

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienst-Rechts

A. Problem und Ziel

Als erster Teil der Reform des Nachrichtendienstrechts werden durch diesen Gesetzentwurf die Übermittlungsvorschriften an die Verfassungsrechtsprechung angepasst.

B. Lösung

Das Nachrichtendienstrecht ist auf der Grundlage jüngerer Verfassungsrechtsprechung umfassend fortzuentwickeln. In einem ersten Teil der Reform des Nachrichtendienst-Rechts werden die Übermittlungsregelungen an die Vorgaben des Bundesverfassungsgereichts angepasst. Da diese Regelungen nur noch bis Ende 2023 anwendbar sind, ist diese Anpassung besonders dringlich. Angesichts jüngerer Innentäterfälle bei den deutschen Nachrichtendiensten gilt dies gleichermaßen für eine wirksame Eigensicherung, die ebenso einbezogen ist. In einem zweiten Teil der Reform soll in 2024 die wertungskonsistente Systematisierung der Regelungen zur Informationsbeschaffung folgen und das Nachrichtendienstrecht insgesamt zukunftsfest ausgestaltet werden.

C. Alternativen

In Betracht kommt die Umsetzung zusammengefasst in einem Gesamtreformgesetz. Da die überarbeiteten Übermittlungsregelungen jedoch noch im Jahr 2023 in Kraft treten müssen, sind Abstimmung und Beratung der breiten Änderungsmaterie in solch engem Zeitrahmen kaum in angemessener Weise möglich.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

E.3 Erfüllungsaufwand der Verwaltung

Die einmaligen Sachmittelkosten belaufen sich auf insgesamt 3 541 000 Euro, die auf die Errichtung technischer Einrichtungen etwa im Bereich der Liegenschaftssicherung zurückzuführen sind. Die für die Wartung der Systeme notwendigen jährlichen Sachkosten werden mit 400 000 Euro kalkuliert. Durch Verwendung der Systeme entstehen jährliche Personalkosten in Höhe von 212 167,70 Euro.

Eventuelle Mehrausgaben im Bereich des Bundes sind finanziell und (plan-)stellenmäßig im jeweiligen Einzelplan auszugleichen.

F. Weitere Kosten

Keine.

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienst-Rechts

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. In § 6 Absatz 3 Satz 5 werden die Wörter „am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt,“ durch die Wörter „nach Ablauf von fünf Jahren“ ersetzt.
2. In § 18 Absatz 1a Satz 2 und 3 wird jeweils die Angabe „§ 19 Abs. 3“ durch die Angabe „§ 25a“ ersetzt.
3. Die §§ 19 bis 22 werden wie folgt gefasst:

„§ 19

Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist

1. zur Abwehr einer Gefahr für die Schutzgüter nach Absatz 2, die bereits im Einzelfall besteht oder in absehbarer Zeit in bestimmter Art zu entstehen droht, oder
2. zur Verhinderung einer Straftat, die im Höchstmaß mit einer Freiheitsstrafe von mindestens zehn Jahren bedroht ist.

(2) Schutzgüter nach Absatz 1 Nummer 1 sind

1. die freiheitliche demokratischen Grundordnung, einschließlich des Gedankens der Völkerverständigung und des friedlichen Zusammenlebens der Völker sowie der Bestand und die Sicherheit des Bundes und der Länder,
2. sonstige Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt sowie Sachen von bedeutendem Wert, deren Erhaltung im besonderen öffentlichen Interesse geboten ist, sowie
3. Leib, Leben oder Freiheit sowie vergleichbar besonders gewichtige Rechtsgüter einer Person.

(3) Das Bundesamt für Verfassungsschutz muss vorbehaltlich des § 23 personenbezogene Daten an die zuständige inländische öffentliche Stelle übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist

1. zur Vorbereitung und Durchführung von Verfahren und Maßnahmen
 - a) wegen einer Verletzung der Verfassungstreuepflicht im öffentlichen Dienst,
 - b) zur Durchsetzung von im Bereich der Gemeinsamen Außen- und Sicherheitspolitik der Europäischen Union beschlossenen wirtschaftlichen Sanktionsmaßnahmen, wenn die Sanktion dem Schutz der Schutzgüter nach Absatz 2 dient, oder
2. zur Abwehr einer sonstigen Gefahr nach Absatz 1, die im Einzelfall besteht und
 - a) von Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 ausgeht oder
 - b) gegenwärtig ist.

