz rechtlich gewährleisteter Geheimnisse,
  - d) wissenschaftliche Erforschung und Bewertung von Bestrebungen und Tätigkeiten nach § 5 Absatz 1,

- e) Schutz konkreter Präventions-, Ausstiegs- oder Deradikalisierungsprojekte, die finanziell oder organisatorisch mit öffentlichen Stellen kooperieren,
- f) Schutz des Kindeswohls bei der Erbringung von Leistungen und Erfüllung der Aufgaben der Kinder- und Jugendhilfe,
- g) Schutz der gesetzlichen Erziehungs- und Bildungsziele der Schulen und der Einrichtungen der Kindertagesbetreuung,
- h) Schutz der zweckgemäßen Verwendung öffentlicher Fördermittel oder sonstiger öffentlicher Vorteilszuwendungen.

Eine nicht öffentliche Stelle, die personenbezogene Daten nach Satz 1 Nummer 3 erhalten hat, darf die Daten für Handlungen, die für die betroffene Person eine nachteilige rechtliche Wirkung entfalten oder diese Person in anderer Weise erheblich beeinträchtigen, nur verwenden, wenn dies zur Abwendung einer zumindest konkretisierten Gefahr für ein Rechtsgut nach § 20a Absatz 3 erforderlich ist und die Verfassungsschutzbehörde zustimmt. Bei einer unmittelbar bevorstehenden Gefahr ist die vorherige Zustimmung der Verfassungsschutzbehörde entbehrlich. Die nicht öffentliche Stelle hat die Verfassungsschutzbehörde unverzüglich über ihre Handlungen und deren Anlass zu unterrichten. In den Fällen des Satzes 2 ist die Übermittlung der betroffenen Person durch den Verfassungsschutz nach Maßgabe des § 11 mitzuteilen.

#### **§ 20f**

##### **Projektbezogene gemeinsame Dateien**

(1) Die Verfassungsschutzbehörde kann für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit dem Bundesamt für Verfassungsschutz, den übrigen Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Zollkriminalamt sowie den Polizeibehörden des Bundes und der Länder eine gemeinsame Datei errichten. Die projektbezogene Zusammenarbeit soll nach Maßgabe der Aufgaben und Befugnisse der in Satz 1 genannten Behörden den Austausch und die gemeinsame Auswertung von Erkenntnissen zu Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 5 Absatz 1 Satz 1 Nummer 1 bis 4 genannten Schutzgüter gerichtet sind, bewirken. Personenbezogene Daten zu Bestrebungen nach Satz 2 dürfen unter Einsatz der gemeinsamen Datei durch die an der projektbezogenen Zusammenarbeit beteiligten Behörden im Rahmen ihrer Befugnisse verwendet werden, soweit dies in diesem Zusammenhang zur Erfüllung ihrer Aufgaben erforderlich ist. Bei der weiteren Verwendung der personenbezogenen Daten finden für die beteiligten Behörden die jeweils für sie geltenden Vorschriften über die Verwendung von Daten Anwendung.

(2) § 22b Absatz 2 bis 6 des Bundesverfassungsschutzgesetzes findet entsprechende Anwendung.



### **§ 20g**

#### **Minderjährigenschutz bei Inlandsübermittlung**

Die Verfassungsschutzbehörde darf personenbezogene Daten, die sich auf das Verhalten minderjähriger Personen beziehen, vorbehaltlich der Sätze 2 und 3 nicht übermitteln. Sie darf die personenbezogenen Daten nur übermitteln, wenn eine Weiterverarbeitung für die Vorbereitung oder Durchführung belastender Maßnahmen mit unmittelbarer Außenwirkung für die betroffene Person ausgeschlossen ist, bei einer Übermittlung nach § 20e Satz 1 Nummer 3 beschränkt auf dessen Buchstaben e bis g. Im Übrigen darf sie personenbezogene Daten nur übermitteln in Bezug auf eine minderjährige Person, die

1. mindestens 14 Jahre alt ist,
  - a) zur Abwehr einer Gefahr nach § 20a Absatz 1 Satz 1,
  - b) zum administrativen Rechtsgüterschutz nach § 20b Absatz 1 Nummer 1 und 8 oder
  - c) zur Verfolgung einer besonders schweren Straftat nach § 20c,
2. noch nicht 14 Jahre alt ist, wenn nach den Umständen des Einzelfalls tatsächliche Anhaltspunkte dafür bestehen, dass von der minderjährigen Person eine Gefahr ausgeht für
  - a) Leib oder Leben einer anderen Person oder
  - b) Einrichtungen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages.

### **§ 21**

#### **Informationsübermittlung an ausländische Stellen**

(1) Für die Übermittlung personenbezogener Daten an ausländische öffentliche und nicht öffentliche Stellen sowie an über- und zwischenstaatliche Stellen gelten die §§ 20a bis 20e entsprechend.

- (2) Die Übermittlung unterbleibt, wenn im Einzelfall
1. auswärtige Belange der Bundesrepublik Deutschland entgegenstehen oder
  2. überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen, insbesondere, wenn hierdurch Leib, Leben oder Freiheit einer Person oder sonstige elementare Menschenrechte gefährdet würden oder Verletzungen von elementaren rechtsstaatlichen Grundsätzen drohen oder
  3. ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrer Umgang mit den Daten bei der empfangenden Stelle nicht hinreichend gesichert ist.

Bei der Prüfung, ob eine Übermittlung zu unterbleiben hat, berücksichtigt die Verfassungsschutzbehörde insbesondere den bisherigen Umgang der empfangenden Stelle mit übermittelten Daten.

(3) Die empfangende Stelle ist darauf hinzuweisen, dass die Daten nur mit Zustimmung der Verfassungsschutzbehörde an Dritte übermittelt werden dürfen und die Verfassungsschutzbehörde sich eine Auskunft über die Weiterverarbeitung der Daten vorbehält.

(4) Die Verfassungsschutzbehörde darf personenbezogene Daten, die sich auf das Verhalten minderjähriger Personen beziehen, vorbehaltlich der Sätze 2 bis 4 nicht übermitteln. Personenbezogene Daten einer minderjährigen Person, die mindestens 16 Jahre alt ist, darf die Verfassungsschutzbehörde nur unter den Voraussetzungen des § 20g Absatz 1 Satz 3 Nummer 1 Buchstabe a und c übermitteln, bei einer Übermittlung zur Strafverfolgung jedoch nur bei dringendem Tatverdacht. Personenbezogene Daten einer minderjährigen Person, die noch nicht 16 Jahre alt ist, darf sie nur übermitteln, wenn nach den Umständen des Einzelfalls tatsächliche Anhaltspunkte dafür bestehen, dass von der minderjährigen Person eine Gefahr ausgeht für

1. Leib oder Leben einer anderen Person oder
2. Einrichtungen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages.

Bei einer Übermittlung an einen Staat, der unmittelbar an die Bundesrepublik Deutschland angrenzt oder Mitgliedstaat der Europäischen Union oder des Nordatlantikvertrages ist, ist § 20g entsprechend anzuwenden.

(5) Die Verfassungsschutzbehörde darf personenbezogene Daten an eine nicht öffentliche Stelle im Ausland übermitteln, wenn dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Abwehr einer dringenden Gefahr für ein Rechtsgut nach § 20a Absatz 3 Nummer 4 unerlässlich ist und überwiegende schutzwürdige Interessen der betroffenen Person nach § 25 Absatz 1 Satz 1 Nummer 3 nicht entgegenstehen.

## **§ 22**

### **Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen und Übermittlung zum Schutz der Betroffenen**

(1) Die Verfassungsschutzbehörde darf personenbezogene Daten, die sie aus allgemein zugänglichen Quellen erhoben hat, einer anderen Stelle übermitteln, wenn dies erforderlich ist

1. zur Erfüllung ihrer Aufgaben oder
2. zur Erfüllung der Aufgaben der empfangenden Stelle.

Eine automatisierte Übermittlung ist zulässig.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die aus allgemein zugänglichen Quellen systematisch erhoben oder zusammengeführt wurden. Die Übermittlung richtet sich in diesen Fällen nach den §§ 20a bis 21 und § 23.

(3) Die Verfassungsschutzbehörde darf personenbezogene Daten zum Schutz der Betroffenen auch übermitteln, wenn offensichtlich ist, dass die Übermittlung im Interesse der betroffenen Person liegt, deren Einwilligung nicht oder nicht rechtzeitig eingeholt werden kann und kein Grund zu der Annahme besteht, dass sie in Kenntnis der Übermittlung ihre Einwilligung verweigern würde. Sie darf personenbezogene Daten insbesondere für Zwecke der Jugendhilfe übermitteln.

**§ 23****Protokollierung der Übermittlungen und weitere Verfahrensregelungen**

(1) Die Verfassungsschutzbehörde protokolliert die empfangende Stelle, die Rechtsgrundlage sowie den Zeitpunkt der Übermittlung. Sie darf Protokolldaten, die ausschließlich zu Zwecken der Datenschutzkontrolle gespeichert werden, nur für diesen Zweck verarbeiten. Die Protokolldaten sind bis zum Ablauf des zweiten Kalenderjahres, das auf das Kalenderjahr der Protokollierung folgt, aufzubewahren und nach Ablauf dieser Aufbewahrungsfrist unverzüglich zu löschen.

(2) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten der betroffenen Person oder einer dritten Person so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnigte Interessen der betroffenen Person oder einer dritten Person an der Geheimhaltung offensichtlich überwiegen. Die empfangende Stelle darf diese Daten nicht nutzen.

(3) Eine Übermittlung an nicht öffentliche Stellen bedarf der Zustimmung der Leitung der Verfassungsschutzabteilung. Für Übermittlungen an inländische nicht öffentliche Stellen kann die Zustimmung auch allgemein für gleichgelagerte Fälle erfolgen. Die Übermittlung ist der betroffenen Person durch die Verfassungsschutzbehörde nach Maßgabe des entsprechend anzuwendenden § 11 mitzuteilen.“

18. § 24 wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird nach der Angabe „Übermittlung von Daten“ die Angabe „und die Vorlage von Unterlagen“ eingefügt.

b) Absatz 3 wird durch den folgenden Absatz 3 ersetzt:

„(3) Die in Absatz 1 genannten Stellen übermitteln von sich aus der Verfassungsschutzbehörde alle ihnen im Rahmen ihrer Aufgaben vorliegenden Daten und Unterlagen über Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen verfolgt werden, und über geheimdienstliche Tätigkeiten. Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizei übermitteln darüber hinaus auch andere ihnen im Rahmen ihrer Aufgabenerfüllung bekannt gewordene Daten und Unterlagen über Bestrebungen im Sinne des § 5 Absatz 1. Die Übermittlung personenbezogener Daten, die aufgrund einer Maßnahme nach § 100a der Strafprozessordnung bekannt geworden sind, ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass jemand eine der im aufgrund von Artikel 10 Absatz 2 Satz 1 des Grundgesetzes erlassenen Bundesgesetz als Voraussetzung für eine Beschränkungsmaßnahme genannten Straftaten plant, begeht oder begangen hat. Auf die nach Satz 3 übermittelten Daten und die dazugehörigen Unterlagen finden die im aufgrund von Artikel 10 Absatz 2 Satz 1 des Grundgesetzes erlassenen Bundesgesetz enthaltenen Bestimmungen über die Nutzung, Übermittlung und Vernichtung von Daten entsprechende Anwendung.“

c) In Absatz 5 Satz 3 wird die Angabe „sind die Daten gesperrt und entsprechend zu kennzeichnen“ durch die Angabe „ist die Verarbeitung einzuschränken und eine entsprechende Kennzeichnung vorzunehmen“ ersetzt.

19. § 24a wird durch den folgenden § 24a ersetzt:

**„§ 24a  
Informationsübermittlung durch nicht öffentliche Stellen  
an die Verfassungsschutzbehörde, Ersuchen an das Bundeszentralamt für Steuern**

- (1) Die Verfassungsschutzbehörde darf im Einzelfall Auskunft einholen bei
1. Luftfahrtunternehmen zu Namen und Anschriften des Kunden sowie zur Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg,
  2. Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge,
  3. denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder daran mitwirken, zu den Umständen des Postverkehrs,
  4. denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu Verkehrsdaten nach § 9 Absatz 1 Satz 1 Nummer 1 bis 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten und
  5. denjenigen, die geschäftsmäßig Telemediendienste erbringen oder daran mitwirken, zu
    - a) Merkmalen zur Identifikation des Nutzers eines Telemediums,
    - b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und
    - c) Angaben über die vom Nutzer in Anspruch genommenen Telemediendienste, soweit Tatsachen die Annahme rechtfertigen, dass dies zur Aufklärung von erheblich beobachtungsbedürftigen Bestrebungen oder Tätigkeiten erforderlich ist.
- (2) Die Verfassungsschutzbehörde darf beim Bundeszentralamt für Steuern Auskünfte nach § 93b Absatz 1 der Abgabenordnung einholen, wenn dies zur Aufklärung von erheblich beobachtungsbedürftigen Bestrebungen und Tätigkeiten nach § 5 Absatz 1 im Einzelfall erforderlich ist. § 3 Absatz 2 Satz 2 des Artikel 10-Gesetzes gilt entsprechend mit der Maßgabe, dass die Auskunft auch über Personen eingeholt werden kann, die die Leistung für die verdächtige Person in Anspruch nehmen.
- (3) Anordnungen nach den Absätzen 1 und 2 dürfen sich nur gegen Personen richten, bei denen
1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie erheblich beobachtungsbedürftige Bestrebungen und Tätigkeiten nach Absatz 1 nachdrücklich fördern, oder
  2. aufgrund bestimmter Tatsachen anzunehmen ist
    - a) bei Auskünften nach Absatz 1 Satz 1 Nummer 1, 2 und 5, dass sie die Leistung für eine Person nach Nummer 1 in Anspruch nehmen, oder
    - b) bei Auskünften nach Absatz 1 Satz 1 Nummer 3 und 4, dass sie für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben, oder im Falle des Absatzes 1 Satz 1 Nummer 4, dass eine Person nach Nummer 1 ihren Anschluss benutzt.

(4) Die Zuständigkeit für Anordnungen nach Absatz 1 Satz 1 Nummer 1 ist in einer Dienstvorschrift zu regeln, die der Zustimmung der für den Verfassungsschutz zuständigen Ministerin oder des für den Verfassungsschutz zuständigen Ministers bedarf. Anordnungen nach Absatz 1 Satz 1 Nummer 2 bis 5 werden von der Leitung der Verfassungsschutzabteilung oder ihrer Stellvertretung schriftlich beantragt und begründet. Im Falle der Auskunft nach Absatz 1 Satz 1 Nummer 2 kann der Antrag auch von einer oder einem Bediensteten der Verfassungsschutzbehörde gestellt werden, die oder der die Befähigung zum Richteramt hat. Zuständig für Anordnungen nach Absatz 1 Satz 1 Nummer 2 bis 5 ist die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister. Die Anordnung einer Auskunft über künftig anfallende Daten ist auf höchstens drei Monate zu befristen. Die Verlängerung dieser Anordnung um jeweils nicht mehr als drei Monate ist auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Anordnungen nach Absatz 1 Satz 1 Nummer 1 und 2 hat die Verfassungsschutzbehörde der betroffenen Person mitzuteilen, sobald eine Gefährdung des Zweckes des Eingriffs ausgeschlossen werden kann.

(5) Über Anordnungen nach Absatz 1 Satz 1 Nummer 3 bis 5 unterrichtet die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister monatlich die Kommission nach § 2 Absatz 1 des Gesetzes zur Ausführung des Artikel 10-Gesetzes vom 17. Juli 1992 (GVOBl. M-V S. 486), das zuletzt durch das Gesetz vom 30. Juli 2007 (GVOBl. M-V S. 278) geändert worden ist, vor deren Vollzug. Bei Gefahr im Verzug kann er den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen. Die Kommission prüft von Amts wegen oder aufgrund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 15 Absatz 5 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 4 des Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts vom 22. Dezember 2023 (BGBl. 2023 I Nummer 413) geändert worden ist, ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Verarbeitung der nach Absatz 1 Satz 1 Nummer 3 bis 5 erlangten personenbezogenen Daten erstreckt. Entscheidungen über Auskünfte, die die Kommission für unzulässig oder nicht notwendig erklärt, hat die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister unverzüglich aufzuheben. Die Daten unterliegen in diesem Falle einem absoluten Verwendungsverbot und sind unverzüglich zu löschen. Für die Verarbeitung der nach Absatz 1 Satz 1 Nummer 3 bis 5 erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden. § 12 Absatz 1 und 3 des Artikel 10-Gesetzes findet entsprechend Anwendung.

(6) Die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister unterrichtet im Abstand von höchstens sechs Monaten die Parlamentarische Kontrollkommission über Anordnungen nach Absatz 1; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben.

(7) Anordnungen sind der verpflichteten Person insoweit schriftlich mitzuteilen, als dies erforderlich ist, um ihr die Erfüllung ihrer Verpflichtung zu ermöglichen. Anordnungen und übermittelte Daten dürfen Betroffenen oder Dritten von der verpflichteten Person nicht mitgeteilt werden.

(8) Die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister unterrichtet das Parlamentarische Kontrollgremium des Bundes jährlich über Anordnungen nach Absatz 1 nach Maßgabe des § 8b Absatz 3 Satz 1 des Bundesverfassungsschutzgesetzes.

(9) Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des Absatzes 1 Satz 1 Nummer 3 bis 5 und der Absätze 2 bis 4 eingeschränkt.“

20. § 24b wird wie folgt geändert:

- a) In Absatz 1 Nummer 2 wird die Angabe „Telekommunikation-Telemedien-Datenschutz-Gesetzes“ durch die Angabe „Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ ersetzt.
- b) In Absatz 3 Satz 2 wird die Angabe „§ 24a Absatz 3 Satz 2 und 4 sowie Absatz 4“ durch die Angabe „§ 24a Absatz 4 Satz 2 und 4 sowie Absatz 5“ ersetzt.

21. § 25 wird wie folgt geändert:

- a) Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) Die Übermittlung von personenbezogenen Daten nach den §§ 20a bis 20e, § 20g, §§ 21 und 22 unterbleibt, wenn

- 1. besondere gesetzliche Verarbeitungsregelungen entgegenstehen,
- 2. die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen unter Berücksichtigung
  - a) der Art der Information,
  - b) der Wertigkeit der Information, auch unter Berücksichtigung des vergangenen Zeitraums und des Alters der betroffenen Person, insbesondere bei Minderjährigen,
  - c) der Art der Erhebung der Information, insbesondere in den Fällen des § 10 Absatz 1,
  - d) drohender, insbesondere verdachtsbegründeter Anschlussmaßnahmen,
  - e) der Verfügbarkeit vorherigen Rechtsschutzes gegen drohende Folgemaßnahmen,
- 3. durch die Übermittlung der personenbezogenen Daten eine dringende Gefahr für ein Rechtsgut nach § 20a Absatz 3 Nummer 4 zu besorgen ist; dies gilt nicht, wenn die Übermittlung dem Schutz solcher Rechtsgüter dient und dieses Schutzinteresse überwiegt, oder
- 4. sonstige überwiegende Sicherheitsinteressen der Übermittlung entgegenstehen; dies ist nicht der Fall, wenn die Übermittlung unerlässlich ist zur
  - a) Abwehr einer gegenwärtigen Gefahr für die Rechtsgüter nach § 20a Absatz 3,
  - b) Verfolgung einer auch im Einzelfall besonders schwerwiegenden Straftat, die im Höchstmaß mit einer Freiheitsstrafe von mindestens zehn Jahren bedroht ist.

Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten bleibt unberührt.“

b) Absatz 2 wird wie folgt geändert:

- aa) In Satz 1 wird die Angabe „den Empfänger“ durch die Angabe „die empfangende Stelle“ ersetzt.
- bb) In Satz 2 wird die Angabe „dem Empfänger“ durch die Angabe „der empfangenden Stelle“ ersetzt.

22. § 26 wird wie folgt geändert:

- a) In Absatz 1 Satz 2 wird die Angabe „die Empfänger“ durch die Angabe „die empfangenden Stellen“ ersetzt.
- b) Absatz 2 Satz 2 wird durch den folgenden Satz ersetzt:

„Die Entscheidung treffen die Leitung der Verfassungsschutzabteilung oder von dieser besonders beauftragte Bedienstete, die die Befähigung zum Richteramt besitzen sollen.“

- c) Absatz 4 wird durch den folgenden Absatz 4 ersetzt:

„(4) Wird die Auskunftserteilung abgelehnt, ist der antragstellenden Person die Rechtsgrundlage dieser Ablehnung mitzuteilen. Sie ist auf ihr Recht hinzuweisen, sich an die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden zu können. Der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit ist auf Verlangen Auskunft zu erteilen. Stellt die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister oder im Verhinderungsfall die Staatssekretärin oder der Staatssekretär im Einzelfall fest, dass durch die Erteilung der Auskunft die Sicherheit des Bundes oder eines Landes gefährdet würde, so darf die Auskunft nur der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit persönlich erteilt werden. Mitteilungen der oder des Landesbeauftragten für den Datenschutz und Informationsfreiheit an die antragstellende Person dürfen keine Rückschlüsse auf den Kenntnisstand der Verfassungsschutzbehörde zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.“

23. In § 27 Absatz 1 Satz 2 wird jeweils die Angabe „Abs.“ durch die Angabe „Absatz“ ersetzt.

24. § 28 wird durch den folgenden § 28 ersetzt:

**„§ 28  
Geheimhaltung**

(1) Die Parlamentarische Kontrollkommission tagt in öffentlicher oder nicht öffentlicher Sitzung, über die jeweils ein Protokoll anzufertigen ist. Die Mitglieder und ihre Beschäftigten sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit in der Parlamentarischen Kontrollkommission bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus der Parlamentarischen Kontrollkommission und nach der Beendigung der Tätigkeit der Beschäftigten. Die Beschäftigten der Kommissionsmitglieder sind konkret für diese Aufgabe zu bestimmen und einer erweiterten Sicherheitsüberprüfung gemäß § 10 des Sicherheitsüberprüfungsgesetzes zu unterziehen. Eine Vertretung außerhalb dieses Personenkreises ist nicht möglich. Näheres zu den Aufgaben und Befugnissen der Beschäftigten der Kommissionsmitglieder regelt die Geschäftsordnung der Kommission.