§ 20

Übermittlung an inländische Stellen zum administrativen Rechtsgüterschutz

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische Stellen übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz der Schutzgüter nach § 19 Absatz 2 vor Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 erforderlich ist, um ohne operative Anwendung unmittelbaren Zwangs

1. Personen, die an den Bestrebungen oder Tätigkeiten beteiligt sind,
 - a) zu deradikalisieren oder
 - b) in ihren Bestrebungen oder Tätigkeiten durch gefährderbezogene Maßnahmen sowie die Gestaltung und Überwachung von Strafvollzug und Führungsaufsicht zu beschränken,
2. die Verfügbarkeit von Mitteln, die für Bestrebungen oder Tätigkeiten eingesetzt werden können, zu verhindern bei
 - a) Beschaffung oder Besitz von Waffen oder Sprengstoffen und deren Grundstoffen,
 - b) Sammlung, Entgegennahme oder Verfügbarmachung von Vermögenswerten zur Förderung der Bestrebungen oder Tätigkeiten,
 - c) Vergabe von öffentlichen Fördermitteln oder sonstigen öffentlichen Vorteilszuwendungen,
3. besondere Gelegenheiten durch besondere Sachverhalte oder Rechtsverhältnisse für Handlungen, die die Bestrebungen oder Tätigkeiten besonders fördern, zu vermeiden, bei
 - a) Zugang zu Sicherheitsbereichen oder Verschlusssachen oder Wahrnehmung von Sicherheitsaufgaben oder Tätigkeit in lebens- oder verteidigungswichtigen Einrichtungen sowie kritischer Infrastrukturen,

- b) Betrieb oder Beeinflussung von Bildungseinrichtungen oder Tätigkeit in ihnen, Nutzung von Telemediendiensten oder Veranstaltung von Versammlungen, wenn dadurch die Bestrebungen oder Tätigkeiten betrieben werden,
 - c) Grundstückserwerb zum Betrieb von Einrichtungen für Bestrebungen oder zur Stärkung des Zusammenhalts der Beteiligten,
 - d) Nutzung oder Betrieb von Gewerbeeinrichtungen und Veranstaltungen zur Stärkung des Zusammenhalts der Beteiligten von Bestrebungen und zur Werbung von Mitgliedern,
 - e) Aufenthalt in Deutschland sowie Ein- und Ausreise der Beteiligten von Bestrebungen oder Tätigkeiten zu deren Förderung,
 - f) Staatsangehörigkeitserwerb,
4. gegenüber solchen Bestrebungen oder Tätigkeiten Verwundbarkeit zu mindern und Resilienz zu stärken durch
- a) Stärkung der Sicherheit in der Informationstechnik,
 - b) Wirtschaftsschutz und Schutz lebens- und verteidigungswichtiger Einrichtungen sowie kritischer Infrastrukturen,
5. auf vergleichbare Weise das Gefährdungspotenzial der Bestrebungen oder Tätigkeiten zu reduzieren.

Im Fall der Nutzung der Daten mit Außenwirkung darf bei einer betroffenen Person auch nicht der Eindruck entstehen, dass die öffentliche Stelle in diesem Fall zur operativen Anwendung unmittelbaren Zwangs befugt ist.

(2) Unter den Voraussetzungen des Absatzes 1 und vorbehaltlich des § 23 muss das Bundesamt für Verfassungsschutz in gesetzlich besonders geregelten Verfahren der Anfrage beim Bundesamt für Verfassungsschutz personenbezogene Daten an die zuständige inländische öffentliche Stelle übermitteln.