(2) Auf Antrag eines Mitglieds beschließt die Parlamentarische Kontrollkommission über die Herstellung der Öffentlichkeit oder die Aufhebung der Vertraulichkeit nach Absatz 1, soweit öffentliche Geheimschutzinteressen, insbesondere die Aufrechterhaltung des Nachrichtenzugangs, oder berechnigte Interessen eines Einzelnen dem nicht entgegenstehen. Der Beschluss bedarf der Mehrheit der gesetzlichen Mitglieder der Kommission. Die für den Verfassungsschutz zuständige Ministerin oder der für den Verfassungsschutz zuständige Minister, im Verhinderungsfalle die Staatssekretärin oder der Staatssekretär, kann einem Beschluss nach Satz 1 widersprechen, wenn die Voraussetzungen der Aufhebung der Vertraulichkeit gemäß Satz 1 nicht vorliegen. Die für den Verfassungsschutz zuständige Ministerin oder der Minister, im Falle seiner Verhinderung die Staatssekretärin oder der Staatssekretär, hat die Gründe hierfür darzulegen. Die Aufhebung der Vertraulichkeit von Beratungsgegenständen, die in die Verantwortlichkeit des Bundes oder eines Landes fallen, ist nur mit deren Zustimmung möglich.

(3) Sitzungsunterlagen und Protokolle verbleiben im Gewahrsam der Verfassungsschutzbehörde und können nur dort von den Mitgliedern der Kommission, ihren Beschäftigten oder der für den Verfassungsschutz zuständigen Ministerin oder dem für den Verfassungsschutz zuständigen Minister, im Verhinderungsfalle durch die Staatssekretärin oder den Staatssekretär, eingesehen werden, es sei denn, der ordnungsgemäße Umgang mit diesen Unterlagen gemäß der Verschlussanweisung für das Land Mecklenburg-Vorpommern ist nach Überzeugung der Parlamentarischen Kontrollkommission auf andere Weise gewährleistet.“

25. § 29 wird wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Angabe „Ministerium für Inneres, Bau und Digitalisierung“ durch die Angabe „für den Verfassungsschutz zuständige Ministerium“ und die Angabe „§ 20 Abs. 4 Satz 3“ durch die Angabe „§ 20 Absatz 5 Satz 3“ ersetzt.



b) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Die Parlamentarische Kontrollkommission kann von dem für den Verfassungsschutz zuständigen Ministerium alle für ihre Kontrollaufgaben erforderlichen Auskünfte, Unterlagen, Akten- und Dateneinsicht, Stellungnahmen und den Zutritt zur Verfassungsschutzbehörde verlangen sowie bei besonderem Aufklärungsbedarf Bedienstete und Auskunftspersonen zum Sachverhalt befragen, sofern dem nicht überwiegende öffentliche (zum Beispiel Aufrechterhaltung des Nachrichtenzugangs) oder private Belange entgegenstehen; das für den Verfassungsschutz zuständige Ministerium hat dies vor der Parlamentarischen Kontrollkommission zu begründen. Die Parlamentarische Kontrollkommission kann ferner die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit beauftragen, die Rechtmäßigkeit einzelner Maßnahmen, welche die Verfassungsschutzbehörde durchgeführt hat, zu überprüfen und der Kommission das Ergebnis der Überprüfung mitzuteilen. Die Befugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit richten sich nach den §§ 30 und 31. Wird die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit nach § 26 Absatz 4 tätig, so kann sie oder er von sich aus die Parlamentarische Kontrollkommission unterrichten, wenn sich Beanstandungen ergeben, eine Mitteilung an die betroffene Person aber aus Geheimhaltungsgründen unterbleiben muss.“

c) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 werden die Angabe „Ministeriums für Inneres, Bau und Digitalisierung“ durch die Angabe „für den Verfassungsschutz zuständigen Ministeriums“ und die Angabe „einen Sachverständigen“ durch die Angabe „eine Sachverständige oder einen Sachverständigen“ ersetzt.

bb) In Satz 2 wird die Angabe „Der Sachverständige“ durch die Angabe „Die oder der Sachverständige“ ersetzt.

d) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 wird die Angabe „Abteilung“ durch die Angabe „Verfassungsschutzabteilung“ ersetzt.

bb) In Satz 2 wird die Angabe „Ministerium für Inneres, Bau und Digitalisierung“ durch die Angabe „für den Verfassungsschutz zuständige Ministerium“ ersetzt.

26. Nach § 29 wird der folgende § 29a eingefügt:

#### **„§ 29a Eingaben**

(1) Bedienstete der Verfassungsschutzabteilung dürfen sich in dienstlichen Angelegenheiten ohne Einhaltung des Dienstweges unmittelbar an die Parlamentarische Kontrollkommission wenden. Diese übermittelt die Eingaben der für den Verfassungsschutz zuständigen Ministerin oder dem für den Verfassungsschutz zuständigen Minister zur Stellungnahme. Die oder der Bedienstete wird namentlich nur bekannt gegeben, soweit in die Bekanntgabe zu diesem Zweck ausdrücklich eingewilligt wurde.

(2) Die Behandlung der Mitteilungen nach Absatz 1 durch die Kommission und die dazu vorgelegten Unterlagen unterliegen der Geheimhaltung gemäß § 28.

(3) An den Landtag gerichtete Eingaben von Bürgerinnen und Bürgern über ein sie betreffendes Verhalten des Verfassungsschutzes werden der Parlamentarischen Kontrollkommission bekannt gegeben.“

27. Die §§ 30 bis 32 werden durch die folgenden §§ 30 bis 33 ersetzt:

### **„§ 30**

#### **Anwendung des allgemeinen Datenschutzrechts**

(1) Gemäß § 2 Absatz 3 des Landesdatenschutzgesetzes gilt das Landesdatenschutzgesetz für den Verfassungsschutz nur, soweit er allgemeine Verwaltungsaufgaben wahrnimmt, und darüber hinaus nach Maßgabe dieses Gesetzes.

(2) Bei der Erfüllung der Aufgaben des Verfassungsschutzes nach § 5 finden die §§ 5 bis 7, § 46, § 47, § 51 Absatz 1 bis 4, §§ 52 bis 54, § 62, §§ 64 und 65, § 69, § 71, §§ 83 und 84 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nummer 149) geändert worden ist, entsprechende Anwendung.

### **§ 31**

#### **Unabhängige Datenschutzkontrolle**

(1) Jede Person kann sich an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten durch die Verfassungsschutzbehörde in ihren Rechten verletzt worden zu sein.

(2) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kontrolliert bei der Verfassungsschutzbehörde die Einhaltung der Vorschriften über den Datenschutz und berät sie entsprechend. Sie oder er ist befugt,

1. die Verfassungsschutzbehörde darauf hinzuweisen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen datenschutzrechtliche Pflichten verstoßen, und
2. festzustellen, wenn die Verfassungsschutzbehörde mit Verarbeitungsvorgängen gegen datenschutzrechtliche Pflichten verstoßen hat.

Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) Die Verfassungsschutzbehörde ist verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit und schriftlich besonders Beauftragte bei der Aufgabenerfüllung zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen, sowie
2. Zutritt in die für die Kontrolle erforderlichen Diensträume zu gewähren.

Dies gilt nicht, soweit das für den Verfassungsschutz zuständige Ministerium im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(4) Die Absätze 1 bis 3 gelten ohne Beschränkung auf die Erfüllung der Aufgaben nach § 5. Sie gelten entsprechend für die Verarbeitung personenbezogener Daten durch andere Stellen, wenn diese der Erfüllung der Aufgaben von Verfassungsschutzbehörden nach § 5 dient.

## **§ 32**

### **Maßnahmen zur Sicherung von Verschlusssachen**

(1) Die Verfassungsschutzbehörde trifft Maßnahmen zur Sicherung von Verschlusssachen nach Maßgabe folgender Vorschriften, um zu erkennen und zu verhindern, dass

1. Geräte der Informations- und Kommunikationstechnik sowie sonstige Gegenstände, die geeignet sind, Verschlusssachen auszubringen, zu zerstören, zu verändern, zu verarbeiten, zu kopieren, unbrauchbar zu machen oder Sabotagehandlungen vorzunehmen, in Diensträume unbefugt eingebracht werden oder
2. andere gegenständliche Verschlusssachen aus Diensträumen unbefugt ausgebracht werden.

(2) Die Verfassungsschutzabteilung darf Personen, die den Sicherheitsbereich der Verfassungsschutzbehörde gemäß § 52 Absatz 2 der Verschlusssachenanweisung für das Land Mecklenburg-Vorpommern vom 8. November 1999 (AmtsBl. M-V 2000 S. 50) betreten oder sich dort aufhalten, und von diesen Personen genutzte Fahrzeuge, mitgeführte Taschen und sonstige Gegenstände

1. verdachtsunabhängig kontrollieren und
2. durchsuchen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Sicherung von Verschlusssachen erforderlich ist.

(3) Eine Kontrolle nach Absatz 2 Satz 1 Nummer 1 ist die oberflächliche Suche nach Gegenständen an Personen, an oder in Taschen, mitgeführten Gegenständen und Fahrzeugen auch unter Einsatz technischer Mittel, ohne dass ein Körperkontakt mit der betroffenen Person stattfindet. Eine Durchsuchung nach Absatz 2 Satz 1 Nummer 2 ist die zielgerichtete und planmäßige Suche, auch unter Einsatz technischer Mittel,

1. am äußeren Körper der betroffenen Person,
2. in Kleidung und Taschen der betroffenen Person,
3. an und in Fahrzeugen einschließlich der dort befindlichen Gegenstände der betroffenen Person sowie
4. in sonstigen Gegenständen der betroffenen Person, die zur unbefugten Verbringung von amtlichen Informationen geeignet sind.

(4) Gegenstände, die sich im Sicherungsbereich befinden, darf die Verfassungsschutzabteilung sicherstellen und untersuchen, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie für eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit verwendet werden oder mit solchen Tätigkeiten gewonnen worden sind, oder
2. diese keiner bestimmten Person zuzuordnen sind und die Sicherstellung und Untersuchung zum Schutz vor einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit erforderlich ist.

Bei Geräten der Informations- und Kommunikationstechnik umfasst das Untersuchen auch das Eingreifen mit technischen Mitteln sowie das Verarbeiten der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten.

(5) Personen, die sich im Sicherungsbereich aufhalten, sind verpflichtet an Maßnahmen nach den Absätzen 2 und 4 mitzuwirken. Entziehen sich Personen Maßnahmen nach den Absätzen 2 und 4 im Sicherungsbereich, darf die Verfassungsschutzbehörde die Maßnahmen auch noch in unmittelbarer Nähe des Sicherungsbereichs vornehmen.

(6) Die Verfassungsschutzbehörde darf optisch-elektronische Einrichtungen zur offenen Überwachung des Sicherungsbereichs nach Maßgabe einer Dienstvorschrift einsetzen. In der Dienstvorschrift sind die Voraussetzungen, das Verfahren und Grenzen der Maßnahme zu regeln. Eine Überwachung höchstpersönlich genutzter Räume ist unzulässig.

(7) Die Verfassungsschutzbehörde kann eine nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung unzulässige Benutzung des Luftraums seines Sicherungsbereichs durch unbemannte Fluggeräte durch geeignete technische Mittel gegen das unbemannte Fluggerät, dessen Steuerungseinheit oder Steuerungsverbindung aufklären und abwehren.

(8) Die Verfassungsschutzbehörde darf die besonderen Mittel nach den §§ 10, 10a bis 10e, §§ 24a und 24b unter den dort genannten Voraussetzungen auch einsetzen, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Sicherung von Verschlusssachen

1. seiner Beschäftigten oder
2. von Personen, die von ihr beauftragt sind,
  - a) im Sicherungsbereich tätig zu sein oder
  - b) sonstige sicherheitsempfindliche Tätigkeiten wahrzunehmen.

(9) Bei der Durchführung von Maßnahmen zur Sicherung von Verschlusssachen hat die Verfassungsschutzbehörde unter mehreren möglichen und geeigneten Maßnahmen diejenigen zu treffen, die den Einzelnen am wenigsten beeinträchtigen. Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

**§ 33****Durchführung von Maßnahmen zur Sicherung von Verschlusssachen**

- (1) Personen gemäß § 32 Absatz 1 sind in geeigneter Form zu belehren über
  1. den ordnungsgemäßen Umgang mit Verschlusssachen,
  2. die Möglichkeit, dass bei ihnen Maßnahmen nach diesen Vorschriften durchgeführt werden können, sowie
  3. deren Pflicht zur Mitwirkung bei der Durchführung der Maßnahmen.
- (2) Maßnahmen nach § 32 Absatz 2 Satz 1 Nummer 2, Absatz 4 und 6 bedürfen der Anordnung der Leitung der Verfassungsschutzabteilung oder ihrer Stellvertretung.
- (3) Sichergestellte Gegenstände sind unverzüglich an die betroffene Person herauszugeben, sobald der Zweck der Maßnahme entfällt. Satz 1 gilt nicht, wenn die Gegenstände zur Einleitung oder Durchführung eines strafrechtlichen Ermittlungsverfahrens an die Strafverfolgungsbehörden weitergegeben werden müssen.
- (4) Bei Maßnahmen nach § 32 Absatz 2 Satz 1 Nummer 2 hat die betroffene Person das Recht, anwesend zu sein. Über eine Durchsuchung nach § 32 Absatz 2 Satz 1 Nummer 2 oder eine Sicherstellung nach § 32 Absatz 4 Satz 1 ist auf Verlangen eine Bescheinigung über die Maßnahme und den Grund der Maßnahme zu erteilen. Maßnahmen nach § 32 Absatz 4, die in Abwesenheit der betroffenen Person durchgeführt worden sind, sind ihr schriftlich mitzuteilen, wenn hierdurch nicht der Zweck der Maßnahme gefährdet wird.
- (5) Bei der Untersuchung von Geräten der Informations- und Kommunikationstechnik, die nicht ausschließlich zur dienstlichen Nutzung überlassen wurden, ist sicherzustellen, dass an dem Gerät nur Veränderungen vorgenommen werden, die für die Datenverarbeitung unerlässlich sind. Vorgenommene Veränderungen sind bei Beendigung der Maßnahme, soweit technisch möglich, rückgängig zu machen. Sichergestellte Telekommunikationsendgeräte sind abweichend von Absatz 3 Satz 1 unabhängig von dem Abschluss der Maßnahmen nach § 32 Absatz 4 an die betroffene Person spätestens nach zwei Wochen herauszugeben. Macht die betroffene Person in den Fällen des Satzes 3 Gründe glaubhaft, nach denen für sie eine Aufrechterhaltung der Sicherstellung nicht zumutbar ist, so ist das mobile Endgerät innerhalb von 48 Stunden nach Darlegung der Gründe an die betroffene Person zurückzugeben. Die Verfassungsschutzbehörde darf vor der Rückgabe ein Abbild der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten zur Datensicherung erzeugen.
- (6) Die Datenerhebung zum Zweck der Erlangung von Erkenntnissen über den Kernbereich privater Lebensgestaltung ist unzulässig. Die Verfassungsschutzbehörde darf Erkenntnisse, die den Kernbereich privater Lebensgestaltung berühren, nicht verarbeiten, weitergeben oder in anderer Weise nutzen. Sie hat, soweit möglich, technisch oder auf sonstige Weise sicherzustellen, dass Erkenntnisse, die den Kernbereich privater Lebensgestaltung berühren, nicht erlangt werden. Soweit Erkenntnisse erlangt wurden, die den Kernbereich privater Lebensgestaltung betreffen, sind diese Daten unverzüglich zu löschen. Erlangung und Löschung von Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach Ablauf von sechs Monaten zu löschen.

(7) Die Verfassungsschutzbehörde kann zur Durchsetzung von Maßnahmen gegenüber Personen, die nach § 32 Absatz 5 mitwirkungspflichtig sind, folgende Mittel anwenden:

1. unmittelbare Einwirkung auf die betroffene Person (körperliche Gewalt) oder Hilfsmittel der körperlichen Gewalt; eine Fesselung der betroffenen Person ist nur dann zulässig, wenn Tatsachen die Annahme rechtfertigen, dass sie die mit der Durchsetzung der Maßnahme beauftragten Personen oder Dritte angreifen, Widerstand leisten oder sich der Kontrolle entziehen wird,
2. unmittelbare Einwirkung auf Gegenstände mittels körperlicher Gewalt oder durch Hilfsmittel der körperlichen Gewalt.

Mittel nach Satz 1 dürfen nur durch besonders qualifizierte und geschulte Personen angewandt werden, die durch die Leitung der Verfassungsschutzabteilung hierzu besonders ermächtigt wurden. Das Grundrecht auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes) und Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes) wird insoweit eingeschränkt.

(8) Widerspruch und Anfechtungsklage gegen Maßnahmen nach § 32 in Verbindung mit § 33 Absatz 2 haben keine aufschiebende Wirkung.“

28. Der bisherige § 32 wird zu § 34.

## **Artikel 2 Inkrafttreten**

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

## **Begründung:**

### **A Allgemeiner Teil**

#### **I. Notwendigkeit der Änderung des Landesverfassungsschutzgesetzes**

Grundlage und Schwerpunkt des vorliegenden Änderungsentwurfes des Landesverfassungsschutzgesetzes (LVerfSchG M-V) sind drei Entscheidungen des Bundesverfassungsgerichts (BVerfG) aus den Jahren 2022 und 2024, mit denen das Gericht ausgeurteilte verfassungsrechtliche Grundzüge aus anderen Rechtsbereichen in die Rechtsgrundlagen des Handelns des Verfassungsschutzes projiziert hat:

- Urteil des BVerfG vom 26. April 2022 – 1 BvR 1619/ – zum Bayerischen Verfassungsschutzgesetz (BayVSG)
- Beschluss des BVerfG vom 28. September 2022 – 1 BvR 2354/13 – zu den Übermittlungsbefugnissen im Bundesverfassungsschutzgesetz (BVerfSchG)
- Beschluss des BVerfG vom 17. Juli 2024 – 1 BvR 2133/22 – zum Hessischen Verfassungsschutzgesetz (HVSG) – veröffentlicht am 17. September 2024

Zwar sind die Entscheidungen nicht zum LVerfSchG M-V ergangen, enthalten aber grundsätzliche Maßgaben, die zu übernehmen sind. Der Gesetzentwurf folgt den Schwerpunkten der Entscheidungen des BVerfG und den dortigen Konkretisierungen.

#### **II. Die Entscheidungen des Bundesverfassungsgerichts**

Im Urteil zum BayVSG postuliert das Gericht zum einen, dass sich das Maß der Verhältnismäßigkeitsanforderungen an heimliche Überwachungsmaßnahmen des Verfassungsschutzes im Einzelnen am jeweiligen Eingriffsgewicht auszurichten hat. Vorauszusetzen ist ein hinreichender verfassungsschutzspezifischer Aufklärungsbedarf, die Beobachtungsbedürftigkeit, die im Einzelfall die Maßnahme als geboten erscheinen lassen und durch hinreichende tatsächliche Anhaltspunkte belegt sein muss. Die Beobachtungsbedürftigkeit muss umso dringender sein, je höher das Eingriffsgewicht der Überwachungsmaßnahme ist. Aufgabe des Gesetzgebers ist es, die Maßgaben zur jeweiligen Beobachtungsbedürftigkeit hinreichend bestimmt und normenklar zu regeln. Das Gericht hält es in diesem Zusammenhang für erforderlich, dass je nach Eingriffsintensität der Maßnahme diese vor ihrer Durchführung einer Kontrolle durch eine unabhängige Stelle unterzogen wird.

Zum anderen sieht das Gericht in der Übermittlung der aus den Überwachungsmaßnahmen des Verfassungsschutzes resultierenden personenbezogenen Daten und Informationen an eine andere Stelle einen potenziellen erneuten Grundrechtseingriff. Wurden die Daten mit nachrichtendienstlichen Mitteln erhoben, kommt es darauf an, ob die empfangende Stelle zu dem jeweiligen Übermittlungszweck eine eigene Datenerhebung und Informationsgewinnung mit vergleichbar schwerwiegenden Mitteln wie die vorangegangene Maßnahme des Verfassungsschutzes erlaubt wäre (Kriterium der hypothetischen Neuerhebung).

Für eine Übermittlung ist vorauszusetzen, dass diese dem Schutz eines gewichtigen Rechtsguts dient. Bei der Festlegung der Übermittlungsschwelle ist zu differenzieren, an welche Stelle übermittelt wird (insbesondere Übermittlung an eine Gefahrenabwehrbehörde, Strafverfolgungsbehörde, andere Behörde mit operativer Anschlussbefugnis, sonstige Stelle oder Übermittlung ins Ausland). Die Anforderungen an die festzulegenden Eingriffsschwellen haben sich am Eingriffsgewicht zu orientieren, was wiederum auch von den operativen Anschlussbefugnissen der empfangenden Behörde abhängt.

Der Beschluss des BVerfG zu den Übermittlungsvorschriften des BVerfSchG konkretisiert die im Urteil zum BayVSG formulierten verfassungsrechtlichen Anforderungen an die Übermittlung von personenbezogenen Daten, die mit nachrichtendienstlichen Maßnahmen gewonnen wurden. Betont wird insbesondere, dass die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen. Ansonsten könnten operativ ausgestattete Behörden Folgemaßnahmen durchführen, also die durch den Verfassungsschutz erlangten Informationen weiter nutzen, ohne dass die für sie selbst als operative Behörden geltenden Erhebungsvoraussetzungen erfüllt sein müssten. Daher sind Anforderungen an den Rechtsgüterschutz und an die Eingriffsschwellen – hier in Form von Übermittlungsschwellen – zu stellen.

Der Beschluss des BVerfG vom 17. Juli 2024 – veröffentlicht erst am 17. September 2024 – erging zum HVSG, das erst auf der Grundlage der vorstehend angeführten Entscheidungen des BVerfG aus 2022 überarbeitet worden war, kontrollierte sozusagen die Umsetzung der vorangegangenen Rechtsprechung. Im Ergebnis wurden Vorschriften zur Definition des Grades der Beobachtungsbedürftigkeit, zu einzelnen Maßnahmen wie der Ortung von Mobilfunkgeräten oder des Einsatzes von verdeckten Bediensteten, aber auch zur Übermittlung an Strafverfolgungsbehörden und sonstigen öffentlichen Stellen als verfassungswidrig erkannt. Hauptsächlich die vom Gesetzgeber formulierten Eingriffsschwellen wurden seitens des Gerichts moniert.

### **III. Wesentlicher Inhalt der Novelle**

Aus der dargestellten Rechtsprechung resultiert überwiegend der vorliegende Änderungsentwurf. Als Schwerpunkte gelten

- die Einführung einer abgestuften Beobachtungsbedürftigkeit in § 6a,
- die Änderungen von Rechtsgrundlagen zu den Maßnahmen des Verfassungsschutzes gemäß §§ 10a bis f inklusive der erstmaligen ausdrücklichen Regelung des Schutzes des Kernbereichs privater Lebensgestaltung und der Personen, die dem Berufsgeheimnis unterliegen (§ 10a) sowie der Einführung der unabhängigen Kontrolle der Maßnahmen (§ 10f) und
- die Änderungen der Rechtsgrundlagen zu Übermittlungen von Erkenntnissen des Verfassungsschutzes (§§ 20 bis 23).



Es kommen hinzu:

- eine Rechtsgrundlage für Auskunftersuchen an das Bundeszentralamt für Steuern gemäß § 24,
- Ergänzungen der Vorschriften zur Parlamentarischen Kontrollkommission im Hinblick auf das Format ihrer Sitzungen und die Mitarbeit von Bediensteten (§§ 27, 28),
- eine Rechtsgrundlage für Eingaben der Bediensteten des Verfassungsschutzes an das Parlamentarische Kontrollgremium gemäß § 29a,
- ergänzende und lückenfüllende Vorschriften zum allgemeinen Datenschutz beim Verfassungsschutz (§§ 30, 31) sowie
- Vorschriften zur Sicherung von Verschlussachen beim Verfassungsschutz gemäß §§ 32, 33.

## **B      Besonderer Teil**

### **Zu Artikel 1 – Änderung des Landesverfassungsschutzgesetzes**

#### **Zu Nummer 1 (Inhaltsübersicht)**

Es handelt sich um Folgeänderungen aufgrund der Änderung des Landesverfassungsschutzgesetzes. Die Änderung der Inhaltsübersicht ist insbesondere aufgrund der Neuregelungen in §§ 10a bis 10f und §§ 20 bis 23 sowie der strukturbedingten Umstellung der §§ 30 bis 33 erforderlich.

#### **Zu Nummer 2 (§ 2 Organisation)**

Die Änderung betrifft die Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde. Die neutrale Formulierung verhindert eine zukünftige gesetzliche Anpassung im Falle eines Neuzuschnitts der Ressorts.

#### **Zu Nummer 3 (§ 5 Aufgaben des Verfassungsschutzes)**

##### **Zu Buchstabe a – § 5 Absatz 1 Nummer 4**

Es handelt sich um eine rechtsförmliche Änderung.

##### **Zu Buchstabe b – § 5 Absatz 2 Satz 1**

Durch die ausdrückliche Erwähnung der Aufgabe, präventiv über Wirtschaftsschutz zu informieren, wird diese auch bisher schon bestehende Aufgabe den aktuellen Erfordernissen entsprechend in den Vordergrund gerückt.

**Zu Buchstabe c – § 5 Absatz 3**

§ 5 Absatz 3 übernimmt die Regelung des bisherigen § 22. Es wird ausdrücklich geregelt, dass bei der Unterrichtung der Öffentlichkeit die Übermittlung personenbezogener Daten unter Anwendung des Verhältnismäßigkeitsprinzips nur dann erfolgen darf, wenn die Veröffentlichung erforderlich ist und im Rahmen einer Güterabwägung die Interessen der Allgemeinheit das Interesse der betroffenen Person überwiegen. In die Prüfung ist einzubeziehen, ob je nach den Umständen des Einzelfalls (insbesondere Umfang und Qualität der Daten) die betroffene oder dritte Person vorab über die Veröffentlichung zu benachrichtigen ist.

**Zu Buchstabe d – § 5 Absatz 4**

Hier wird sowohl eine rechtsförmliche Änderung umgesetzt als auch eine flexiblere Beschreibung der im Rahmen der Mitwirkung erfolgenden Personenüberprüfungen eingeführt.

**Zu Buchstabe e – § 5 Absatz 5**

Es handelt sich um eine Folgeänderung zu Buchstabe c.

**Zu Nummer 4 (§ 6 Begriffsbestimmungen)****Zu Buchstabe a – § 6 Absatz 2**

Die Neufassung dieses Absatzes beschreibt zum einen, wann eine Person einer Bestrebung im Sinne von § 5 Absatz 1 zugerechnet wird. Es wird nunmehr der Klarheit halber eine nachdrückliche Unterstützung der in Absatz 1 hinsichtlich ihrer Zielausrichtung definierten Bestrebungen verlangt, die Hervorhebung der Ausrichtung auf Gewaltanwendung entfällt. Zum anderen stellt sie klar, dass entsprechende Bestrebungen unter den dort genannten Bedingungen auch von Einzelpersonen ausgehen können. Rechnung getragen wird dem Umstand, dass unter den Bedingungen moderner Kommunikation einerseits und aufgrund der Erkenntnisse zu Radikalisierungsverläufen andererseits die Bedrohung durch Einzelpersonen der durch Personenzusammenschlüssen gleichzustellen ist. Soziale Medien eröffnen der Agitation und den Hassbotschaften von Einzelpersonen eine hohe Alltagsverbreitung und enorme Wirkungsbreite. Ebenso zeigen die Anschläge der jüngsten Vergangenheit, dass die dort gezeigten Radikalisierungsverläufe eine bessere Aufklärung im Vorfeld militanter Handlungen erforderlich machen, wenn tatsächliche Anhaltspunkte erkennbar sind. Im Sinne der Einheit der Rechtsordnung wird die bisherige Regelung der des Bundes angepasst.

**Zu Buchstabe b – § 6 Absatz 4 (Streichung)**

Aufgrund der Neuformulierung des § 6 Absatz 2 (siehe vorstehend Buchstabe a) ist dieser Absatz nicht mehr erforderlich.

**Zu Buchstabe c – § 6 Absatz 4 (neu)**

Es handelt sich um eine Folgeänderung zu Buchstabe b.

**Zu Buchstabe d – § 6 Absatz 6 (Streichung)**

Aufgrund der Neuformulierung des § 6 Absatz 2 (siehe vorstehend Buchstabe a) ist dieser Absatz nicht mehr erforderlich.

**Zu Nummer 5 (§ 6a Beobachtungsbedürftigkeit)**

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 26. April 2022 (1 BvR 1619/17) zum Bayerischen Verfassungsschutzgesetz grundsätzliche Aussagen zur gesetzlichen Ausgestaltung der Verhältnismäßigkeit von heimlichen nachrichtendienstlichen Mitteln in Bezug auf ihr jeweiliges Eingriffsgewicht getroffen (BVerfG, a. a. O., Rn. 149 ff.). Der Gesetzgeber muss die dem Eingriffsgewicht der verschiedenen Überwachungsbefugnisse entsprechenden Eingriffsschwellen durch Maßgaben zur jeweils erforderlichen Beobachtungsbedürftigkeit hinreichend bestimmt und normenklar regeln. Dabei muss die Beobachtungsbedürftigkeit umso dringender sein, je höher das Eingriffsgewicht der Überwachungsmaßnahme ist (BVerfG, a. a. O., Rn. 181, 190). Das bedeutet nicht, dass der Gesetzgeber im Gesetz selbst festlegen muss, welche Bestrebungen in welchem Maße beobachtungsbedürftig sind. Erforderlich ist aber eine abstrakt beschreibende Bezeichnung des dem Eingriffsgewicht jeweils angemessenen Maßes der Beobachtungsbedürftigkeit, für das zudem hinreichend bestimmte Kriterien vorgegeben sein müssen (BVerfG, a. a. O., Rn. 202). Die nachrichtendienstliche Beobachtungsbedürftigkeit hängt vor allem von der Intensität der Bedrohung der Schutzgüter des Verfassungsschutzes ab.

**Zu § 6a Absatz 1**

Eine „einfache“ Beobachtungsbedürftigkeit muss dementsprechend – als Basis- oder Einstiegsstufe – bei jeglichem Einsatz nachrichtendienstlicher Mittel gemäß § 10 vorhanden sein, ohne dass ein herausgehobenes Eingriffsgewicht festgestellt wird. Diese normale Beobachtungsbedürftigkeit setzt voraus, dass die Bedingungen des grundsätzlichen Beobachtungsauftrags im Sinne von § 7 Absatz 1 Satz 2 in Verbindung mit § 5 Absatz 1 gegeben sind. Dementsprechend ist der Begriff „beobachtungsbedürftig“ in § 6a Absatz 1 durch eine Bezugnahme auf § 5 Absatz 1 Nummer 1, 3 und 4 bestimmt.

**Zu § 6a Absatz 2**

Tätigkeiten nach § 5 Absatz 1 Nummer 2 („sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht im Geltungsbereich dieses Gesetzes“) sind in § 6a Absatz 1 nicht genannt, sondern werden der nächsthöheren Stufe der Beobachtungsbedürftigkeit unter § 6a Absatz 2 zugeordnet. Aufgrund der Bedrohung durch eine fremde Macht und den dahinterstehenden erhöhten Ressourcen ist bei hinreichend tatsächlichen Anhaltspunkten für einen solchen Sachverhalt (siehe zu dieser Voraussetzung § 6a Absatz 4) eine erhebliche Beobachtungsbedürftigkeit nach § 6a Absatz 2 gerechtfertigt.

**Zu § 6a Absatz 3**

Die Begriffsbestimmung „erheblich beobachtungsbedürftig“ im Sinne von § 6a Absatz 2 setzt voraus, dass sonstige Bestrebungen gemäß § 5 Absatz 1 vorliegen, die „allgemein, insbesondere nach Verhaltens- oder Wirkungsweise geeignet sind, die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes erheblich zu beeinträchtigen“. Laut Bundesverfassungsgericht steigt die Beobachtungsbedürftigkeit, je deutlicher tatsächliche Anhaltspunkte vorliegen, die es möglich erscheinen lassen, dass die Schutzgüter des Verfassungsschutzes konkret bedroht sind und dass gegen sie gerichtetes Handeln erfolgreich sein kann (BVerfG, a. a. O., Rn. 193 m. w. N.). Als Indizien für die erhebliche Beobachtungsbedürftigkeit einer Bestrebung führt das Gericht selbst eine Reihe von Kriterien an (BVerfG, a. a. O., Rn. 194 f.), die als Maßstab einer entsprechenden Beurteilung der Beurteilungspotenzialität in den Gesetzestext dieser Begriffsbestimmung in § 6a Absatz 3 abgestuft übertragen werden:

- Gewaltorientierung oder volksverhetzende Betätigung
- strafrechtlich relevantes Verhalten
- Maß der Abschottung
- Größe: Mitglieder- und Sympathisantenbestand und -entwicklung, Organisationsstruktur, Mobilisierungsgrad, Kampagnenfähigkeit, finanzielle Lage
- Wirkkraft in der Gesellschaft (Publikationen, Bündnisse, Unterstützerstrukturen, Vertretung in Ämtern, Mandate)
- Kontraindikation: legalistisches Vorgehen; aber abhängig von Umständen des Einzelfalls z. B. besonders beobachtungsbedürftig, wenn in sehr großem Stil besonders wirkungsvoll Fehlinformationen verbreitet oder aber eine Atmosphäre der Angst oder Bedrohung herbeigeführt wird und dies geeignet ist, den freien Prozess politischer Willensbildung nachhaltig zu beeinträchtigen.

Die nach Absatz 2 für die Einstufung der erheblichen Beobachtungsbedürftigkeit einer Bestrebung festzustellende Eignung der Bestrebung stellt auf deren Verhaltens- oder Wirkungsweise ab. Laut Bundesverfassungsgericht (Beschluss zum HVSG vom 17. Juli 2024 – 1 BvR 2133/22, juris Rn. 149) sind vom Gesetzgeber Indizien und Anhaltspunkte vorzugeben, unter deren Berücksichtigung der Verfassungsschutz eine Gesamtbetrachtung der Potenzialität der Bestrebung vorzunehmen hat. Dementsprechend sind in Absatz 3 Satz 1 bis 3 die vorgenannten Kriterien je nach Stringenz im Hinblick auf die Eignung eingestellt worden, um die vom Verfassungsschutz vorzunehmende Beurteilung der Beeinträchtigungspotenzialität zu steuern.

Während Absatz 3 Satz 1 Nummer 1 bis 3 ergebnisbindende Vorgaben enthält – die Bestrebung begeht zur Zielverfolgung Straftaten –, bei deren Vorliegen die Eignung nach Absatz 2 anzunehmen ist (BVerfG a. a. O., Rn. 153 f.), haben die Kriterien der Sätze 2 und 3 nur indiziellen Charakter oder die Qualität von Anhaltspunkten.

Satz 2 Nummer 1 und 2 beschreibt Verhaltens- und Vorgehensweisen von Bestrebungen, bei deren Vorliegen in der Regel von einer Eignung auszugehen ist, es aber im Sinne einer widerlegbaren Vermutung einer weiteren Beurteilung im Einzelfall bedarf, ob tatsächlich eine Beeinträchtigungspotenzialität anzunehmen ist oder Anhaltspunkte nicht gegen die Vermutung sprechen.

Satz 3 Nummer 1 bis 4 sind als abstrakte Anhaltspunkte zu verstehen, bei deren Vorliegen die Eignung nach Absatz 2 anzunehmen sein kann, wenn auch die Gesamtbeurteilung des Einzelfalls zu einem hinreichenden Maß über konkrete und gewichtige tatsächliche Umstände verfügt, die den Rückschluss auf die Möglichkeit erfolgreichen Agierens der Bestrebung gegen die Schutzgüter des Verfassungsschutzes rechtfertigen (BVerfG a.a.O., Rn. 155 f.). Wenn eine Bestrebung vollkommen dilettantisch, wenn auch in erheblichem Umfang gesellschaftlichen Einfluss auszuüben sucht, kann beispielsweise von einer Beeinträchtigungspotenzialität nicht ausgegangen werden.

Während der Gesetzgeber also mit den Regelungen des Absatzes 3 Satz 1 bis 3 abstrakte Vorgaben normiert, bei deren Vorliegen von einer erheblichen Beeinträchtigungspotenzialität auszugehen oder diese zumindest indiziell in Betracht zu ziehen ist, obliegt die anschließende Gesamtbetrachtung der Potenzialität in den Fällen der Sätze 2 und 3 der Einschätzungsprärogative des Verfassungsschutzes. Diese Ausgestaltung begründet das Gericht damit, dass „gerade in dem vom Verfassungsschutz aufzuklärenden Vorfeldbereich [...] Bewertungen aufgrund geringer Tatsachendichte in besonderem Maße von Erfahrung, Fachwissen und nachrichtendienstlichen Erkenntnislagen abhängig [sind], über die die Verfassungsschutzbehörde verfügt, nicht aber der Gesetzgeber, der entsprechende Kriterien formuliert“ (BVerfG a. a. O., Rn. 149 m. w. N.).

Zu den einzelnen nachrichtendienstlichen Maßnahmen und der Bedeutung der Einstufung der Beobachtungsbedürftigkeit im Hinblick auf deren unabhängige Kontrolle siehe §§ 10b Absatz 4, 10c bis 10e unter Nummer 10 und 11.

#### **Zu § 6a Absatz 4**

Absatz 4 Satz 1 und 2 weisen auf die besondere Bedeutung von tatsächlichen Anhaltspunkten für die Einstufung der Beobachtungsbedürftigkeit nach den Absätzen 1 bis 3 hin. Die Anhaltspunkte müssen sich auf die Möglichkeit einer konkreten Bedrohung der Schutzgüter des Verfassungsschutzes in § 5 Absatz 1 in Verbindung mit § 6 Absatz 1 und 3 und auf den Erfolg des gegen sie gerichteten Handelns beziehen. Satz 3 bestimmt die Notwendigkeit einer jährlichen Aktualisierung der Einstufung sowie Satz 4 ihren Wegfall nach Zeitablauf. Die 5-Jahresfrist des Satzes 4 stellt sicher, dass durch taktisches vorübergehendes Ruhigverhalten des Beobachtungsobjektes dieses nicht aus dem Blickfeld des Verfassungsschutzes gerät. Gleichwohl müssen die Voraussetzungen des Absatzes 4 zum Zeitpunkt einer geplanten Maßnahme konkret vorliegen und es darf nicht auf die jährliche Aktualisierung verwiesen werden.

**Zu Nummer 6 (§ 7 Rahmen für die Tätigkeit der Verfassungsschutzbehörde)**

In § 7 wird der vollständige Absatz 1 durch den neu formulierten Absatz 1 ersetzt<sup>1</sup>.

Es handelt sich um Änderungen, die rechtsförmlicher und stilistischer Natur sind sowie um eine Anpassung an die Begriffsbestimmungen in Artikel 4 Nummer 2 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 (Datenschutz-Grundverordnung). Darüber hinaus wird anstelle des bisherigen allgemeinen Verweises auf das Landesdatenschutzgesetz auf den neugefassten § 30 und dessen Maßgaben verwiesen.

**Zu Nummer 7 (§ 9 Formen der Datenerhebung)**

In § 9 werden die bisherigen Absätze 1 und 2 durch die neu formulierten Absätze 1 und 2 ersetzt<sup>1</sup>.

Während § 9 Absatz 1 Satz 1 die Voraussetzungen regelt, unter denen personenbezogene Daten ohne Kenntnis der betroffenen oder einer dritten Person erhoben werden können, normiert Satz 2 – in Verbindung mit Satz 3 – bei Nichtvorliegen der Voraussetzungen des Satzes 1 Nummer 1 bis 3 die konkrete Verfahrensweise, wonach die Datenerhebung nicht nur mit einfacher Kenntnis, sondern – konkreter – mit ausdrücklicher Einwilligung erfolgen muss.

Wie in Absatz 1 Satz 2 erfolgt in Satz 3 eine Anpassung an die Begrifflichkeit im Datenschutz („Einwilligung“ anstelle von „Aufklärung“).

Die Streichung des bisherigen Absatzes 1 Satz 4 resultiert daraus, dass dort eine Fallkonstellation geregelt wurde, bei der eine Aufklärung bzw. Einwilligung unterbleibt. Diese Konstellation ist jedoch nach Satz 1 zu beurteilen, sodass der Satz entfallen kann.

Darüber hinaus handelt es sich um eine Anpassung des Gesetzestextes an die Begriffsbestimmungen in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung sowie an die geschlechterneutrale Sprache und rechtsförmliche Änderungen.

**Zu Nummer 8 (§ 10 Informationsbeschaffung mit nachrichtendienstlichen Mitteln)**

Die erfolgte vollständige Ersetzung des § 10 betrifft allgemeine rechtsförmliche Änderungen und Anpassungen des Gesetzestextes an die geschlechterneutrale Sprache<sup>1</sup>.

Im speziellen ergeben sich darüber hinaus Änderungen in § 10 Absatz 1 als Folgeänderungen aufgrund der Änderung in § 10 Absatz 2 Satz 1 Nummer 2 und § 10b.

---

<sup>1</sup> Nach der Neuauflage des Handbuchs der Rechtsförmlichkeit, 4. Auflage 2024 (HdR4), ist künftig der Grundsatz „Revision statt Binnenrevision“ zu beachten. Das bedeutet, dass grundsätzlich ganze Gliederungseinheiten (Paragraf, Absatz, Satz oder Nummer) ersetzt und nur noch ausnahmsweise Einzeländerungen innerhalb von Gliederungseinheiten vorgenommen werden sollen. Dieses gilt für diese und weitere gleichgelagerte Stellen.

**Zu § 10 Absatz 1 Nummer 3**

Die schon bisher unter § 10 Absatz 1 Nummer 3 aufgeführte nachrichtendienstliche Maßnahme „Observationen“ erfährt nun in der eingefügten Vorschrift des § 10c besondere Regelungen, auf die hier verwiesen wird.

**Zu § 10 Absatz 1 Nummer 7**

Die schon bisher unter § 10 Absatz 1 Nummer 7 aufgeführte nachrichtendienstliche Maßnahme „verdecktes Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13 des Grundgesetzes“ erfährt nun in der eingefügten Vorschrift des § 10d besondere Regelungen, auf die hier verwiesen wird.

**Zu § 10 Absatz 1 Nummer 9**

Die zu § 10 Absatz 1 Nummer 9 zu streichende Angabe hat aufgrund früherer Änderungen des Gesetzes keine Bedeutung mehr.