§ 21

Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische Strafverfolgungsbehörden zur Strafverfolgung übermitteln, wenn dies im Einzelfall aufgrund bestimmter Tatsachen erforderlich ist, um eine besonders schwere Straftat zu verfolgen.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 sind Straftaten, die im Höchstmaß mit Freiheitsstrafe bedroht sind von

- 1. mindestens zehn Jahren,
- 2. fünf Jahren und besonderen Staatsschutzbezug aufweisen aus dem
 - a) Strafgesetzbuch § 80a (Aufstacheln zum Verbrechen der Aggression), § 83 Absatz 2 (Vorbereitung eines hochverräterischen Unternehmens), § 85 Absatz 1 (Verstoß gegen ein Vereinigungsverbot), § 88 (Verfassungsfeindliche Sabotage), § 89 Absatz 1 (Verfassungsfeindliche Einwirkung auf Bundeswehr und

- öffentliche Sicherheitsorgane), § 95 (Offenbaren von Staatsgeheimnissen), § 96 Absatz 2 (Auskundschaften von Staatsgeheimnissen), § 97 Absatz 1 (Preisgabe von Staatsgeheimnissen), § 100a (Landesverräterische Fälschung), § 102 (Angriff gegen Organe und Vertreter ausländischer Staaten), § 106 Absatz 1 (Nötigung des Bundespräsidenten und von Mitgliedern eines Verfassungsorgans), § 107 (Wahlbehinderung), § 107a (Wahlfälschung), § 108 (Wählernötigung), § 108b (Wählerbestechung), § 108e Absatz 1 und 2 (Bestechlichkeit und Bestechung von Mandatsträgern), § 109d (Störpropaganda gegen die Bundeswehr), § 109e Absatz 1 bis 3 und 5 (Sabotagehandlungen an Verteidigungsmitteln), § 109f Absatz 1 (Sicherheitsgefährdender Nachrichtendienst), § 109g Absatz 1 (Sicherheitsgefährdendes Abbilden), § 129a Absatz 3 und 5 Satz 2 auch in Verbindung mit § 129b (Bildung terroristischer Vereinigungen), § 130 Absatz 1 und 3 (Volksverhetzung),
- b) Außenwirtschaftsgesetz § 18 Absatz 1 bis 5, auch in Verbindung mit Absatz 9,
 - c) Gesetz über die Kontrolle von Kriegswaffen § 19 Absatz 1, § 20a Absatz 1 und § 22a Absatz 1,
 - d) Ausführungsgesetz zu dem Übereinkommen vom 13. Januar 1993 über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen § 16 Absatz 1,
3. fünf Jahren, wenn sie zu Tätigkeiten nach § 3 Absatz 1 Nummer 2 für eine fremde Macht begangen worden sind,
4. fünf Jahren, wenn sie zu Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 und 4 begangen worden sind, aus dem Strafgesetzbuch
- a) § 125a (Besonders schwerer Fall des Landfriedensbruchs), § 127 (Betreiben krimineller Handelsplattformen im Internet), § 129 Absatz 1 Satz 1 und Absatz 5 auch in Verbindung mit § 129b (Bildung krimineller Vereinigungen), § 138 (Nichtanzeige geplanter Straftaten),
 - b) Sechzehnter Abschnitt (Straftaten gegen das Leben),
 - c) Siebzehnter Abschnitt (Straftaten gegen die körperliche Unversehrtheit),
 - d) Achtzehnter Abschnitt (Straftaten gegen die persönliche Freiheit),
 - e) § 253 (Erpressung), § 303b Absatz 2 und 3 (Computersabotage), § 305a (Zerstörung wichtiger Arbeitsmittel),
 - f) Achtundzwanzigster Abschnitt (Gemeingefährliche Straftaten),
 - g) Neunundzwanzigster Abschnitt (Straftaten gegen die Umwelt),
 - h) Dreißigster Abschnitt (Straftaten im Amt),
5. fünf Jahren aus dem Waffengesetz § 51 Absatz 1 und § 52 Absatz 1, wenn die verdächtige Person eine Person nach § 5 Absatz 2 Nummer 2 oder Nummer 3 des Waffengesetzes ist.
- (3) Unter den Voraussetzungen des Absatzes 1 und vorbehaltlich des § 23 muss das Bundesamt für Verfassungsschutz personenbezogene Daten an Strafverfolgungsbehörden übermitteln

1. in den Fällen des Absatzes 2 Nummer 1, wenn bestimmte Tatsachen dafür vorliegen, dass die Straftat zu Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 begangen worden ist, und
2. in den Fällen des Absatzes 2 Nummer 2 bis 5.