**Zu § 10 Absatz 1 Nummer 12**

Die Änderung zu § 10 Absatz 1 Nummer 12 ist mit Blick auf die einschlägige Rechtsprechung erforderlich: Maßnahmen der Internetaufklärung sind dem Verfassungsschutz nicht grundsätzlich verwehrt (so BVerfG, Urteil vom 27.02.2008, 1 BvR 370/07, 1 BvR 595/07 – Online-Durchsuchung –, Rn. 304 ff.). Weder greift das heimliche Aufklären des Internets in das allgemeine Persönlichkeitsrecht ein, wenn Daten, die der Inhaber des Systems für die Internetkommunikation vorgesehen hat, auf dem technisch dafür vorgesehenen Weg erhoben werden. Noch ist das Recht auf informationelle Selbstbestimmung betroffen, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. Ein Grundrechtseingriff liegt aber vor, wenn sich eine staatliche Stelle unter einer Legende in eine Kommunikationsbeziehung begibt und dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde.

In der Benennung der nachrichtendienstlichen Mittel in § 10 ist in Nummer 12 der Text daher entsprechend der vorgenannten Rechtsprechung zu schärfen. Nicht jede Internetaufklärung durch den Verfassungsschutz unterliegt den qualifizierten Anforderungen eines nachrichtendienstlichen Mittels des § 10. Als Schwelle zum nd-Mittel-Einsatz ist die Ausnutzung eines schutzwürdigen Vertrauens der betroffenen oder einer dritten Person anzusehen. Nur wenn das schutzwürdige Vertrauen in die Identität und die Wahrhaftigkeit des Kommunikationspartners ausgenutzt wird, etwa durch Überwinden vorgesehener Überprüfungs- bzw. Zugangssicherungsmechanismen per Legende, ist die Internetaufklärung durch den Verfassungsschutz als nachrichtendienstliches Mittel anzusehen und den Anforderungen insbesondere des § 10 Absatz 2 und 3 unterworfen.

Klarzustellen ist, dass der Begriff des Internets auch die sogenannten sozialen Medien umfasst. Soziale Medien funktionieren definitionsgemäß nur über das Internet, da sie auf digitaler Vernetzung und Interaktivität basieren. Es gibt keine sozialen Medien, die ohne Internet existieren, da ihre grundlegenden Merkmale – wie der schnelle Austausch von Inhalten und die Vernetzung von Nutzern – eine Internetverbindung voraussetzen. Sie unterfallen folglich auch der Aufklärung des Internets durch den Verfassungsschutz im oben dargestellten Sinne.

#### **Zu § 10 Absatz 1 Nummer 13**

Die Ortung von Mobilfunkgeräten war bisher in § 10 Absatz 7 geregelt, ohne in der Aufzählung des § 10 Absatz 1 genannt zu werden. Da sie aufgrund ihrer Eingriffswirkung als nachrichtendienstliche Maßnahme im Sinne dieser Vorschrift zu qualifizieren ist, wird sie als Nummer 13 ausdrücklich aufgeführt und die Regelungen ihrer Voraussetzungen aus gesetzesstrukturellen Gründen in den § 10e verlagert.

#### **Zu § 10 Absatz 2**

Die durch den Vorbehalt „soweit nicht anders geregelt“ vorgenommene Ergänzung in § 10 Absatz 2 Satz 1 Satzteil 1 ist erforderlich, da neben den generellen Regelungen des Absatzes 2 für einige nachrichtendienstliche Maßnahmen spezielle Regelungen gelten.

#### **Zu § 10 Absatz 3**

Durch den hinzugefügten Satz in § 10 Absatz 3 Satz 4 (neu) wird auf die Differenzierung der Beobachtungsbedürftigkeit bei besonders eingriffsintensiven nachrichtendienstlichen Maßnahmen und die daraus folgende Notwendigkeit der unabhängigen Kontrolle dieser Maßnahmen hingewiesen.

#### **Zu § 10 Absatz 3a**

Die Sätze 4 bis 6 des bisherigen § 10 Absatz 3 werden aus inhaltlichen Gründen in einen neuen Absatz 3a überführt. Weitere Änderungen im Text erfolgten aus rechtsförmlichen Gründen sowie aufgrund der Anpassung an die Begriffsbestimmungen in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung.

#### **Zur Streichung der bisherigen Absätze 6 und 7**

Die Notwendigkeit der Regelungen in § 10 Absatz 6 entfällt, da die nachrichtendienstliche Maßnahme des § 10 Absatz 1 Nummer 7 im neuen § 10d geregelt wird.

Da die bisher ausschließlich in § 10 Absatz 7 normierte nachrichtendienstliche Maßnahme der Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartenummer neu unter § 10 Absatz 1 Nummer 13 aufgeführt und im neuen § 10e geregelt wird, entfällt die Notwendigkeit der Regelungen in § 10 Absatz 7.



**Zu Nummer 9 (§ 10a Schutz des Kernbereichs privater Lebensgestaltung und der Personen, die dem Berufsgeheimnis unterliegen)****Zu § 10a Absatz 1**

Der neu eingefügte § 10a enthält eine allgemeine Regelung zum Schutz des Kernbereichs privater Lebensführung und der Personen, die dem Berufsgeheimnis unterliegen, im Rahmen des Einsatzes nachrichtendienstlicher Mittel.

Nach der Rechtsprechung des BVerfG beansprucht der Kernbereich privater Lebensgestaltung gegenüber allen Überwachungsmaßnahmen Beachtung, weshalb der Gesetzgeber Regelungen schaffen müsse, die einen wirksamen Schutz normenklar gewährleisten (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – BKA-Gesetz, Rn. 123 m. w. N.). Auch wenn das BVerfG im BKAG-Urteil eine eigene gesetzliche Regelung nur für „verletzungsgeneigte Befugnisse“ gefordert hat, die „typischerweise zur Erhebung kernbereichsrelevanter Daten führen“, und die Maßstäbe des BKAG-Urteils nicht unmittelbar auf das Recht der Nachrichtendienste übertragbar sind, wird nun mit Absatz 1 eine allgemeine Regelung für alle nachrichtendienstlichen Mittel geschaffen werden. Diese gilt für die allgemeinen nachrichtendienstlichen Mittel i. S. v. § 10 Absatz 1, soweit nicht spezielle Regelungen getroffen sind.

Der Gesetzgeber ist nach Ansicht des BVerfG nicht verpflichtet, bestimmte Personengruppen von Überwachungsmaßnahmen von vornherein auszunehmen (BVerfG a. a. O. Rn. 132). Gleichwohl wird nun in Absatz 1 Satz 1 Nummer 2 und Absatz 2 auch eine allgemeine Regelung zum Schutz von Personen, die dem Berufsgeheimnis unterliegen, eingeführt, die bei allen nachrichtendienstlichen Mitteln zu beachten ist.

Nach Absatz 1 Satz 2 ist die Maßnahme zu unterbrechen, wenn eine hinreichende Wahrscheinlichkeit für relevante Inhalte im Sinne des Satzes 1 besteht und für eingesetzte Bedienstete keine Gefährdung oder Enttarnung droht. Bei Zweifeln über deren Vorliegen oder die Dauer ihres Vorliegens darf nach Absatz 1 Satz 3 die Maßnahme nur in Form einer ausschließlichen automatischen Aufzeichnung durch- oder fortgeführt werden (BVerfG, a. a. O., juris Rn. 239 ff.), sofern eine solche Möglichkeit besteht. Über Zweifelsfälle entscheidet nach Satz 4 die Kommission gemäß § 10f. Eventuell aus dem Kernbereich privater Lebensgestaltung erhobene Erkenntnisse dürfen nicht verarbeitet werden und sind zu löschen (Satz 5). Dokumentationspflichten ergeben sich aus Satz 6.

**Zu § 10a Absatz 2**

Absatz 2 entspricht inhaltlich dem § 3b Absatz 2 Satz 2 G 10 und damit einem bundeseinheitlichen Standard. Im Unterschied zu § 3b Absatz 2 G 10 sind Rechtsanwältinnen und Rechtsanwälte den Verteidigerinnen und Verteidigern gleichgestellt und unterfallen der Schutzvorschrift nach Absatz 1.

**Zu Nummer 10 (§ 10b Vertrauensleute und verdeckte Bedienstete)**

Laut Bundesverfassungsgericht (Beschluss vom 17. Juli 2024 zum HVSG – 1 BvR 2133/22 – juris Rn. 184 ff.) handelt es sich beim Einsatz von Vertrauensleuten und verdeckten Bediensteten um eines der schwerwiegendsten Mittel, das dem Verfassungsschutz zur Verfügung steht. Dabei könne das Eingriffsgewicht je nach konkreter Ausgestaltung erheblich variieren. Das Gewicht hänge insbesondere von der Dauer des Einsatzes, aber auch davon ab, welche Intensität die geschaffenen und genutzten Beziehungen erlangen. Je länger der Einsatz dauert, je tiefergehende Vertrauensbeziehungen entstehen und je mehr private Informationen erlangt werden, umso dringender muss der Beobachtungsbedarf sein und umso größeren Aufklärungsgewinn muss die Maßnahme versprechen. Der Gesetzgeber darf die Wahrung der Verhältnismäßigkeitsanforderungen nicht vollständig dem Verfassungsschutz überlassen, sondern muss für das Eingriffsgewicht einerseits und die Dringlichkeit der Maßnahme andererseits maßgebliche Gesichtspunkte selbst regeln.

**Zu § 10b Absatz 1**

Dementsprechend ist § 10b Absatz 1 Satz 2 neu zu fassen. Es wird darauf hingewiesen, dass tatsächliche Anhaltspunkte sowohl für die Annahme einer beobachtungsbedürftigen Bestrebung als auch für das Gebotensein der Aufklärung vorliegen müssen. Dabei ist zu beachten, ob die Vertrauensperson mit dem Betroffenen nur oberflächlich kommuniziert oder eine Vertrauensbeziehung herstellt und ausnutzt. Nur in der letztgenannten Fallgestaltung liegt ein Eingriff von höherem Gewicht vor, der nur durch eine erhebliche Beobachtungsbedürftigkeit im Sinne des neuen § 6a legitimiert werden kann.

**Zu § 10b Absatz 1a**

Aufgrund der Qualifizierung einer Maßnahme nach § 10b als einem der schwerwiegendsten Mittel, das dem Verfassungsschutz zur Verfügung steht, werden im neuen § 10b Absatz 1a die Voraussetzung geregelt, unter denen sich eine solche Maßnahme gegen eine Person richten darf. Hier kommt insbesondere der in § 10b Absatz 1a Nummer 2 geregelten sog. Zusammenhangsperson besondere Bedeutung zu, einer Person, die nur zu einer unmittelbaren Zielperson im Sinne von § 10 Absatz 1a Nummer 1 im Kontakt steht, ohne selbst Beteiligter einer Bestrebung zu sein. Da eine Maßnahme gegenüber einer solchen Person besonders schwer wiegt (siehe BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 341), werden die Voraussetzungen unter § 10b Absatz 1a Nummer 2 Buchstabe a und b normiert.

**Zu § 10b Absatz 4**

Um die Anforderungen des Verhältnismäßigkeitsprinzips an diese nachrichtendienstliche Maßnahme und die besonderen Eingriffsschwellen zu normieren, ist die Einfügung eines neuen Absatzes 4 erforderlich.

Je länger der Einsatz von Vertrauensleuten oder verdeckten Bediensteten dauert, desto höher ist das Eingriffsgewicht dieser Maßnahme des Verfassungsschutzes zu bemessen. Im Sinne des Verhältnismäßigkeitsgrundsatzes, dem jeder Eingriff unterworfen ist, muss dementsprechend auch die Beobachtungsbedürftigkeit umso dringender sein.

In Umsetzung der vom Bundesverfassungsgericht ausgeurteilten Maßgabe, wonach der Gesetzgeber Eingriffsschwellen zu normieren hat, wird in Absatz 4 festgelegt, dass als Bemessungsmaßstab des Eingriffs die Zeitdauer gilt. Ab einer Einsatzdauer von sechs Monaten muss eine erhebliche Beobachtungsbedürftigkeit im Sinne von § 6a Absatz 2 und 3 vorliegen (siehe dazu unter Nummer 5), um diesen Eingriff als verhältnismäßig im engeren Sinne zu beurteilen. Darüber hinaus ist die konkrete Maßnahme aufgrund der Eingriffstiefe der unabhängigen Kontrolle gemäß § 10f zu unterziehen (siehe dazu unter Nummer 11).

Allerdings ist nicht nur die Einsatzdauer in die Beurteilung der Eingriffstiefe einzustellen. In der Beurteilung des Einzelfalls kann es auch auf die Qualität der Maßnahme ankommen. Soll das Verhältnis zur Vertrauensperson nicht nur zum Abschöpfen von Informationen im Wege einfacher Kommunikation genutzt, sondern dazu ein intensiveres Vertrauensverhältnis hergestellt werden, kann auch unterhalb der Eingriffsschwelle von sechs Monaten die Eingriffstiefe zur Notwendigkeit einer erheblichen Beobachtungsbedürftigkeit und der Beteiligung der unabhängigen Kontrolle erforderlich sein.

Darüber hinaus wird eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache und rechtsförmliche Änderungen sowie die Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde vorgenommen.

#### **Zu Nummer 11 (§§ 10c bis 10f)**

Die folgenden §§ 10c bis 10f werden zusammengefasst<sup>1</sup>:

#### **§ 10c – Observationen**

Je länger eine Observation von Personen durch den Verfassungsschutz dauert, desto höher ist das Eingriffsgewicht dieser Maßnahme zu bemessen. Im Sinne des Verhältnismäßigkeitsgrundsatzes, dem jeder Eingriff unterworfen ist, muss dementsprechend auch die Beobachtungsbedürftigkeit umso dringender sein. In Umsetzung der vom Bundesverfassungsgericht ausgeurteilten Maßgabe, wonach der Gesetzgeber Eingriffsschwellen zu normieren hat, wird in Absatz 2 festgelegt, dass als Bemessungsmaßstab des Eingriffs die Zeitdauer gilt. Ab einer durchgehenden Observation von länger als 48 Stunden oder mehr als vier Tagen muss eine erhebliche Beobachtungsbedürftigkeit im Sinne von § 6a Absatz 2 und 3 vorliegen (siehe dazu unter Nummer 5), um diesen Eingriff als verhältnismäßig im engeren Sinne zu beurteilen. Darüber hinaus ist die konkrete Maßnahme aufgrund der Eingriffstiefe der unabhängigen Kontrolle gemäß § 10f zu unterziehen (siehe dazu unter dieser Nummer). Weiterhin wird in Absatz 4 das Erfordernis der Mitteilung jeder durchgeführten Observation an die betroffene Person nach Maßgabe des § 11 normiert.

**§ 10d – Verdecktes Mithören oder Aufzeichnen des nicht öffentlichen Wortes unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13 des Grundgesetzes**

§ 10d ersetzt vor dem Hintergrund der neuen Rechtsprechung des Bundesverfassungsgerichts den bisherigen § 10 Absatz 6 (siehe zu Nummer 8). Auch bei dieser Maßnahme steigt das Eingriffsgewicht, je länger sie dauert. Insbesondere ist dies der Fall, wenn die Maßnahme mit einer Observation zusammenfällt und das gesamte Eingriffsgewicht in die Verhältnismäßigkeitserwägungen einzustellen ist. Im Sinne des Verhältnismäßigkeitsgrundsatzes muss dementsprechend auch die Beobachtungsbedürftigkeit umso dringender sein. In Umsetzung der vom Bundesverfassungsgericht ausgeurteilten Maßgabe, wonach der Gesetzgeber Eingriffsschwellen zu normieren hat, ist bei festgelegter Dauer der Maßnahme eine erhebliche Beobachtungsbedürftigkeit erforderlich und diese der unabhängigen Kontrolle zu unterziehen. Die Regelung des Absatzes 1 Satz 2 stellt dabei sicher, dass die Eingriffsschwelle des Satzes 1 nicht als starre Grenzen zu verstehen sind. Wenn im Einzelfall die Zeitgrenzen nicht erreicht sind, kann nach Beurteilung der Eingriffstiefe dennoch die erhebliche Beobachtungsbedürftigkeit erforderlich sein.

Die bisherige Regelung des § 10 Absatz 6 verlangte, dass jedes verdeckte Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13 GG der Zustimmung der G10-Kommission bedurfte. Die neue Regelung des § 10d entspricht demgegenüber der aktuellen differenzierenden Betrachtungsweise des BVerfG (Urteil vom 26. April 2022, insbesondere Rn. 214, 217), wonach erst bei eingriffsintensiven Maßnahmen über die normierte Schwelle hinaus die unabhängige Kontrolle einzuschalten ist (so Absatz 2). Zu betonen ist dazu, dass eine Maßnahme nach § 10d ausdrücklich nur außerhalb des Schutzbereiches des Artikels 13 (Unverletzlichkeit der Wohnung) stattfinden darf. In Absatz 3 wird die Pflicht zur Mitteilung jeder Maßnahme nach § 10 Absatz 1 Nummer 7 gegenüber der betroffenen Person nach Maßgabe des § 11 normiert. Absatz 4 ersetzt die bisherige Regelung des § 10 Absatz 6 Satz 2 im Hinblick auf die Verarbeitung der gewonnenen Daten und verweist auf die entsprechend anzuwendenden Regelungen des § 4 des Artikel 10-Gesetzes, soweit im Landesverfassungsschutzgesetz keine abweichenden Regelungen getroffen werden.

**§ 10e – Verdeckte Standortermittlung und Ermittlung der Geräte- und Kartennummern mit technischen Mitteln**

Der neue § 10e ersetzt den bisherigen § 10 Absatz 7, der bisher die Anwendung technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummern regelte.

§ 10 Absatz 7 wurde mit Wirkung vom 28. Januar 2009 in das LVerfSchG eingefügt. Ausweislich der Begründung dieses Absatzes (Drucksache 5/1936 vom 28. Oktober 2008, S. 14 f.) sollte damit in erster Linie „eine ausdrückliche gesetzliche Ermächtigung [...] zum Einsatz des sog. IMSI-Catchers zur Ermittlung der Geräte und Kartennummer von Telefonen“ geschaffen werden, um damit die zugehörige Telefonnummer über den Provider zu ermitteln. Der Einsatz des IMSI-Catchers wurde in der Folge den strengen Voraussetzungen des Artikel 10-Gesetzes unterworfen, indem auf verschiedene Regelungen des § 24a verwiesen wurde, die wiederum ihren Ursprung im Artikel 10-Gesetz finden.

Auf der Grundlage der Entscheidungen des Bundesverfassungsgerichts aus 2022 und 2024 zu den entsprechenden Vorschriften des Bayerischen und Hessischen Verfassungsschutzgesetzes (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 317 ff., und BVerfG-Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 120 ff.) wird die Regelung der verdeckten Standortermittlung und Ermittlung der Geräte- und Kartennummern mit technischen Mitteln in § 10d neu strukturiert und anders rechtlich eingeordnet.

Im Hinblick auf den Anwendungsbereich als Rechtsgrundlage zur verdeckten Standortermittlung mit technischen Mitteln stellt zunächst Absatz 1 Nummer 1 klar, dass nicht nur der Standort eines Mobiltelefons davon erfasst ist, sondern auch andere Gegenstände wie beispielsweise ein Pkw, dessen Standort durch das Anbringen eines GPS-Trackers ermittelt werden kann, soweit dadurch personenbezogene Daten ermittelt werden. Generell gilt für die Standortermittlung eines Mobiltelefons das Versenden von sogenannten stillen SMS als übliches Mittel. Für die Standortbestimmung wird dem IMSI-Catcher keine praktische Einsatzmöglichkeit beigemessen, da die Kenntnis des ungefähren Aufenthaltsortes der Zielperson vorauszusetzen und die technische Reichweite des Gerätes begrenzt ist (so auch BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 319, 323). Generell eröffnet die Rechtsgrundlage zur Ermittlung von Standortdaten die Möglichkeit, in die durch Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG grundrechtlich geschützte informationelle Selbstbestimmung der Betroffenen einzugreifen. Die Ermittlung von Standortdaten kann zu Bewegungsprofilen führen, die als schwerwiegende Grundrechtseingriffe zu qualifizieren sind. Während eine frühere Entscheidung des Bundesverfassungsgerichts darüber hinaus einen Eingriff in den Schutzbereich des Fernmeldegeheimnisses aus Artikel 10 Absatz 1 GG verneint (BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, so auch Löffelmann, in: Handbuch des Rechts der Nachrichtendienste, 2017, VI § 5 Rn. 69), bedarf es nach den Entscheidungen des BVerfG zum Bayerischen und Hessischen Verfassungsschutzgesetz keiner abschließenden Entscheidung, welches der beiden Grundrechte zur Anwendung kommt. Denn die Maßgaben des Artikels 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG, die auch im neuen § 10e ihren Niederschlag finden, lassen sich weitgehend auf die speziellere Garantie des Artikels 10 GG übertragen.

Absatz 1 Satz 2 übernimmt die bisherige Regelung des § 10 Absatz 7 Satz 4 im Hinblick auf die Verarbeitung der gewonnenen Daten und verweist auf die entsprechend anzuwendenden Regelungen des § 4 des Artikel 10-Gesetzes, soweit im Landesverfassungsschutzgesetz keine abweichenden Regelungen getroffen werden.

Besondere Bedeutung hat eine Maßnahme zur Ermittlung des Standortes aufgrund ihrer Eingriffsintensität, wenn sie eine räumliche Nachverfolgung im engen Zeittakt über einen längeren Zeitraum und damit die Erstellung eines Bewegungsprofils zulässt (siehe dazu BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 125 ff.). Dementsprechend sensibilisiert Absatz 2 für entsprechende Maßnahmen, die nicht nur punktuellen Charakter haben, wie z. B. die Standortfeststellung zum Beginn einer Observation, sondern aufgrund einer längeren Zeitdauer der ermittelten Standorte nach und nach ein Bewegungsbild der Person mit erhöhter Persönlichkeitsrelevanz entwickeln. Für solche Fälle von erhöhter Eingriffstiefe normiert Absatz 2 das Erfordernis einer erheblichen Beobachtungsbedürftigkeit im Sinne von § 6a und eine Befassung der unabhängigen Kontrolle nach § 10f.

Absatz 3 Satz 1 zeigt indiziell auf, welche unterschiedlichen Fallgestaltungen der Standortermittlung zu einem erhöhten Eingriffsgewicht führen können. Absatz 3 Satz 3 konkretisiert in zeitlicher Hinsicht im Wege von widerleglichen Regelbeispielen Schwellenwerte für Maßnahmen, die eine erhebliche Beobachtungsbedürftigkeit und einer unabhängigen Kontrolle bedürfen.

Absatz 4 legt fest, gegen welche Zielpersonen sich die Maßnahmen nach § 10e richten dürfen und wie personenbezogene Daten Dritter zu schützen sind. Zur Erhebung personenbezogener Daten Dritter allgemein siehe § 9 Absatz 2.

### **Zu § 10f – Unabhängige Kontrolle**

Der Gesetzgeber ist nach den genannten maßgeblichen Entscheidungen des Bundesverfassungsgerichts gehalten, die dem Eingriffsgewicht der verschiedenen Überwachungsbefugnisse entsprechenden Eingriffsschwellen durch Maßgaben zur jeweils erforderlichen Beobachtungsbedürftigkeit hinreichend bestimmt und normenklar zu regeln. Dementsprechend wird neben der herkömmlichen normalen Beobachtungsbedürftigkeit für besonders schwerwiegende Eingriffe in die Persönlichkeitssphäre das Erfordernis der erheblichen Beobachtungsbedürftigkeit eingeführt (siehe § 6a und zu Nummer 5).

Da im Rahmen der Tätigkeit des Verfassungsschutzes mit besonders eingriffsintensiven Überwachungsmaßnahmen zu rechnen ist, indem verdeckt höchstprivate Informationen erfasst werden, knüpft das Bundesverfassungsgericht an die Maßnahmen mit dem Erfordernis einer erheblichen Beobachtungsbedürftigkeit (siehe § 10b Absatz 4 – Einsatz von Vertrauensleuten und verdeckten Bediensteten, § 10c Absatz 2 – Observationen, § 10d Absatz 1 – Verdecktes Mithören oder Aufzeichnen des nicht öffentlichen Wortes unter Einsatz technischer Mittel außerhalb des Schutzbereiches des Artikels 13 des Grundgesetzes, § 10e Absatz 2 – Verdeckte Standortermittlung und Ermittlung von Karten- und Gerätenummern mit technischen Mitteln) eine vorherige Kontrolle dieser Maßnahmen durch eine unabhängige Stelle. „Eine vorbeugende Kontrolle ist bedeutsames Element eines effektiven Grundrechtsschutzes und gewährleistet, dass die Entscheidung über eine heimliche Maßnahme auf die Interessen der Betroffenen hinreichend Rücksicht nimmt, wenn diese selbst ihre Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen können.“ – so das Bundesverfassungsgericht (Urteil vom 26. April 2022 – 1 BvR 1619/17 – juris Rn. 214 f. m. w. N.).

Im Hinblick auf die organisatorische Zuordnung der unabhängigen Stelle äußert das Bundesverfassungsgericht für den Verfassungsschutz keine Vorgaben. Dass die Vorabkontrolle gerade durch ein Gericht erfolgt, sei verfassungsgerichtlich grundsätzlich nicht vorgegeben (a. a. O. juris Rn. 224). Nach ständiger Rechtsprechung des Bundesverfassungsgerichts kann ein solches Kontrollorgan sowohl innerhalb des Parlaments als auch als unabhängige Institution im Funktionsbereich der Exekutive angesiedelt werden (BVerfG, Urteil vom 15. Dezember 1970 – 2 BvR 1/69 – Rn. 77; BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 – Rn. 39).

§ 10f Absatz 1 überträgt die Aufgabe der unabhängigen Kontrolle der G 10-Kommission. Bei der G 10-Kommission handelt es sich um ein Kontrollorgan eigener Art außerhalb der rechtsprechenden Gewalt, das generell als Ersatz für den fehlenden gerichtlichen Rechtsschutz dient. Es agiert innerhalb des Funktionsbereichs der Exekutive, ist aber nicht in diese kooperiert (BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 – Rn. 41). Die für eine effektive unabhängige Vorabkontrolle notwendige gesetzlich gewährleistete Unabhängigkeit ergibt sich aus § 2 Absatz 3 Satz 2 des Gesetzes zur Ausführung des Artikel 10-Gesetzes (G10AG MV). Der oder die Vorsitzende muss gemäß § 2 Absatz 3 Satz 1 G10AG MV die Befähigung zum Richteramt aufweisen. Die Mitglieder der G 10-Kommission (eine Vorsitzende oder ein Vorsitzender sowie drei Beisitzer) werden für die Dauer einer Legislaturperiode gewählt (§ 2 Absatz 3 Satz 3 G10AG MV), sodass in personeller Hinsicht Kontinuität hinsichtlich der Aufgabenwahrnehmung – auch bezüglich länger angelegter Maßnahmen – sichergestellt ist. Dies, aber auch die notwendigerweise bei den Mitgliedern vorhandene Erfahrung in der Beurteilung nachrichtendienstlicher Sachverhalte stellen das Fundament für die notwendige Gesamtexpertise der Kommission sicher. Da die G 10-Kommission aufgrund ihrer herkömmlichen Aufgabe bereits über Kenntnisse zu schwerwiegenden Überwachungsmaßnahmen im Schutzbereich des Artikels 10 GG verfügt, kann hierauf bei der Beurteilung von weiteren nachrichtendienstlichen Maßnahmen zurückgegriffen werden. Nicht zuletzt ist sowohl die Kommission als auch ihr Ausschussbüro gewohnt, mit Verschlusssachen aller Geheimhaltungsgrade umzugehen.

Absatz 1 Satz 3 zeigt auf, dass angeordnete nachrichtendienstliche Maßnahmen, die die Kontrolle nicht bestanden haben, unverzüglich aufzuheben sind.

Absatz 2 Satz 1 legt fest, dass die Kommissionskontrolle durch die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung schriftlich zu beantragen ist. Damit liegt die Befugnis zur Antragstellung in derselben Verantwortung wie die Anordnungsbefugnis, die gemäß Absatz 4 ebenso der Leitung der Verfassungsschutzabteilung oder ihrer Stellvertretung obliegt.

Absatz 2 Satz 2 in Verbindung mit Absatz 3 regeln Antragsform und Inhalte der substantiierten Begründung eines Kontrollantrages und auch die Behandlung von Informationen anderer Behörden sowie schützenswerter Details der Tätigkeit des Verfassungsschutzes.

Absatz 5 erklärt § 2 Absatz 1 Satz 2 und 5 sowie Absatz 3 und 4 des Gesetzes zur Ausführung des Artikel 10-Gesetzes für anwendbar.

Absatz 6 trifft Vorkehrungen für den Fall, dass von der Regelung des entsprechend anzuwendenden § 2 Absatz 1 Satz 5 des Gesetzes zur Ausführung des Artikel 10-Gesetzes Gebrauch gemacht wird, wonach der Kommission die für die Erfüllung ihrer Aufgaben notwendige Personalausstattung zur Verfügung zu stellen ist. Die Regelungen des Absatzes 6 sind an die Regelungen für die Parlamentarische Kontrollkommission in § 28 Absatz 1 angelehnt.

**Zu Nummer 12 (§ 11 Mitteilung an betroffene Personen)**

Die Norm wird zum einen sprachlich überarbeitet und zum anderen inhaltlich an die Bundesnorm des § 12 des Artikel 10-Gesetzes (Mitteilung an Betroffene) angepasst, indem insbesondere der Kommission gemäß § 10f die abschließende Entscheidung übertragen wird, die Mitteilung über zwölf Monate nach Beendigung der nachrichtendienstlichen Maßnahme zurückzustellen oder gänzlich zu unterlassen. In Satz 3 wird die Zuständigkeitsregelung eingefügt, wonach die Leitung der Verfassungsschutzabteilung oder ihre Stellvertretung die notwendigen Entscheidungen nach den Sätzen 2 und 3 entsprechend der Umstände des Einzelfalls trifft.

**Zu Nummer 13 (§ 12 Registereinsicht durch die Verfassungsschutzbehörde)**

Es handelt sich um rechtsförmliche Änderungen und eine Anpassung an die Begriffsbestimmungen in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung.

**Zu Nummer 14 (§ 14 Dateianordnung)**

In § 14 werden die bisherigen Absätze 2 und 3 durch die neuformulierten Absätze 2 und 3 ersetzt<sup>1</sup>.

Die Neufassung berücksichtigt eine Korrektur der Behördenbezeichnung, die verbunden wird mit der geschlechterneutralen Sprache, und bezieht nunmehr auch Änderungen von Dateianordnungen mit ein. Darüber hinaus wird die Pflicht der Verfassungsschutzabteilung eingefügt, zur besseren Übersicht und für Zwecke der Kontrolle ein Verzeichnis der geltenden Dateianordnungen zu führen. Die Regelung in Absatz 3 beinhaltet datenschutzrechtliche Maßgaben, die auf dem Grundsatz der Verhältnismäßigkeit beruhen.

**Zu Nummer 15 (§ 16 Verarbeitung personenbezogener Daten von Minderjährigen)**

§ 16 wird vollständig ersetzt<sup>1</sup>.

Die Neuregelung in Absatz 1, wonach auch personenbezogene Daten von Minderjährigen unter 14 Jahren verarbeitet werden können, berücksichtigt, dass zunehmend Fälle bekannt werden, in denen sich bereits unter 14-jährige Personen innerhalb kürzester Zeit – insbesondere über das Internet – radikalisierten und sogar bereit sind, Anschläge zu verüben.

Neben den üblichen Speichervoraussetzungen der §§ 9 und 15, die auch für alle Personen ab dem 14. Lebensjahr gelten, bestehen für die unter 14-Jährigen allerdings strengere Voraussetzungen. Es müssen im Einzelfall tatsächliche Anhaltspunkte dafür bestehen, dass sie eine der in § 3 Absatz 1 des Artikel 10-Gesetzes genannten Straftaten planen, begehen oder begangen haben, also besonders bedeutsame Rechtsgüter betroffen sind.

Die neue Regelung des Absatzes 2 Satz 1 beinhaltet im Vergleich zu § 17 Absatz 3 Satz 2 und 3 im Hinblick auf das Alter der von Absatz 1 Satz 1 Betroffenen erheblich verkürzte Überprüfungs- und Löschfristen.



**Zu Nummer 16 (§ 17 Speichern, Berichtigen, Löschen und Verarbeitungseinschränkung personenbezogener Daten)**

Die Änderungen beinhalten jeweils eine Anpassung an die Begriffsbestimmungen in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung. Darüber hinaus wird in Absatz 5 Satz 6 durch die vorgenommene ergänzende Angabe „der Wahrung schutzwürdiger Interessen des Betroffenen“ ein direkter Bezug zur Regelung des Absatzes 5 Satz 3 hergestellt.

**Zu Nummer 17 (§§ 20 bis 23)**

Die folgenden §§ 20 bis 23 werden zusammengefasst<sup>1</sup>:

**Zu § 20 – Zweckbindung, Weiterverarbeitung**

Zweckbindung ist ein zentraler Grundsatz des allgemeinen Datenschutzrechts. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Eine Weiterverarbeitung ist nur zulässig, wenn sie mit dem ursprünglichen Zweck vereinbar ist oder wenn eine gesetzliche Grundlage vorliegt. Das Landesverfassungsschutzgesetz erfüllt den Grundsatz der Zweckbindung, indem die Zwecke der Verarbeitung personenbezogener Daten in den spezifischen Regelungen geregelt sind.

**Zu § 20 Absatz 1**

Der neue § 20 Absatz 1 Satz 1 stellt klar, dass erhobene personenbezogene Daten über den dafür vorhandenen Anlass hinaus genutzt werden können, wenn dies zur eigenen Aufgabenerfüllung gemäß § 5 dient. Die eigene Weiternutzung unterliegt nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung, wenn sie auf gesetzlicher Grundlage erfolgt (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 278). Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die ursprüngliche Datenerhebung. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt nur im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. Die weitere Nutzung solcher Daten ist für den Verfassungsschutz auf jeden Fall unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt (BVerfG, a. a. O. Rn. 281 ff.). Sollen die Daten aber für eine Maßnahme genutzt werden, deren Rechtsgrundlage zum Schutz anderer Rechtsgüter normiert ist, so liegt im Vergleich zur ursprünglichen Datenerhebung ein Fall der Zweckänderung vor. Es wäre sicherzustellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird, also sämtliche Voraussetzungen einer Ermächtigungsgrundlage für die weitere Nutzung gegeben sind.

§ 20 Absatz 1 Satz 2 weist darauf hin, dass die Übermittlung personenbezogener Daten an eine andere Stelle ein Fall der Nutzungs- oder Zweckänderung darstellt. Etwaige Übermittlungen der aus heimlichen Überwachungsmaßnahmen des Verfassungsschutzes stammenden Information an andere Stellen sind dann an Voraussetzungen gebunden, die seitens der Verfassung an entsprechende eigene Grundrechtseingriffe der empfangenden Stellen zu richten sind („Kriterium der hypothetischen Datenneuerhebung“; vgl. BVerfG, a. a. O., Rn. 284 ff., 287). Nach dem Kriterium der „hypothetischen Datenneuerhebung“ kommt es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften.

Das Bundesverfassungsgericht führt im Hinblick auf die Situation des Verfassungsschutzes aus: „Die weitreichenden Überwachungsbefugnisse der Verfassungsschutzbehörden können verfassungsrechtlich nur gerechtfertigt werden, wenn die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen („informationelles Trennungsprinzip“; vgl. BVerfGE 133, 277 <329 Rn. 123>; 156, 11 <50 Rn. 101, 51 f. Rn. 105>). Ansonsten böte der Umstand, dass die Verfassungsschutzbehörde selbst nicht über operative Anschlussbefugnisse verfügt, den Überwachten am Ende doch kaum Schutz: Die der Verfassungsschutzbehörde verschlossenen eingriffsintensiven Folgemaßnahmen könnten dann von operativ ausgestatteten Behörden durchgeführt werden, die dabei die durch die Verfassungsschutzbehörde erlangten Informationen weitenutzten, ohne dass die für sie selbst als operative Behörden geltenden Datenerhebungsvoraussetzungen erfüllt sein müssten. Aufseiten der empfangenden Behörde würden so die grundrechtsschützenden Eingriffsschwellen der Befugnisse operativer Behörden umgangen; zugleich verlöre auf Seiten der Verfassungsschutzbehörden der Umstand, dass diese ohne operative Anschlussbefugnisse sind, seinen schützenden Effekt.“ (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 172).

Dementsprechend ist die bisherige Vorschrift des § 20 zur Informationsübermittlung an Behörden und andere Stellen durch die Regelungen der §§ 20a bis 20e, § 20g, §§ 21 und 22 zu ersetzen. In diesen werden differenzierend nach der jeweiligen Aufgabenstellung und den Befugnissen der empfangenden Stelle die Anforderungen sowohl an den Rechtsgüterschutz als auch an die Eingriffsschwellen – hier in Form von Übermittlungsschwellen – normiert. Die neue Nutzung der Daten muss einerseits dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten solchen Gewichts dienen, dass dies eine Neuerhebung durch die empfangende Stelle mit vergleichbar schwerwiegenden Mitteln die vorangegangene Überwachung durch den Verfassungsschutz rechtfertigen könnte. Andererseits setzt die Übermittlung grundsätzlich einen Anlass voraus, der eine ebenso eingriffsintensive Ersterhebung durch die empfangende Stelle verfassungsrechtlich rechtfertigen würde (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 231 m. w. N.).

#### **Zu § 20 Absatz 2 bis 4**

Die Absätze 2 und 3 schützen die Rechte der von der Übermittlung betroffenen Personen, indem Vorgaben für die Weiterverarbeitung durch die empfangende Stelle gemacht werden.

Absatz 2 enthält entsprechende Prüf- und Löschpflichten.

Absatz 3 sichert die Bindung der empfangenden Stelle an den Übermittlungszweck.

Absatz 4 erstreckt das Auskunftsrecht von Personen, bei denen eine nachteilige Folge in einem Verfahren zur vorbeugenden Personenüberprüfung auf der Übermittlung des Verfassungsschutzes beruht, darauf, dass diese nachteilige Folge durch die Übermittlung des Verfassungsschutzes verlasst wurde.

**Zu § 20a – Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr**

§ 20a regelt die Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten für Zwecke der Gefahrenabwehr. Sie ermöglicht Datenübermittlungen zur Wahrnehmung von Aufgaben, zu deren Erfüllung die Empfangsbehörde durch entsprechende Anschlussmaßnahmen in Grundrechte eingreifen darf. Solche Datenübermittlungen haben besonderes Gewicht, weil durch sie die weitreichenden Aufklärungsbefugnisse der Verfassungsschutzbehörde in den Dienst potenziell schwerwiegender Anschlussmaßnahmen durch Polizei- oder andere Ordnungsbehörden gestellt werden.

Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine Datenübermittlung von einer Verfassungsschutzbehörde an eine Behörde mit derartigen Anschlussbefugnissen nur zugelassen werden, wenn sie zur Abwehr einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 235 ff.; Beschluss vom 28. September 2022 – 1 BvR 2354/13 – Rn. 124 ff.).

**Zu § 20a Absatz 1**

Gemäß Absatz 1 Satz 1 sind beide Voraussetzungen anhand von tatsächlichen Anhaltspunkten im Einzelfall festzustellen. Während hiermit eine Befugnis vorliegt, in deren Rahmen ein Entschließungsermessen auszuüben ist, regelt Absatz 1 Satz 2 die Voraussetzungen, bei deren Vorliegen im Interesse eines wirksamen Rechtsgüterschutzes eine Verpflichtung zur Übermittlung besteht.

**Zu § 20a Absatz 2**

Absatz 2 enthält eine Legaldefinition der konkretisierten Gefahr, die an die Rechtsprechung des Bundesverfassungsgerichts anknüpft.

Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, Urteil vom 20. April 2016 – 1 BvR 1140/09 – Rn. 112).

Speziell in Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können die Anforderungen an die Erkennbarkeit des Geschehens weiter abgesenkt werden, wenn dafür bereits genauere Erkenntnisse über die beteiligten Personen bestehen. Hier gilt, dass Überwachungsmaßnahmen auch dann erlaubt werden können, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, dafür aber das individuelle Verhalten einer Person bereits die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (BVerfG, Urteil vom 20. April 2016 – 1 BvR 1140/09 – Rn. 112).

**Zu § 20a Absatz 3**

Absatz 3 zählt die besonders gewichtigen Rechtsgüter auf, zu deren Schutz eine Übermittlung für Zwecke der Gefahrenabwehr zulässig ist. Die Aufzählung orientiert sich an der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 105 m. w. N.).

**Zu § 20b – Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz**

§ 20b regelt Datenübermittlungen von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten mit präventiver Zielsetzung, wobei die Eingriffsschwelle abweichend von dem allgemeinen Erfordernis einer zumindest konkretisierten Gefahr wie in § 20a bestimmt wird. Er ist damit als Ausnahmebestimmung bzw. Erweiterung im Verhältnis zu § 20a zu verstehen. Infolgedessen ist vor einem Rückgriff auf § 20b stets vorrangig zu prüfen, ob nicht bereits eine zumindest konkretisierte oder gar konkrete Gefahr vorliegt und damit der Anwendungsbereich von § 20a eröffnet ist. In Abgrenzung zu § 20a wird die auch zu einer behördlichen Intervention führende Datenübermittlung hier als präventiver Rechtsgüterschutz bezeichnet, was den nicht bereits gefahrveranlassenden, sondern vorbeugend risikoregulierenden Charakter umschreibt.

Die Befugnisse nach § 20b betreffen teilweise auch Übermittlungen an Stellen, die grundsätzlich operative Anschlussbefugnisse ausüben können, ist aber enumerativ auf absolute Ausnahmefälle beschränkt, in denen Sicherheitsinteressen der Allgemeinheit infolge zwingender rechtlicher Wertungen die mit der Datenübermittlung einhergehenden Grundrechtseingriffe zulasten Einzelner überwiegen und damit zu rechtfertigen sind.

Erkennbares Leitbild des Bundesverfassungsgerichts für die Entwicklung der strengen Erfordernisse für die Datenübermittlung an Behörden mit operativen Anschlussbefugnissen ist die Abgrenzung von Nachrichtendiensten und Polizeibehörden (vgl. grundlegend BVerfGE 133, 277 Rn. 115 ff.; darauf Bezug nehmend mit dem Begriff der „Gefahrenabwehrbehörden“ BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 234 ff.; BVerfG, Beschluss vom 28. September 2022 – 1 BvR 2354/13 – Rn. 124 ff.).

Polizeibehörden verfügen über ein breites Arsenal aktioneller und informationeller Befugnisse einschließlich diverser Möglichkeiten der Anwendung unmittelbaren Zwangs. Zugleich eröffnet dies unter Verhältnismäßigkeitsgesichtspunkten einen gewissen Spielraum bei Übermittlungen an andere Behörden, die zwar ebenfalls über Anschlussbefugnisse zu belastenden Maßnahmen verfügen, bei denen allerdings aufgrund ihres spezifischeren Handlungsspielraums und -instrumentariums in geringerem Maße durch die Übermittlung ein Risiko für Folgeeingriffe in Grundrechte besteht.