§ 22

Übermittlung an inländische Stellen ohne belastende Maßnahmen mit Außenwirkung

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische Stellen übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Vorbereitung und Durchführung eigener Maßnahmen erforderlich ist und die Übermittlung nicht auf unmittelbar außenwirksame Maßnahmen zu Lasten der betroffenen Person zielt.

(2) Das Bundesamt für Verfassungsschutz muss personenbezogene Daten vorbehaltlich des § 23 an den Bundesnachrichtendienst übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte zur Erfüllung der gesetzlichen Aufgaben des Bundesnachrichtendienstes erforderlich ist.

(3) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische Stellen übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz der Schutzgüter nach § 19 Absatz 2 vor Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 erforderlich ist und die Übermittlung zur Erfüllung von Aufgaben der empfangenden Stelle erfolgt, die nicht auf unmittelbar außenwirksame Maßnahmen zu Lasten der betroffenen Person zielen. Dies gilt insbesondere für die

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

Liegen die Voraussetzungen nach § 19 Absatz 1 und § 20 Absatz 1 nicht vor, darf der Empfänger die übermittelten Daten nicht für Maßnahmen nutzen, die die betroffene Person mit unmittelbarer Außenwirkung belasten.“

4. Die §§ 23 bis 25 werden durch die folgenden §§ 23 bis 25d ersetzt:

„§ 23

Übermittlungsverbot

Personenbezogene Daten dürfen nicht nach den §§ 19 bis 22 übermittelt werden, 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) ihrer Wertigkeit, auch unter Berücksichtigung eines vergangenen Zeitraums und des Alters der betroffenen Person, insbesondere bei Minderjährigen,
 - c) der Art der Erhebung, insbesondere im Falle des § 8 Absatz 2,
 - d) drohender, insbesondere verdachtsgegründeter Anschlussmaßnahmen,
 - e) der Verfügbarkeit vorherigen Rechtsschutzes gegen drohende Folgemaßnahmen,
3. durch die Übermittlung der personenbezogenen Daten eine dringende Gefahr für ein Schutzgut nach § 19 Absatz 2 Nummer 3 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 Schutzgüter nach § 19 Absatz 2,
 - 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.

§ 24

Minderjährigenschutz

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten über das Verhalten Minderjähriger vor Vollendung des 14 Lebensjahres nach den §§ 19 und 20 nur übermitteln, solange die Voraussetzungen der Speicherung nach § 11 Absatz 1 Satz 1 erfüllt sind. Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig

- 1. nach § 19 zum Schutz der Schutzgüter nach dessen Absatz 2 Nummer 3,
- 2. nach § 20, wenn nicht ausgeschlossen werden kann, dass durch die Person eine Gefahr nach § 19 Absatz 1 Nummer 1 besteht.

§ 25

Weiterverarbeitung durch den Empfänger

(1) Der Empfänger prüft, ob die nach den §§ 19 bis 22 übermittelten personenbezogenen Daten für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, dass die Daten nicht erforderlich sind, hat er 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. Der Empfänger darf diese weiteren Daten jedoch nicht nutzen.

(2) Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur verarbeiten

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

Das Bundesamt für den Verfassungsschutz hat den Empfänger auf den Zweck der Übermittlung und die Zweckbindung nach Satz 1 und darauf hinzuweisen, wenn die Nutzung zur Anwendung operativen Zwangs nach § 20 Absatz 1 oder zu unmittelbar außenwirksamen Maßnahmen zu Lasten der betroffenen Person nach § 22 Absatz 3 Satz 3 ausgeschlossen ist. Dies gilt nicht für Übermittlungen im Rahmen verdeckter Ermittlungen. Der Empfänger ist verpflichtet, dem Bundesamt für Verfassungsschutz auf dessen Verlangen Auskunft über die weitere Verarbeitung zu geben.