Solche Behörden können zwar in gewissem Umfang auf Zwangsbefugnisse zurückgreifen und verfügen zum Teil über Eingriffsbefugnisse, deren Einsatz die Lebensgestaltung der betroffenen Person dauerhaft beeinträchtigen kann. Beispiele bilden eine Gewerbeuntersagung oder eine Ausweisung. Andererseits unterscheiden sich die Fähigkeiten solcher Behörden zu Grundrechtseingriffen und Zwangsmaßnahmen in ihrer Breite und Tiefe deutlich von denen der Polizeibehörden, was im Rahmen der verfassungsrechtlich gebotenen Verhältnismäßigkeitsabwägung zu berücksichtigen ist.

Daher ist für jede Übermittlungskonstellation abzuwägen, ob der durch die Übermittlung verfolgte Rechtsgüterschutz und das Maß der dadurch vermittelten Grundrechtsbeeinträchtigung in einem angemessenen Verhältnis zueinanderstehen. Das schließt es zugleich aus, solche Übermittlungen auf Grundlage einer Generalklausel zuzulassen. Vor diesem Hintergrund ist es nur ausnahmsweise vertretbar, Datenübermittlungen der Verfassungsschutzbehörde an Sicherheitsbehörden mit Eingriffs- oder Zwangsbefugnissen unterhalb der Schwelle einer konkretisierten Gefahr zuzulassen.

#### **Zu § 20b Absatz 1**

§ 20b Absatz 1 enthält vor diesem Hintergrund einen abschließenden Katalog von besonderen Übermittlungstatbeständen zur Erfüllung sicherheitsbehördlicher Aufgaben, die dem Schutz besonders gewichtiger Rechtsgüter dienen und ein Abweichen von dem allgemeinen Erfordernis des Vorliegens einer konkretisierten Gefahr aufseiten der datenempfangenden Stelle rechtfertigen. Hierbei geht es um Datenübermittlungen zur Wahrnehmung von Aufgaben, in deren Rahmen die Empfangsbehörden zu Maßnahmen befugt sind, die gegebenenfalls auch im Wege des Verwaltungszwangs oder mittels unmittelbaren Zwangs vollstreckt werden können. Beispielsweise dürfen die Aufenthaltsbehörden eine ausländische Person ausweisen (§ 53 des Aufenthaltsgesetzes – AufenthG) und die durch die Ausweisung begründete Ausreisepflicht gegebenenfalls durch eine Abschiebung vollstrecken (§ 58 AufenthG). Darüber hinaus dürfen diese Behörden etwa Wohnungen durchsuchen (§ 58 Absatz 6 AufenthG) oder eine Person in Abschiebungshaft nehmen (§ 62 AufenthG).

#### **Zu § 20b Absatz 2**

Absatz 2 regelt Datenübermittlungen zur Prüfung der Voraussetzungen begünstigender Maßnahmen. Solche Maßnahmen können die rechtlich geschützten Interessen der betroffenen Person erheblich berühren, haben jedoch weder selbst Zwangscharakter noch können sie mit Zwangsmitteln durchgesetzt werden. Das strenge Erfordernis einer konkretisierten Gefahr als Mindestschwelle der Datenübermittlung gilt für sie daher nicht, während sich die verfassungsrechtlichen Anforderungen an den Rechtsgüterschutz auch auf diese Übermittlungen erstrecken (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 254). Nach Absatz 2 reicht es daher aus, wenn die Übermittlung aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Vorbereitung, Durchführung oder Überprüfung einer begünstigenden Maßnahme und zum Schutz der Rechtsgüter des § 20a Absatz 3 erforderlich ist. Beispiele für solche Maßnahmen sind eine Wirtschaftssubvention, die Vergabe eines öffentlichen Auftrags oder eine Gnadenentscheidung.

#### **§ 20c – Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung**

Die Vorschrift des § 20c regelt die Voraussetzungen, unter denen die Verfassungsschutzbehörde mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an Strafverfolgungsbehörden zum Zweck der Strafverfolgung übermitteln darf.

Auch für solche Übermittlungsvorgänge, die neben dem Informationserhebungsakt als weitere, eigenständige Grundrechtseingriffe einzustufen sind, verlangt das Bundesverfassungsgericht, dass diese dem Schutz eines besonders gewichtigen Rechtsguts dienen müssen. Darüber hinaus kommen Übermittlungen an Strafverfolgungsbehörden nur zur Verfolgung besonders schwerer Straftaten in Betracht und setzen zudem voraus, dass ein durch bestimmte Tatsachen begründeter Verdacht vorliegt, für den konkrete und verdichtete Umstände als Tatsachenbasis vorhanden sind (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Ls. Nr. 3; BVerfG, Beschluss vom 28. September 2022 – 1 BvR 2354/13 – Rn. 137).

Mit Blick auf den materiell-strafrechtlichen Rechtsgüterschutz und das im deutschen Strafverfahren jedenfalls grundsätzlich geltende Legalitätsprinzip ist bei Vorliegen der Voraussetzungen dieser Bestimmung das Ermessen zur Übermittlung personenbezogener Daten in der Regel auf null reduziert. Aspekten wie der effektiven (weiteren) Erfüllung des nachrichtendienstlichen Beobachtungsauftrags einschließlich Fragen des Quellenschutzes kann dann lediglich im Zusammenhang mit Art und Umfang der weiterzugebenden Daten Rechnung getragen werden. In Sonderfällen kann zudem eine Übermittlung nach § 25 Absatz 1 ausgeschlossen sein.

#### **Zu § 20c Absatz 1**

In materieller Hinsicht verlangt Absatz 1 Satz 1 das Vorliegen von bestimmten Tatsachen für die Begehung einer besonders schweren Straftat. Insofern genügt zwar das Vorliegen eines strafprozessualen Anfangsverdachts gemäß § 152 Absatz 2 StPO. Dieser muss sich aber auf bestimmte, bereits erwiesene Tatsachen gründen und ein gewisses Maß an Konkretisierung und Verdichtung erreicht haben (BVerfGE 109, 279 Rn. 247; BGH NStZ-RR 2010, 282). Der Sache nach wird somit ein qualifizierter Tatverdacht verlangt, der über das Vorliegen lediglich „zureichender tatsächlicher Anhaltspunkte“ für das Vorliegen einer verfolgbaren Straftat hinausreicht.

#### **Zu § 20c Absatz 2**

Absatz 2 regelt, was als „besonders schwere Straftat“ zu verstehen ist. Absatz 2 Nummer 1 resultiert daraus, dass im Strafverfahrensrecht mit § 100b Absatz 2 StPO ein Straftatenkatalog existiert, der im Kontext mit der Eingriffsschwere der jeweiligen Ermittlungsmaßnahme festlegt, welche Straftaten besonders schwere Straftaten sind. Im Hinblick auf Verweisungen auf andere Gesetze hat das Bundesverfassungsgericht zwar ausgeführt, dass diese begrenzt bleiben müssen und insbesondere durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, nicht ihre Klarheit verlieren dürfen (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 272). In Bezug auf die Wertung von Straftaten als besonders schwer kann der Gesetzgeber aber laut dem Bundesverfassungsgericht auch auf bereits bestehende Straftatenkataloge zurückgreifen (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 206). Sofern hier, wie mit Absatz 2 Nummer 1 geschehen, auf den vom Bundesgesetzgeber festgelegten Straftatenkatalog in § 100b Absatz 2 StPO verwiesen wird, ist dies grundsätzlich unbedenklich, wenn auf diese von einem anderen Gesetzgeber erlassene Bestimmung nicht dynamisch, sondern statisch verwiesen wird (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 383 ff.). Die statische Verweisung folgt dabei aus der ersten Inbezugnahme der Strafprozessordnung in § 10a Absatz 1 Nummer 2 (neu).

Absatz 2 Nummer 2 orientiert sich bei der Bestimmung der erforderlichen Schwere der Straftat allein an der Strafdrohung. Das Bundesverfassungsgericht hat klargestellt, dass als besonders schwere Straftaten solche anzusehen sind, die mit einer Höchststrafe von mehr als fünf Jahren bedroht sind (BVerfG, Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21 – Rn. 179). Nach der gesetzlichen Systematik werde in Tatbeständen mit einem fünf Jahre übersteigenden oberen Strafraumen sogleich eine Höchststrafe von zehn Jahren Freiheitsentzug oder mehr normiert. Diese Höchststrafe sei denjenigen Delikten vorbehalten, die ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 203 m. w. N.).

Absatz 2 Nummer 3 sieht besonders schwere Straftaten als gegeben an, wenn diese im Höchstmaß mit Freiheitsstrafe von mindestens fünf Jahren bedroht sind und weitere Umstände hinzukommen. Die besondere Schwere ergibt sich in Abgrenzung zu Nummer 2 nicht allein aus der Strafdrohung. Es wird die Rechtsprechung des Bundesverfassungsgerichts aufgegriffen, wonach auch eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren dann als besonders schwer eingestuft werden, wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint. Dabei muss die Qualifizierung einer Straftat als besonders schwer in der Strafnorm selbst einen objektivierten Ausdruck finden, also insbesondere in deren Strafraumen und gegebenenfalls in tatbestandlich umschriebenen oder in einem Qualifikationstatbestand enthaltenen Begehungsmerkmalen und Tatfolgen (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 205 f.).

Insofern wird in Nummer 3 auf die in § 20a Absatz 3 genannten besonders gewichtigen Rechtsgüter Bezug genommen, die bereits für eine Übermittlung nachrichtendienstlich erhobener personenbezogener Daten für Zwecke der Gefahrenabwehr einschlägig sind. Insoweit werden mit der freiheitlichen demokratischen Grundordnung, dem Bestand und der Sicherheit des Bundes oder eines Landes sowie bestimmten auf das Verhältnis zum Ausland gerichteten Interessen der Bundesrepublik (vgl. § 20a Absatz 3 Nummer 1 und 2) besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft bezogen (so ausdrücklich BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 208).

Auch die weiteren in § 20a Absatz 3 Nummer 3 und 4 genannten besonders gewichtigen Rechtsgüter weisen eine besondere Bedeutung für die Rechtsgemeinschaft auf. Dies gilt aus der Natur der Sache heraus nicht nur für die Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, sowie Sachen von bedeutendem Wert und bedeutende Vermögenswerte, deren Erhaltung im besonderen öffentlichen Interesse geboten ist, sondern auch für die Individualrechtsgüter Leben sowie – bei einer erheblichen Gefährdung im Einzelfall – die körperliche Integrität und die Freiheit einer Person. Denn auch diese Rechtsgüter haben vor dem Hintergrund der staatlichen Schutzpflichten, dem damit zusammenhängenden Aufgabenkanon der Sicherheitsbehörden sowie – mit Blick auf die Strafverfolgung – unter dem Gesichtspunkt der Generalprävention eine besondere Bedeutung für die Rechtsgemeinschaft.

Neben der Berücksichtigung des Strafrahmens, des jeweils zu schützenden Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft sind nach den Vorgaben des Bundesverfassungsgerichts aber auch die ein besonderes Unrecht indizierenden tatbestandlich umschriebenen Begehungsformen und Tatfolgen in den Blick zu nehmen. In dieser Hinsicht ist allerdings eine katalogmäßige Auflistung der infrage kommenden Straftatbestände nicht zielführend, da die mit den Bestrebungen nach § 5 Absatz 1 Satz 1 Nummer 1, 3 und 4 erfassten Phänomenbereiche, die in diesen Phänomenbereichen agierenden Beobachtungsobjekte und die jeweiligen Beobachtungsszenarien zu vielgestaltig sind, um sie mit einem abschließenden Katalog infrage kommender besonders schwerer Straftaten abbilden zu können.

Das Bundesverfassungsgericht hat zwar ausgeführt, dass besonders schwere Straftaten im Zuge von Übermittlungsbefugnissen in der Regel durch Straftatenkataloge näher zu konkretisieren sind (BVerfGE 154, 152 Rn. 221). Unter Hinweis auf den Beurteilungsspielraum des Gesetzgebers bei der Bestimmung des Unrechtsgehalts eines Delikts hat das Gericht aber auch gebilligt, dass neben einem Straftatenkatalog hinsichtlich der Schwere der Tat ergänzend auch eine Einzelfallbetrachtung hinzutreten kann und insofern kein Verstoß gegen das Bestimmtheitsgebot vorliegt (so zu § 100a StPO: BVerfG 129, 208 Rn. 203, 208, zu § 100c StPO: BVerfGE 109, 279 Rn. 234, zum Rückgriff auf gespeicherte Verkehrsdaten: BVerfGE 125, 260 Rn. 229).

Insofern kommt es nach Absatz 2 Nummer 3 neben der Berücksichtigung des Mindesthöchststrafrahmens von fünf Jahren und dem Bezug zu einem besonders gewichtigen Rechtsgut im Sinne des § 20a Absatz 3 darauf an, ob die in Betracht kommende Straftat im Einzelfall aufgrund der tatbestandlich umschriebenen Begehungsformen und Tatfolgen als besonders schwer qualifiziert werden kann. Sofern im Tatbestand einer Strafrechtsnorm oder eines Qualifikationstatbestandes gesetzlich umschrieben, könnte in dieser Hinsicht etwa auf die Schutzwürdigkeit (sonstiger) verletzter Rechtsgüter, den Grad der Bedrohung der Allgemeinheit, die Art der Begehung der Tat, die Anzahl der Geschädigten (etwa bei gemeingefährlichen Straftaten) und/oder das Ausmaß des Schadens sowie die Folgen der Tat für die betroffenen Rechtsgüter abgestellt werden (vgl. BVerfGE 129, 208 Rn. 208; BVerfGE 109, 279 Rn. 235). Die in Betracht kommenden Strafnormen müssen dabei allerdings einer objektivierten Betrachtung unterzogen werden; weder die Qualifizierung als Staatsschutzdelikt (§§ 74a, 120 des Gerichtsverfassungsgesetzes) noch die alleinige Bezugnahme auf Verfassungsschutzgüter können die besondere, deutlich über dem Durchschnitt liegende Schwere des jeweiligen Straftatbestandes begründen (BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 – Rn. 202, 208).

Im Hinblick auf die insbesondere für die Abfassung dieser Vorschrift maßgebliche Rechtsprechung des Bundesverfassungsgerichts wird auf den nachfolgend wiedergegebenen Beschluss der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 27. Januar 2025 zum Tagesordnungspunkt „Innere Sicherheit angesichts der Anschläge von Aschaffenburg, Magdeburg, Mannheim und Solingen“ unter Ziffer 8 hingewiesen:

- „8. Sie nimmt Bezug auf den Beschluss der IMK in ihrer Sitzung vom 12. bis 14. Juni 2017 zu TOP 34 und betont mit Nachdruck, dass eine Intensivierung des Informationsaustauschs zwischen den Sicherheitsbehörden zur effektiven Abwehr von Terrorakten und anderen schwerwiegenden Bedrohungen, die auf eine Destabilisierung des Gemeinwesens zielen oder dazu beitragen, unverzichtbar ist.



- a) Sie stellt fest, dass die Rechtsprechung des Bundesverfassungsgerichts in den vergangenen Jahren der informationellen Zusammenarbeit einen immer engeren Rahmen vorgegeben hat. Vor allem für die Übermittlung nachrichtendienstlich erlangter Informationen an Polizei- und Strafverfolgungsbehörden hat die Rechtsprechung sehr hohe und im internationalen Vergleich einzigartige Hürden aufgestellt. Damit wird eine Zusammenführung der bei verschiedenen Sicherheitsbehörden vorliegenden Informationen zur umfassenden Bewertung der von einzelnen Personen und Gruppierungen ausgehenden Sicherheitsgefährdung erschwert.
- b) Die IMK weist darauf hin, dass im Grundgesetz die Zusammenarbeit zwischen Nachrichtendiensten und Polizeibehörden des Bundes und der Länder ausdrücklich vorausgesetzt wird.
- c) Sie spricht sich vor diesem Hintergrund dafür aus, eine Klarstellung durch den verfassungsändernden Gesetzgeber dahingehend zu prüfen, dass diese Zusammenarbeit auch den Informationsaustausch umfasst. Auf diesem Weg könnten die Sicherheitsbehörden von Bund und Ländern auch verfassungsrechtlich verpflichtet werden, zum Schutz von besonders gewichtigen Rechtsgütern, insbesondere von Leib und Leben sowie den Existenzgrundlagen des Staates, eng zusammenzuarbeiten, und die dafür geltenden Anforderungen an den Informationsaustausch konkretisiert werden.“

#### **Zu § 20d – Übermittlung an inländische öffentliche Stellen ohne belastende Maßnahmen mit Außenwirkung**

Die durch eine Datenübermittlung drohenden Anschlussmaßnahmen durch die empfangenden Stellen mit mehr oder weniger gewichtigen Eingriffen in grundrechtlich geschützte Positionen sind nur gerechtfertigt, wenn dies der Abwehr einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut dient (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 235 ff.). Von dem Erfordernis einer konkretisierten Gefahr für ein solches Rechtsgut kann nur ausnahmsweise abgewichen werden. Dies ist der Fall, wenn durch die Übermittlung veranlasste, belastende Anschlussmaßnahmen durch die empfangende Stelle gegenüber der betroffenen Person ausgeschlossen sind und damit die vom Bundesverfassungsgericht in seiner Folgenbetrachtung ausgeführten Rechtsnachteile bei dieser Person nicht eintreten können.

Vor dem Hintergrund, dass die übermittelten Daten nicht zulasten der betroffenen Person außenwirksam eingreifend genutzt werden dürfen, regelt § 20d Datenübermittlungen einerseits für die nachrichtendienstliche Aufgabenwahrnehmung selbst (Absatz 1) und andererseits solche für die informationelle Kooperation etwa zur Erstellung gemeinsamer Erkenntnisprodukte der Gefahrerforschung (Absatz 2).

#### **Zu § 20d Absatz 1**

Nach § 20d Absatz 1 Satz 1 dürfen mit nachrichtendienstlichen Mitteln erhobene personenbezogene Daten an öffentliche Stellen übermittelt werden, wenn dies aufgrund tatsächlicher Anhaltspunkte zur Aufklärung einer beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 5 erforderlich ist. Die Zielrichtung der Datenübermittlung dient damit allein der Verbesserung der Erkenntnislage der Verfassungsschutzbehörde. Wurden die Informationen im Hinblick auf eine erheblich beobachtungsbedürftige Bestrebung oder Tätigkeit erhoben, so darf nach Absatz 1 Satz 2 auch die Weiterleitung nur zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit erfolgen.

**Zu § 20d Absatz 2**

Gemäß § 20d Absatz 2 darf eine Übermittlung nachrichtendienstlich erhobener personenbezogener Daten an öffentliche Stellen zur Erfüllung von Aufgaben erfolgen, die die empfangende Stelle ohne unmittelbar außenwirksame Maßnahmen zulasten der betroffenen Person wahrnimmt. Voraussetzung ist, dass die Übermittlung aufgrund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz der Schutzgüter nach § 20a Absatz 3 vor Bestrebungen oder Tätigkeiten nach § 5 Absatz 1 erforderlich ist.

Zum Verständnis, was unter „unmittelbar außenwirksamen Maßnahmen zulasten betroffener Personen“ zu verstehen ist, kann auf verwaltungsverfahren- und verwaltungsvollstreckungsrechtliche Maßstäbe zurückgegriffen werden. Bezug genommen wird auf für das Vorliegen eines Verwaltungsaktes konstitutive Merkmal der Außenwirkung oder die Differenzierung zwischen einem belastenden und begünstigenden Verwaltungsakt.

Im Hinblick auf den in Absatz 2 Satz 2 Nummer 1 normierten Übermittlungszweck der Erforschung und Bewertung der Bedrohung erfasst die Regelung in erster Linie eine Datenübermittlung an gemeinsame Zentren, wie dem Gemeinsamen Terrorismusabwehrzentrum (GTAZ) im Rahmen analytischer Projekte der Sicherheitsbehörden. Zu denken ist hierbei an die Erstellung von Lagebildern zur abstrakten Beschreibung der allgemeinen Gefährdungslage oder Fallanalysen, zur Ermittlung von Vorgehensmustern sowie zur Erstellung allgemeiner Handlungskonzepte, die auf die allgemeine Lagebewertung, nicht aber auf individuelle Anschlussmaßnahmen zielen. Absatz 2 Satz 2 Nummer 2 bezieht sich auf Forschungsvorhaben in Kooperation mit wissenschaftlichen, beispielsweise universitären Forschungseinrichtungen, wobei eine nicht anonymisierte Übermittlung personenbezogener Daten in der Regel allerdings verzichtbar sein dürfte.

**Zu § 20e – Übermittlung an inländische nicht öffentliche Stellen**

§ 20e regelt die Übermittlung personenbezogener Daten gegenüber nicht öffentlichen inländischen Stellen. Eine solche Übermittlung birgt für die betroffene Person gewichtige Risiken. Zwar verfügen nicht öffentliche Stellen nicht über die spezifischen Machtmittel der staatlichen Gewalt. Gleichwohl können sie die rechtlich geschützten Interessen der betroffenen Person empfindlich beeinträchtigen, etwa durch die Vorenthaltung von Leistungen, auf die diese Person für ihre Lebensgestaltung angewiesen ist, oder durch den Ausschluss aus sozialen Zusammenhängen mit hoher Bedeutung für die Persönlichkeitsentfaltung. Zudem unterliegen nicht öffentliche Stellen nicht den rechtsstaatlichen und demokratischen Bindungen und Kontrollen, die für Hoheitsträger gelten und eine Datenübermittlung zur Durchführung hoheitlicher Maßnahmen zumutbar machen. Dementsprechend ist eine solche Übermittlung daher grundsätzlich unzulässig. Den spezifischen Risiken der Datenübermittlung an nicht öffentliche Stellen ist durch begrenzte Ausnahmetatbestände Rechnung zu tragen.