(3) 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 des Bundesamtes für Verfassungsschutz veranlasst ist.

§ 25a

Übermittlung an ausländische sowie über- und zwischenstaatliche Stellen

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen zur Weiterverarbeitung ohne Folgemaßnahmen mit unmittelbarer Außenwirkung übermitteln, wenn dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist

1. zum Schutz der Schutzgüter nach § 19 Absatz 2 oder zum Schutz der Sicherheit eines anderen Staates oder einer über- und zwischenstaatlichen Einrichtung,
2. zur Aufklärung von § 21 entsprechenden Straftaten.

Eine Aufklärung von Straftaten im Sinne von Satz 1 Nummer 2 umfasst nicht die Verwendung von personenbezogenen Daten im Rahmen eines Strafverfahrens. Die Regelungen des Gesetzes über die internationale Rechtshilfe in Strafsachen bleiben unberührt. Eine Übermittlung zum Schutz eines anderen Staates oder zur Aufklärung von Staatsschutzdelikten, die gegen einen anderen Staat begangen worden sind, ist unbeschadet des Absatz 2 nur zulässig, wenn dort die grundlegenden demokratischen und rechtsstaatlichen Prinzipien sowie die elementaren Menschenrechte gewährleistet sind.

(2) Die Übermittlung unterbleibt, wenn folgende Belange entgegenstehen:

1. besondere gesetzliche Regelungen zur Verarbeitung personenbezogener Daten oder
2. wesentliche auswärtige Belange der Bundesrepublik Deutschland oder
3. überwiegende schutzwürdige Interessen einer Person.

Überwiegende schutzwürdige Interessen stehen insbesondere entgegen, wenn Leib, Leben oder Freiheit einer Person oder sonstige elementare Menschenrechte gefährdet würden oder Verletzungen von elementaren rechtsstaatlichen Grundsätzen drohen.

Bei der Prüfung, ob eine Übermittlung zu unterbleiben hat, berücksichtigt das Bundesamt für Verfassungsschutz insbesondere den bisherigen Umgang des Empfängers mit übermittelten Daten und die Gewährleistung eines zum Schutz der Menschenrechte angemessenen Datenschutzes.

(3) Die übermittelten personenbezogenen Daten dürfen

1. nur zu dem Zweck, zu dem sie ihm übermittelt wurden, und
2. unbeschadet des Absatzes 4 nicht für Folgemaßnahmen mit unmittelbarer Außenwirkung zu Lasten der betroffenen Person

weiterverarbeitet werden. Das Bundesamt für Verfassungsschutz hat den Empfänger hierauf hinzuweisen. Es hat ihn ferner darauf hinzuweisen, dass es sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

(4) Das Bundesamt für Verfassungsschutz darf einer Verwendung der personenbezogenen Daten für Maßnahmen mit unmittelbarer Außenwirkung zu Lasten der betroffenen Person zustimmen

1. zur operativen Anwendung unmittelbaren Zwangs, wenn eine konkretisierte Gefahr im Sinne des § 19 Absatz 1 für die Schutzgüter nach Absatz 1 Satz 1 Nummer 1 vorliegt,
2. zu anderen Folgemaßnahmen mit unmittelbarer Außenwirkung, wenn ein konkretes Risiko im Sinne des § 20 Absatz 1 für die Schutzgüter nach Absatz 1 Satz 1 Nummer 1 vorliegt, das durch die administrative Folgemaßnahme gemindert werden kann,
3. zur Verfolgung von Straftaten bei verdichteten tatsächlichen Anhaltspunkten für § 21 entsprechende Straftaten.