**Zu § 20e Satz 1**

Zulässig sind solche Übermittlungen nur zum Schutz eines der besonders gewichtigen Rechtsgüter nach § 20a Absatz 3 zu den Zwecken der abschließend in § 20e Satz 1 Nummer 1 bis 3 aufgeführten Übermittlungstatbestände.

**Zu § 20e Satz 2**

§ 20e Satz 2 flankiert wegen der besonderen Risiken von Übermittlungen an nicht öffentliche Stellen die Datenübermittlungen durch eine Verwendungsbeschränkung. Die empfangende nicht öffentliche Stelle darf die übermittelten Daten im Rahmen des Übermittlungszwecks grundsätzlich nicht für Handlungen nutzen, die für die betroffene Person eine nachteilige rechtliche Wirkung entfalten (wie etwa die Kündigung eines Vertrages) oder eine andersartige erhebliche Beeinträchtigung bewirken. Solche Handlungen setzen vielmehr eine zumindest konkretisierte Gefahr für ein Rechtsgut gemäß § 20a Absatz 3 voraus und sind grundsätzlich an eine vorherige Zustimmung der Verfassungsschutzbehörde gebunden. In einer akuten Krisenlage (unmittelbar bevorstehende Gefahr) kann auf die vorherige Zustimmung verzichtet werden, da ansonsten die Abwendung der Gefahr vielfach nicht mehr möglich wäre. Stattdessen hat die empfangende Stelle die Verfassungsschutzbehörde unverzüglich über den Sachverhalt zu unterrichten.

**Zu § 20e Satz 5**

Satz 5 postuliert aufgrund der potenziell weitreichenden Folgen der Übermittlung für eine betroffene Person eine Mitteilungspflicht als Ausfluss des Grundrechts auf informationelle Selbstbestimmung und zur Garantie eines effektiven Rechtsschutzes nach Artikel 19 Absatz 4 GG.

**§ 20f – Projektbezogene gemeinsame Dateien**

Es handelt sich um eine Folgeänderung aufgrund der neu eingefügten §§ 20a bis 20e.

**§ 20g – Minderjährigenschutz bei Inlandsübermittlung****Zu § 20g Satz 1**

Minderjährige bedürfen eines besonderen Schutzes, der spezifische Aspekte der Jugendphase berücksichtigt. So wie § 16 eine Verarbeitung personenbezogener Daten Minderjähriger nur unter besonders strengen Voraussetzungen ermöglicht, gilt dies erst recht für eine Übermittlung der Daten. Gemäß § 20g Satz 1 gilt ein Verbot der Übermittlung unter Erlaubnisvorbehalt gemäß den Bedingungen der Sätze 2 und 3.

**Zu § 20g Satz 2**

Grundsätzlich ist nach Satz 2 eine Übermittlung ausnahmsweise nur dann möglich, wenn die Übermittlung nicht zu einer belastenden Maßnahme mit Außenwirkung für die minderjährige Person führt sowie bei einer Übermittlung an eine nicht öffentliche Stelle die Zwecke des § 20e Satz 1 Nummer 3 Buchstabe e bis g erreicht werden sollen.

**Zu § 20g Satz 3 Nummer 1**

Hinsichtlich von Daten minderjähriger Personen, die das 14. Lebensjahr vollendet haben, gelten mit Satz 3 Nummer 1 Buchstabe a und c dieselben strengen Übermittlungsvoraussetzungen wie für volljährige Personen. Bei Datenübermittlungen zum präventiven Rechtsgüterschutz erfolgt hingegen eine Beschränkung auf den Übermittlungsanlass „Überprüfung der Verfassungstreue von Personen, die eine Tätigkeit im öffentlichen Dienst anstreben oder in diesem beschäftigt sind“ oder zu Zwecken der Strafvollstreckung (Satz 2 Nummer 1 Buchstabe b in Verbindung mit § 20b Nummer 1 und 8).

**Zu § 20g Satz 3 Nummer 2**

Für minderjährige Personen, die noch nicht das 14. Lebensjahr vollendet haben, gelten für Übermittlungen strengere Voraussetzungen. Hier muss nach den Umständen des Einzelfalls darauf geschlossen werden können, dass von der betroffenen Person eine Gefahr für Leib oder Leben einer Person sowie für Einrichtungen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages ausgeht (Satz 3 Nummer 2 Buchstabe a und b). Hat sich eine solche Gefahr bereits konkretisiert, ist die Übermittlung erst recht möglich. Die Regelung trägt dem Umstand Rechnung, dass zunehmend Fälle bekannt werden, in denen sich bereits unter 14-jährige Personen innerhalb kürzester Zeit radikalisierten und teils auch bereit sind, Anschläge zu verüben.

**Zu § 21 – Informationsübermittlung an ausländische Stellen**

Der neu formulierte § 21 dient der Umsetzung der durch das BVerfG im Hinblick auf die Übermittlung an ausländische Stellen aufgestellten Anforderungen (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 260 ff.), auch wenn die Norm einen äußerst geringen Praxisbezug aufweist. Für die Übermittlung an ausländische öffentliche Stellen gelten danach die gleichen Voraussetzungen wie für die Übermittlung im Inland (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 261). Absatz 1 verweist daher auf die entsprechenden Regelungen in §§ 20a bis 20e, um den Anforderungen des Kriteriums der hypothetischen Datenneuerhebung auch bei Übermittlungen an ausländische Stellen Rechnung zu tragen.

In Übereinstimmung mit dem genannten Urteil regelt Absatz 2, dass eine Übermittlung der Daten an ausländische Stellen unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland dem entgegenstehen oder ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrer Umgang mit den Daten bei der empfangenden Stelle nicht hinreichend gesichert ist (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 266).

Schutzwürdige Betroffeneninteressen sind dabei insbesondere aus grundrechtlicher und rechtsstaatlicher Perspektive zu beurteilen, wobei deren elementare Anforderungen – speziell die Achtung der Menschenwürde, etwa mit dem Folterverbot – absolute, abwägungsfeste Schranken bilden. Von einem angemessenen Datenschutzniveau kann jedenfalls bei Staaten ausgegangen werden, welche die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsabkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden.

Die gesetzlich geforderte Menschenrechtsgewährleistung kann im Empfängerstaat entweder allgemein gesichert sein oder im Einzelfall durch Abreden (oder implizit mit dem Ausschluss operativer Anschlussmaßnahmen), die dazu allerdings verlässlich sein müssen (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 267 ff.).

Absatz 3 regelt eine potenzielle Übermittlung oder Weiterverarbeitung der übermittelten Daten durch die ausländische Stelle.

Absatz 4 Satz 1 schließt die Übermittlung von personenbezogenen Daten minderjähriger Personen vorbehaltlich der Sonderregelungen der Sätze 3 bis 4 aus.

Absatz 5 ermöglicht eine ausnahmsweise Übermittlung auch an nicht öffentliche Stellen.

## **§ 22 – Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen und Übermittlung zum Schutz der Betroffenen**

### **Zu § 22 Absatz 1**

Die Vorschrift des § 22 Absatz 1 regelt die Übermittlung personenbezogener Daten an öffentliche Stellen, wenn die Daten nicht mit nachrichtendienstlichen Mitteln erhoben wurden oder allgemein zugänglich sind (z. B. Daten aus gespeicherten Presseartikeln). In diesen Fällen besteht die Gefahr einer Umgehung spezifischer Datenerhebungsvoraussetzungen nicht, sodass eine Datenübermittlung in diesen Fällen auch unterhalb der verfassungsgerichtlich definierten Übermittlungsschwellen in Betracht kommt. Das BVerfG hat ausdrücklich erklärt, dass seine strengen Vorgaben nur für die Übermittlung von personenbezogenen Daten gelten, die mit nachrichtendienstlichen Mitteln erhoben wurden (BVerfG, Urteil v. 26. April 2022 – 1 BvR 1619/17 – Rn. 234 ff.). Für die Zulässigkeit der Übermittlung genügt es somit, dass die Daten für die Erfüllung eigener gesetzlicher Aufgaben der Verfassungsschutzbehörde oder solcher der empfangenden Stelle erforderlich sind.

### **Zu § 22 Absatz 2**

Absatz 2 regelt die Übermittlung von personenbezogenen Daten, die durch die Verfassungsschutzbehörde besonders erhoben oder verarbeitet worden sind. Die Übermittlung richtet sich dann nach den Vorschriften der §§ 20a bis 21 und 23.

### **Zu § 22 Absatz 3**

Die Regelung des Absatzes 3 soll dem Schutz betroffener Personen auch in atypischen – insofern von den vorausgegangen Übermittlungsvorschriften noch nicht zureichend abgedeckten – Fällen verbessert Rechnung tragen. Ein solcher Fall ist beispielsweise die Übermittlung von Informationen, die einen Beschuldigten in einem Strafverfahren entlasten. Die vom Bundesverfassungsgericht vorgegebenen hohen deliktsbezogenen Übermittlungsvoraussetzungen (nur bei besonders schweren Straftaten) dienen ihrerseits dem Schutz betroffener Personen vor belastenden Übermittlungen, sind also bei begünstigenden Übermittlungen nicht einschlägig.

Ähnliche Friktionen zwischen allgemein zum Betroffenenenschutz aufgestellten Übermittlungsvoraussetzungen und einer im Einzelfall für den Betroffenen vorteilhaften Übermittlung sind auch in anderen Bereichen denkbar, etwa bei der Gefahrenabwehr Hinweise, wonach die betroffene Person unbeteiligt ist, mithin gegen sie keine Maßnahmen als Störer zu richten sind.

Eingeschlossen ist eine rechtsklare Übermittlungsgrundlage zur Information der Jugendhilfe, etwa in Fällen der Rückkehrer, die in den nahöstlichen Krisenregionen in terroristische Strukturen eingebunden waren. Dabei handelte es sich teilweise um Familien mit Kindern, die dort geboren worden sind, bei Rückkehr nach Deutschland angesichts der besonderen familiären Zusammenhänge aber womöglich besonderer staatlicher Fürsorge bedürfen.

Grundsätzlich hat die Klärung des tatsächlichen Willens der betroffenen Person, also die Einholung einer Einwilligung, Vorrang. Dann enthält § 9 Absatz 1 Satz 2 zweiter Halbsatz die Übermittlungsgrundlage. Typischerweise wird es der Verfassungsschutzabteilung jedenfalls zum Schutz seiner operativen Belange nicht möglich sein, offen auf die betroffene Person zuzugehen und ihr Behördenwissen zu offenbaren. Im Falle der Jugendhilfe kann im Übrigen gerade ein Sachverhalt übermittlungsveranlassend sein, wonach das Kind Schutz gegenüber dem Personensorgeberechtigten benötigt. Insofern ist Satz 2 auch *lex specialis* gegenüber Satz 1, da hier nicht auf den mutmaßlichen Willen des betroffenen Minderjährigen bzw. der personensorgeberechtigten Person abzustellen ist.

## **§ 23 – Protokollierung der Übermittlungen und weitere Verfahrensregelungen**

### **Zu § 23 Absatz 1**

Die in Absatz 1 geregelte Protokollierung ist vom Bundesverfassungsgericht vorgegeben (BVerfG, Beschluss vom 28. September 2022 – 1 BvR 2354/13 – Rn. 107, 138, 160). Die Protokollierungspflicht ist unabhängig davon, wie die Übermittlung erfolgt, bezieht also auch mündliche Auskünfte ein. Hierbei muss der Gegenstand der Übermittlung, aber nicht der nähere Inhalt festgehalten werden.

Die Auswertbarkeitsmaßgabe in Satz 2 trägt dem Zweck der Regelung Rechnung, Kontrollen zu erleichtern. Sie geht hierzu über die bereits im geltenden Recht enthaltene allgemeine Dokumentationspflicht hinaus (siehe den bisherigen § 23 Satz 1) und ermöglicht damit gezielte Kontrollen u. a. auch zu den nach der Verfassungsrechtsprechung sensiblen Übermittlungen nach § 20a, an die sich operative Zwangsmaßnahmen anschließen können, um die hierfür geltenden besonderen Voraussetzungen zu prüfen.

Für die Weiterverarbeitung unterscheidet Satz 3 danach, ob die Daten ausschließlich zu Kontrollzwecken gespeichert werden. In diesen Fällen sind die Daten nach einer für eine Kontrolle geeigneten Frist zu löschen. Üblicherweise erfolgt die Dokumentation von Übermittlungen allerdings originär für Fachzwecke, um für die weitere Aufgabenwahrnehmung nachvollziehbar zu halten, wer welche Information erhalten hat.

**Zu § 23 Absatz 2**

Absatz 2 regelt spezielle Fallgestaltungen wie etwa die Weitergabe technischer Aufzeichnungen, etwa der Videodatei einer Observation, die typischerweise auch unbeteiligte Dritte im öffentlichen Raum erfasst, die unter Umständen bestimmbar wären, sodass es sich hierbei um personenbezogene Daten handeln kann. Ein weiterer Bedarfsfall kann die Ermöglichung wissenschaftlicher Forschung auf Basis einschlägiger Vorgänge sein. Hier wäre typischerweise eine datumsscharfe Vorselektion durch die Behörde mit untragbaren Aufwänden verbunden, unter Umständen auch für das Forschungsvorhaben methodisch unzutraglich.

**Zu § 23 Absatz 3**

Absatz 3 regelt das Entscheidungsverfahren für Übermittlungen an nicht öffentliche Stellen sowie die Mitteilungspflicht an den Betroffenen in diesen Fällen.

**Zu Nummer 18 (§ 24 Informationsübermittlung durch öffentliche Stellen an die Verfassungsschutzbehörde)****Zu Buchstabe a – Absatz 1 Satz 1**

Die Einfügung stellt klar, dass der Verfassungsschutz nicht nur selektierte Daten, sondern auch Übermittlung von Unterlagen zur Auswertung verlangen kann.

**Zu Buchstabe b – Absatz 3**

Die Einfügung stellt klar, dass die Regelung nicht nur Daten, sondern auch Unterlagen betrifft. Darüber hinaus erfolgt eine rechtsförmliche Änderung.

Die Regelung des bisherigen Satzes 4 entspricht nicht mehr der jüngsten Rechtsprechung des Bundesverfassungsgerichts und kann daher entfallen.

**Zu Buchstabe c – Absatz 5 Satz 3**

Es handelt sich um eine Änderung zur Anpassung an die Begriffsbestimmungen in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung.

**Zu Nummer 19 (§ 24a Informationsübermittlung durch nicht öffentliche Stellen an die Verfassungsschutzbehörde, Ersuchen an das Bundeszentralamt für Steuern)**

Nach dem Grundsatz „Revision statt Binnenrevision“ sollen grundsätzlich ganze Gliederungseinheiten ersetzt und nur noch ausnahmsweise Einzeländerungen innerhalb von Gliederungseinheiten vorgenommen werden. Vor diesem Hintergrund wird § 24a vollständig ersetzt.

**Zu Absatz 1**

Das in Bezug genommene Gesetz ist 2021 unter dem Namen Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Kraft getreten und wurde 2024 umbenannt, um das deutsche Recht an die Terminologie „digitaler Dienst“ der europäischen Verordnung anzupassen. Es handelt sich somit hier um eine Folgeänderung im LVerfSchG M-V.

Außerdem wird Absatz 1 hinsichtlich der Eingriffsschwelle an die Rechtsprechung des Bundesverfassungsgerichts angepasst (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 – Rn. 330 f.), wonach die Eingriffsschwelle an die Beobachtungsbedürftigkeit von Bestrebungen anzuknüpfen hat. Die bisherige Regelung stellte auf schwerwiegende Gefahren ab, was nach aktueller Rechtsprechung systematisch falsch ist. Denn der Verfassungsschutz ist im Gefahrenvorfeld tätig. Dementsprechend wird für die Maßnahmen nach Absatz 1 erhebliche Beobachtungsbedürftigkeit verlangt.

**Zu Absatz 2**

Aufgrund § 93 Absatz 8 Satz 1 Nummer 3 der Abgabenordnung wird den Ländern die Möglichkeit eröffnet, über eigene Landesregelungen die Befugnis zu schaffen, dass die Verfassungsschutzbehörden der Länder Kontostammdatenauskünfte erhalten. Durch den neuen § 24a Absatz 2 werden diese Befugnis und die notwendigen Voraussetzungen normiert.

**Zu Absatz 3**

Es handelt sich sowohl um rechtsförmliche Änderungen als auch um eine komplementäre Einfügung zu Buchstabe c.

**Zu den Absätzen 4 bis 8**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache, die Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde und eine rechtsförmliche Änderung.

**Zu Absatz 9**

Es handelt sich um eine Folgeänderung aufgrund des neu eingefügten Absatzes 2.

**Zu Nummer 20 (§ 24b Auskunftsverlangen zu Bestandsdaten)****Zu Buchstabe a – § 24b Absatz 1**

Vgl. Begründung zu Nummer 19 (zu § 24a Absatz 1).



**Zu Buchstabe b – § 24b Absatz 3**

Es handelt sich um eine Folgeänderung aufgrund des eingefügten neuen § 24a Absatz 2.

**Zu Nummer 21 (§ 25 Übermittlungsverbote, Nachberichtspflicht)****Zu Buchstabe a – § 25 Absatz 1**

Die Übermittlungsverbote werden an die neuen Übermittlungsregelungen angepasst. Verbessert wird die Bestimmtheit der Norm bezüglich der Regelungen zur Verhältnismäßigkeit (Satz 1 Nummer 2) sowie zur Abwägung kollidierender Sicherheitsinteressen (Satz 1 Nummer 3). Es werden jeweils abwägungsleitende Vorgaben präzisiert.

Satz 1 Nummer 1 verdeutlicht den Spezialitätsgehalt gerade der besonderen Zweckbindungen, die zur Weiterverarbeitung von Daten gelten, die mit besonders intensiven Eingriffen gewonnen worden sind. Eine solche Regelung enthält beispielsweise § 4 Absatz 4 G 10.

Soweit zu gewichtig eingreifenden Befugnissen keine besonderen Übermittlungsbeschränkungen bereits abstrakt im Gesetz vorgegeben sind, wirkt einerseits bereits die hohe Zweckhürde in § 20a Absatz 1 bzw. § 20c begrenzend. Zudem sind die Erhebungsumstände im Rahmen der konkreten Verhältnismäßigkeitswürdigung im Einzelfall zu betrachten (Nummer 2 Buchstabe c).

In Satz 1 Nummer 2 werden mit den Buchstaben b, d und e typischerweise verhältnismäßigkeitsrelevante Gesichtspunkte neu aufgenommen. Buchstabe b berücksichtigt, dass der Aussagegehalt von Informationen mit Zeitablauf gemindert sein kann, speziell bei Minderjährigen angesichts deren Persönlichkeitsreifung. Buchstabe d beruht auf der Abschätzung, dass bei Anschlussmaßnahmen, die bereits auf noch nicht abschließend geklärter Sachverhaltsgrundlage erfolgen, ein spezifisches Risiko informationeller Fehlsteuerung besteht (wobei diese Risikolage allerdings typischerweise im jeweiligen Fachrecht mit der jeweiligen Befugnisgestaltung – Eingriffe bereits mit Verdachtserkenntnissen zu rechtfertigen – bewältigt wird).

Die Nummern 3 und 4 weisen darauf hin, zwischen Übermittlungszweck und kollidierenden Sicherheitsinteressen abzuwägen. Nummer 3 regelt die Kollision mit besonders gewichtigen Individualrechtsgütern. Diese sollen besonders geschützt werden. Deshalb erfolgt hier eine Abwägung nur, wenn die Übermittlung ebenso dem Individualrechtsgüterschutz dient. Nummer 4 enthält im zweiten Halbsatz zusätzlich eine abwägend gewichtende Vorstrukturierung zur Relevanz von Sicherheitsbelangen.

**Zu Buchstabe b – § 25 Absatz 2**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache.

**Zu Nummer 22 (§ 26 Auskunft an betroffene Personen)****Zu Buchstabe a – § 26 Absatz 1 Satz 2**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache.

**Zu Buchstabe b – § 26 Absatz 2 Satz 2**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache.

**Zu Buchstabe c – § 26 Absatz 4**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache.

**Zu Nummer 23 (§ 27 Parlamentarische Kontrollkommission)**

Es handelt sich um eine rechtsförmliche Änderung.

**Zu Nummer 24 (§ 28 Geheimhaltung)**

§ 28 wird vollständig ersetzt<sup>1</sup>.

**Zu Absatz 1**

Die Angabe in Satz 1 „öffentlicher und nicht öffentlicher“ stellt klar, dass die gesamte Sitzung der Parlamentarischen Kontrollkommission bei Bedarf öffentlich stattfinden kann und nicht nur – wie Absatz 2 Satz verstanden werden kann – in einzelnen Teilen die Öffentlichkeit hergestellt werden kann.

Mit Blick auf die in § 28 Absatz 1 Satz 4 konkretisierte Möglichkeit der Einbeziehung von Kommissionspersonal ist eine Ergänzung in Absatz 1 Satz 2 hinsichtlich der Geheimhaltung erforderlich.

Die Geheimhaltungspflicht des Satzes 2 gilt auch für die Beschäftigten über die Beendigung ihrer Tätigkeit hinaus.

Da § 27 Absatz 3 Satz 3 gewährleistet, dass der Kommission das notwendige Personal zur Verfügung gestellt wird, sind diesbezüglich weitere Maßgaben erforderlich. Die Sätze 4 und 5 stellen sicher, dass die Anforderungen des personellen Geheimschutzes erfüllt werden, da die Beschäftigten in hohem Maße mit geheimhaltungsbedürftigen Angelegenheiten im Sinne von § 1 Absatz 1 bis 3 SÜG M-V umgehen. Ebenso sind der Klarheit halber gemäß Satz 6 die Aufgaben und Befugnisse der Beschäftigten zu regeln. Da bisher schon organisatorische Einzelheiten der Sitzungen in der Geschäftsordnung der Kommission – so u. a. das Recht auf Teilnahme – normiert sind, sollte diese um die weiteren Maßgaben ergänzt werden.

**Zu den Absätzen 2 und 3**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache und die Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde.

**Zu Nummer 25 (§ 29 Kontrollrechte der Parlamentarischen Kontrollkommission)****Zu Buchstabe a – § 29 Absatz 1 Satz 1**

Es handelt sich um eine Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde und eine rechtsförmliche Änderung.

**Zu Buchstabe b – § 29 Absatz 2**

Es handelt sich um eine Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde, die Korrektur der Behördenbezeichnung und eine rechtsförmliche Änderung.

**Zu Buchstabe c – § 29 Absatz 3**

Es handelt sich um eine Anpassung des Gesetzestextes an die geschlechterneutrale Sprache und die Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde.

**Zu Buchstabe d – § 29 Absatz 4**

Es handelt sich um eine Umstellung des Gesetzestextes auf eine neutrale Bezeichnung der obersten Landesbehörde.

**Zu Nummer 26 (§ 29a Eingaben)**

Die Expertenkommission für den Verfassungsschutz, die vom seinerzeitigen Minister für Inneres und Europa am 19. Januar 2021 zur strukturellen Untersuchung der Abteilung für Verfassungsschutz eingesetzt wurde, schlug mit Abschlussbericht vom 14. Mai 2021 vor, „ein Petitionsrecht von Mitarbeiterinnen und Mitarbeitern des Verfassungsschutzes gegenüber der Parlamentarischen Kontrollkommission“ einzuführen.

Mit Absatz 1 wird ein solches Recht eingeführt sowie die Vertraulichkeit einer solchen Eingabe gegenüber der Parlamentarischen Kontrollkommission und die Möglichkeit einer Stellungnahme durch die zuständige Ministerin oder den Minister sichergestellt.

Gemäß Absatz 2 wird die Geheimhaltung durch Verweisung auf die entsprechende Regelung der Parlamentarischen Kontrollkommission in § 28 geregelt.

Absatz 3 normiert, dass auch sonstige an den Landtag gerichtete Eingaben den Verfassungsschutz betreffend der Kontrollkommission bekannt gegeben werden.

**Zu Nummer 27 (§§ 30 bis 33)**

Die folgenden §§ 30 bis 33 werden zusammengefasst<sup>1</sup>:

**Zu § 30 – Anwendung des allgemeinen Datenschutzrechts**

Das LVerfSchG M-V regelt die Rechtsgrundlagen für die Tätigkeit der Verfassungsschutzabteilung. Die Funktionsfähigkeit des Verfassungsschutzes muss dabei aber im Einklang stehen mit den Rechten der betroffenen Personen und hierbei insbesondere dem Schutz der personenbezogenen Daten. Insofern können die Vorschriften des LVerfSchG in großen Teilen auch als spezielles Datenschutzrecht verstanden werden. Soweit das allgemeine Datenschutzrecht dadurch nicht verdrängt wird, findet es Anwendung.

**Zu § 30 Absatz 1**

So weist § 30 Absatz 1 auf § 2 Absatz 3 DSG M-V hin, wonach das Datenschutzgesetz des Landes anzuwenden ist, soweit der Verfassungsschutz allgemeine Verwaltungsaufgaben wahrnimmt.

**Zu § 30 Absatz 2**

Darüber hinaus verweist Absatz 2 auf eine Reihe weiterer Normen des Bundesdatenschutzgesetzes, die im Hinblick auf die fachliche Aufgabenerfüllung des Verfassungsschutzes entsprechende Anwendung finden:

- §§ 5 bis 7 (Datenschutzbeauftragte öffentlicher Stellen)
- § 46 (Begriffsbestimmungen)
- § 47 (Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten)
- § 51 Absatz 1 bis 4 (Einwilligung)
- § 52 (Verarbeitung auf Weisung des Verantwortlichen)
- § 53 (Datengeheimnis)
- § 54 (Automatisierte Einzelentscheidung)
- § 62 (Auftragsverarbeitung)
- § 64 (Anforderung an die Sicherheit der Datenverarbeitung)
- § 65 (Meldungen von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten)
- § 69 (Anhörung der oder des Bundesbeauftragten)
- § 71 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)
- § 83 (Schadensersatz und Entschädigung)
- § 84 (Strafvorschriften)

**Zu § 31 – Unabhängige Datenschutzkontrolle****Zu § 31 Absatz 1**

§ 31 Absatz 1 begründet das Jedermannsrecht, sich wegen einer behaupteten Verletzung seiner Datenschutzrechte durch die Verarbeitung personenbezogener Daten beim Verfassungsschutz an die Landesbeauftragten oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu wenden.

**Zu § 31 Absatz 2**

Nach Absatz 2 Satz 1 kontrolliert die oder der Beauftragte „die Einhaltung der Vorschriften über den Datenschutz“ und berät den Verfassungsschutz entsprechend. Kontroll- und Beratungsgegenstand sind nicht allein die personenbezogenen Daten, sondern der Umgang mit diesen am Maßstab der anzuwendenden Datenschutzvorschriften. Satz 3 soll für den Regelfall eine Doppelzuständigkeit mit der G-10-Kommission verhindern, schließt sie aber grundsätzlich nicht aus.

**Zu § 31 Absatz 3**

Absatz 3 Satz 1 und 2 regeln die einzelnen Unterstützungspflichten durch die Verfassungsschutzbehörde, während Satz 3 im Einzelfall dem für den Verfassungsschutz zuständigen Ministerium eine Widerspruchsmöglichkeit aufzeigt.

**Zu § 31 Absatz 4**

Absatz 4 stellt klar, dass die Regelungen der Absätze 1 bis 3 die gesamte Aufgabewahrnehmung der Verfassungsschutzbehörde einbeziehen (Satz 1). Speicherungen beispielsweise in der Antiterrordatei sind ebenso umfasst wie Angelegenheiten der Personalverwaltung und die Tätigkeiten Dritter für Aufgaben der Verfassungsschutzbehörde (Satz 2), z. B. im Rahmen von Übermittlungen nach § 24.

**Zu § 32 – Maßnahmen zur Sicherung von Verschlusssachen**

Die Tätigkeit des Verfassungsschutzes beruht in hohem Umfang auf Verschlusssachen. Verschlusssachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform (§ 2 Absatz 1 Satz 1 SÜG M-V). Insbesondere materielle Verschlusssachen – Dokumente und elektronische Speichermedien – bedürfen eines hohen Schutzes, um Informationsabflüsse zu vermeiden. Im Vordergrund der Vorschriften der §§ 32 und 33 steht – über das Hausrecht hinaus – die räumliche Sicherung der Dienststelle, indem spezifische Befugnisse gesetzlich geregelt werden, zumal durch die erforderlichen Maßnahmen auch die Grundrechte der betroffenen Personen berührt werden.

**Zu § 32 Absatz 1**

§ 32 Absatz 1 definiert mit den Nummern 1 und 2 zunächst als Gegenstand von Sicherungsmaßnahmen die materiellen Verschlusssachen, Geräte der Informations- und Kommunikationstechnik sowie andere gegenständliche Verschlusssachen. Gemäß Absatz 1 Nummer 2 (am Ende) sind Ziel von Sicherungsmaßnahmen aber auch Gegenstände und Geräte, die – ohne Verschlusssachen zu sein – in der Lage sind, negativ im Sinne von Sabotage auf Verschlusssachen einzuwirken.

**Zu § 32 Absatz 2**

Absatz 2 Satz 1 definiert die Möglichkeiten von Personenkontrollen in zweierlei Hinsicht:

Absatz 2 Satz 1 Nummer 1 berechtigt zu verdachtsunabhängigen Kontrollen. Als verdachtsunabhängige Kontrollen sind routinemäßige oder stichprobenhafte Maßnahmen, eventuell unter Einsatz von Mobilfunkdetektoren, zu verstehen.

Wenn demgegenüber Tatsachen die Annahme rechtfertigen, dass zur Sicherung von Verschlussachen dies erforderlich ist, also im Sinne einer verdachtsabhängigen Kontrolle, ermöglicht Absatz 2 Satz 1 Nummer 2 eine Durchsuchung.

**Zu § 32 Absatz 3**

Die verdachtsunabhängige Personenkontrolle nach Absatz 3 Satz 1 ist als „oberflächliche Suche nach Gegenständen an Personen, an und in Taschen, mitgeführten Gegenständen und Fahrzeugen auch unter Einsatz technischer Mittel“ zu verstehen. Herauszuheben ist, dass diese Maßnahmen ausdrücklich ohne Körperkontakt mit den betroffenen Personen stattfinden müssen.

Die (verdachtsabhängige) Durchsuchung ist hingegen gemäß Absatz 3 Satz 2 definiert als „zielgerichtete und planmäßige Suche“ auch unter Einsatz technischer Mittel am äußeren Körper der betroffenen Person, in ihrer Kleidung oder Taschen, an und in Fahrzeugen oder in sonstigen Gegenständen. Eine weitergehende körperliche Untersuchung der betroffenen Person selbst ist in jedem Fall unzulässig und kann nur durch die Polizei nach den hierfür geltenden Vorschriften vorgenommen werden.

**Zu § 32 Absatz 4**

Absatz 4 regelt die zum Schutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten notwendigen Befugnisse zur Sicherstellung und Untersuchung von Gegenständen, gegenüber deren Nutzung tatsächliche Anhaltspunkte einen entsprechenden Verdacht begründen müssen oder die keiner Person zuzuordnen sind. Die Befugnis schließt auch die verdachtsabhängige Durchsuchung verschlossener Gegenstände ein, die zur privaten Nutzung überlassen wurden, wie z. B. Kleiderschränke und Schreibtischfächer.

**Zu § 32 Absatz 5**

Absatz 5 Satz 1 normiert die Mitwirkungspflicht bei Kontrollen und Durchsuchungen nach Absatz 2 für die Personen, die sich im Sicherheitsbereich der Verfassungsschutzabteilung aufhalten, sowie bezüglich der Sicherstellungsmaßnahmen nach Absatz 4. Satz 2 erstreckt komplementär zu Satz 1 die Befugnisse nach den Absätzen 2 und 4 auch auf das unmittelbare Umfeld des Sicherheitsbereichs (zum Begriff siehe § 23 Absatz 1 Nummer 4 und Absatz 2 Nummer 2 des Bundespolizeigesetzes).

**Zu § 32 Absatz 6**

Absatz 6 ermöglicht eine verdachtsunabhängige offene Überwachung innerhalb des Sicherheitsbereiches einschließlich von Diensträumen mit optisch-elektronischen Mitteln. Die Überwachung ist offen, wenn auf sie in geeigneter Weise hingewiesen wird. Die Überwachung muss dem Schutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeit dienen und verhältnismäßig sein. Die Überwachung von Arbeitsräumen, die ausschließlich durch eine bestimmte Person genutzt werden und eine permanente Beobachtung dieser Person ermöglichen würde, sowie die Überwachung von Sanitär- oder Umkleideräumen sind nach Satz 3 ausgeschlossen. Es gelten die weiteren Grundsätze entsprechender Datenaufzeichnung: keine Nutzung zur Leistungskontrolle, strikte Begrenzung der Datenspeicherung auf den erforderlichen Umfang, unverzügliche Löschung nach Nutzung der Daten. Einzelheiten sind in einer Dienstvorschrift zu regeln.

**Zu § 32 Absatz 7**

Absatz 7 beinhaltet eine spezifische Befugnis zum Schutz vor unbemannten Fluggeräten, die sich in unmittelbarer Nähe zum Sicherheitsbereich befinden. Ermöglicht werden dadurch die Detektion und Abwehr (in der Regel durch Übernahme der Steuerung). Für Maßnahmen nach Absatz 7 gelten insbesondere die allgemeinen und spezifischen Verhältnismäßigkeitsvorgaben in Absatz 9.

**Zu § 32 Absatz 8**

Absatz 8 erstreckt die Befugnis zur Durchführung nachrichtendienstlicher Maßnahmen auch auf die Aufklärung sicherheitsgefährdender Tätigkeiten von Beschäftigten der Verfassungsschutzabteilung und sonstiger Personen, die mit sicherheitsempfindlicher Tätigkeit im Hinblick auf Verschlusssachen betraut oder beauftragt sind, im Sicherheitsbereich tätig zu sein. Diese Erweiterung des materiellen Befugnistatbestands ist für Sachverhalte nötig, bei denen die sicherheitsgefährdende Tätigkeit tatbestandlich keine Bedrohung im Sinne von § 5 Absatz 1 darstellt, beispielsweise, wenn Außenstehende geschützte Informationen über Beschäftigte für andere Zwecke, etwa für kommerzielle oder allgemein kriminelle, beschaffen.

**Zu § 32 Absatz 9**

In Absatz 9 wird klarstellend die Verhältnismäßigkeit auch der speziellen Befugnisse nach § 32 betont, die bereits generell in § 7 Absatz 2 für die Tätigkeit der Verfassungsschutzbehörde normiert ist.

**Zu § 33 – Durchführung von Maßnahmen zur Sicherung von Verschlusssachen****Zu § 33 Absatz 1**

Wichtig ist, dass die potenziell von den Maßnahmen betroffenen Personen, also Bedienstete und Besucher der Dienststelle, über den ordnungsgemäßen Umgang mit Verschlusssachen, die möglichen Maßnahmen nach den §§ 32 und 33 und ihre Mitwirkungspflicht informiert werden müssen.

**Zu § 33 Absatz 2**

Absatz 2 regelt die Zuständigkeit für und die Notwendigkeit von Anordnungen der Maßnahmen nach § 32. Diese müssen wie üblich inhaltlich bestimmt sein, d. h. speziell zur Einhaltung der Voraussetzungen der Maßnahme ausführen, und sind nach den Grundsätzen der Aktenführung in der Verwaltung zu dokumentieren.

**Zu § 33 Absatz 3**

Absatz 3 schützt die Interessen der betroffenen Person in Bezug auf sichergestellte Gegenstände. Für Gegenstände, die ausschließlich zur dienstlichen Nutzung überlassen wurden, ist eine Sicherstellung nicht erforderlich; sie werden auch von der Herausgaberegulierung entsprechend nicht erfasst. Der Bezug auf die betroffene Person beinhaltet, dass eine Herausgabe nicht erfolgen muss, wenn klar ist, dass die Person nicht zum Besitz berechtigt ist. Eine diesbezügliche Pflicht zur Prüfung der Besitzberechtigung besteht nicht. Für sichergestellte Telekommunikationsendgeräte gelten ergänzend engere Herausgabeanforderungen nach Absatz 4 Satz 3 bis 5.

**Zu § 33 Absatz 4**

Absatz 4 Satz 1 regelt das Anwesenheitsrecht der betroffenen Person bei Kontrollmaßnahmen nach § 32 Absatz 2 Nummer 2. Weil nach § 32 Absatz 4 zulässige Durchsuchungen verschlossener Gegenstände in Räumen, wenn erforderlich, auch ohne Anwesenheit der betroffenen Person durchgeführt werden können, stellt Satz 3 klar, dass die betroffene Person in diesen Fällen nach Beendigung der Maßnahme zu informieren ist, sobald der Zweck der Maßnahme nicht gefährdet wird.

**Zu § 33 Absatz 5**

Absatz 5 schützt die Interessen der betroffenen Person in Bezug auf sichergestellte Gegenstände der Informations- und Kommunikationstechnik.

Neben dem widerrechtlichen Verbringen von schutzwürdigen Informationen in Form von analogen Medien beinhalten widerrechtlich in Sicherheitsbereiche ein- und ausgeführte elektronische Speichermedien für den Geheimschutz sowie den Schutz betriebsnotwendiger informationstechnischer Systeme ein zunehmend erhebliches Gefährdungspotenzial, wobei zusätzlich von einem größeren Verbreitungs- und Weitergabepotenzial digitaler Medien auszugehen ist.



Für den Fall des unbefugten Einbringens digitaler Endgeräte muss daher zumindest ein vergleichbares Geheimschutz- und Sicherheitsniveau wie für analoge Medien gewährleistet werden. Dies wird durch § 32 Absatz 4 gewährleistet, nach dem auch die lediglich anlassbezogene Untersuchung sichergestellter mobiler Informations- und Kommunikationstechnik zulässig ist. Der Tatbestand des § 32 Absatz 4 knüpft dabei ausschließlich an Informations- und Kommunikationstechnik an, die auf dem Gelände der Liegenschaften der Verfassungsschutzabteilung aufgefunden werden. Dadurch ist der Anwendungsbereich örtlich begrenzt und inhaltlich strikt auf die Aufgaben und Zwecke der Sicherung limitiert.

Um Eingriffe in das elektronische Speichermedium im erforderlichen Maß zu beschränken, hat eine Untersuchung in der Regel durch Spiegelung der im elektronischen Speichermedium enthaltenen Daten zu erfolgen. Satz 1 schützt die Integrität des informationstechnischen Systems. So dürfen nur unbedingt notwendige Eingriffe erfolgen. Technische Veränderungen sind, soweit technisch möglich, rückgängig zu machen, um den Eigentümer vor Beeinträchtigungen zu schützen. Eine Herausgabe sichergestellter mobiler Telekommunikationsendgeräte, die nicht zur dienstlichen Nutzung überlassen wurden, hat nach Satz 2 abweichend zu Absatz 2 unabhängig vom Abschluss der Untersuchung nach § 32 Absatz 4 spätestens nach zwei Wochen zu erfolgen. Macht die betroffene Person die Notwendigkeit einer früheren Herausgabe geltend, ist dies angemessen zu berücksichtigen. Die Sätze 4 und 5 enthalten eine Regelung speziell für den Fall, dass die betroffene Person darlegt, dass sie auf die Erreichbarkeit mittels ihres privaten Mobiltelefons oder anderer mobiler Endgeräte oder deren Nutzung angewiesen ist (nachvollziehbare Gründe, etwa zur Nutzung des Gerätes aus familiären oder gesundheitlichen Gründen).

#### **Zu § 33 Absatz 6**

Absatz 6 enthält eine spezifische Regelung zum Kernbereichsschutz. Untersuchungen nach § 32 Absatz 4 haben den Kernbereich privater Lebensgestaltung der betroffenen Personen zu wahren. Der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit und sichert einen gegenüber dem Staat unantastbaren Menschenwürdekern. Auch hochrangige Interessen der Allgemeinheit können einen Eingriff in diesen geschützten Bereich privater Lebensgestaltung nicht rechtfertigen. Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge, Überlegungen und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen. Geschützt ist insbesondere die nicht öffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden. Es besteht daher ein umfassendes Verwertungsverbot. Demgegenüber gehören z. B. die Besprechung und Planung von Straftaten nicht zum Kernbereich privater Lebensgestaltung, selbst wenn sie auch Höchstpersönliches zum Gegenstand haben. Ob eine personenbezogene Kommunikation dem Kernbereich zuzuordnen ist, hängt von den Besonderheiten des jeweiligen Einzelfalls ab. Kommt es trotz Satz 1 zur Erhebung kernbereichsrelevanter Daten, schreibt Satz 4 die unverzügliche Löschung vor. Die Sätze 5 bis 7 enthalten Kernbereichsschutzspezifische Dokumentationsvorgaben zu Kontrollzwecken und damit korrespondierende Löschungspflichten.

**Zu § 33 Absatz 7**

Absatz 7 enthält eine spezifische Befugnis zur zwangsweisen Durchsetzung von Maßnahmen nach § 32 Absatz 2 und 4 ausschließlich gegenüber Personen, die nach § 32 Absatz 5 mitwirkungspflichtig sind. Die Zwangsmittel sind auf den spezifischen Sonderbereich der Sicherung von Verschlusssachen begrenzt und in Absatz 6 abschließend enumerativ geregelt. Der Begriff der Hilfsmittel der körperlichen Gewalt wird bereits in § 2 UZwG verwendet. Nach Absatz 6 kommen neben technischen Sperren als Hilfsmittel im Einzelfall insbesondere auch Fesseln in Betracht, deren Einsatz in Nummer 1 jedoch ausdrücklich eingeschränkt wird. Der Einsatz von Waffen, wie insbesondere Schusswaffen, ist unzulässig. Die zwangsweise Durchsetzung der Kontrollbefugnisse darf nur durch Personen erfolgen, die über eine qualifizierte Ausbildung (Schulung) verfügen. Die Verfassungsschutzabteilung hat dafür Sorge zu tragen, dass die Beschäftigten entsprechend ausgebildet werden.

**Zu § 33 Absatz 8**

Absatz 8 regelt die sofortige Vollziehbarkeit der Maßnahmen nach § 32. Ohne die sofortige Vollziehbarkeit droht ein Informationsverlust und in der Folge könnte der Zweck der Eigensicherungsmaßnahme und könnten in diesem Zusammenhang begangene Straftaten nicht verfolgt werden. Die betroffene Person hat gleichwohl die Möglichkeit, eine gerichtliche Überprüfung der Maßnahmen zu veranlassen.

**Zu Nummer 28 (§ 34 Inkrafttreten, Außerkrafttreten)**

Es handelt sich um eine Folgeänderung aufgrund der neu eingefügten §§ 32 und 33.

**Zu Artikel 2 – Inkrafttreten**

Die Vorschrift regelt das Inkrafttreten des Gesetzes.