Für die Übermittlung personenbezogener Daten über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres an Stellen eines Staates, der weder unmittelbar an die Bundesrepublik Deutschland angrenzt noch Mitgliedstaat der Europäischen Union oder des Nordatlantikvertrages ist, gilt dies nur zur Abwehr einer im Einzelfall bestehenden Gefahr für Leib oder Leben einer Person oder bei dringendem Verdacht auf eine § 21 entsprechende Straftat. Eine Zustimmung ist unzulässig, wenn die Belange nach Absatz 2 entgegenstehen.

(5) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine nichtöffentliche Stelle im Ausland übermitteln, wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur Abwehr einer dringenden Gefahr für ein Schutzgut nach § 19 Absatz 2 Nummer 3 unerlässlich ist und überwiegende schutzwürdige Interessen der betroffenen Person nach § 23 Satz 1 Nummer 2 nicht entgegenstehen.

(6) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten auch an inländische Stellen übermitteln, wenn dies zur Vorbereitung einer Übermittlung nach den vorstehenden Absätzen erforderlich ist. § 25 Absatz 2 ist anzuwenden.

§ 25b

Übermittlung zum Schutz der betroffenen Person

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten 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. Es darf personenbezogene Daten insbesondere für Zwecke der Jugendhilfe übermitteln.

§ 25c

Weitere Verfahrensregelungen

(1) Das Bundesamt für Verfassungsschutz protokolliert den Empfänger, die Rechtsgrundlage sowie den Zeitpunkt der Übermittlung. Die Protokolldaten müssen danach auswertbar sein, ob die Übermittlung nach § 19, § 20, § 21, § 22 oder § 25a erfolgt ist. Das Bundesamt für Verfassungsschutz darf Protokolldaten, die ausschließlich zu Zwecken der Datenschutzkontrolle gespeichert werden, nur für diesen Zweck verarbeiten. Es muss diese Protokolldaten am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, löschen.

(2) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten der betroffenen Person oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen. Der Empfänger darf diese Daten nicht nutzen.

(3) Eine Übermittlung an nichtöffentliche Stellen bedarf der Zustimmung der Amtsleitung des Bundesamtes für Verfassungsschutz. Für Übermittlungen an inländische nichtöffentliche Stellen kann die Zustimmung auch allgemein für gleichgelagerte Fälle erfolgen. Die Übermittlung ist dem Betroffenen durch das Bundesamt für Verfassungsschutz mitzuteilen, sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist.

§ 25d

Nicht nachrichtendienstlich erhobene personenbezogene Daten

Personenbezogene Daten, die das Bundesamt für Verfassungsschutz nicht mit nachrichtendienstlichen Mitteln (§ 8 Absatz 2) erhoben hat, darf es abweichend von den §§ 19 bis 22 und 25a auch für sonstige erhebliche Zwecke der öffentlichen Sicherheit oder für sonstige erhebliche Interessen des Empfängers übermitteln, es sei denn der Übermittlung stehen besondere gesetzliche Verarbeitungsregelungen oder überwiegende schutzwürdige Interessen der betroffenen Person entgegen. Die §§ 23, 25 und 25c sind nicht anzuwenden.“

5. Nach § 26 wird folgender § 26a eingefügt:

„§ 26a

Übermittlung durch Landesverfassungsschutzbehörden an Strafverfolgungs- und Sicherheitsbehörden

(1) Die Verfassungsschutzbehörden der Länder übermitteln den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien personenbezogene Daten unter den Voraussetzungen von § 19 und § 21

sowie § 22 Absatz 3. Auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

(2) Die Verfassungsschutzbehörden der Länder übermitteln dem Bundesnachrichtendienst personenbezogene Daten unter den Voraussetzungen des § 22 Absatz 2.“

6. Vor § 27 werden die folgenden § 26b und § 26 c eingefügt:

„§ 26b

Besondere Eigensicherungsbefugnisse

(1) Die Eigensicherung dient dem Schutz der Beschäftigten, Einrichtungen, Gegenstände, Quellen und amtlichen Informationen des Bundesamts für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten. Das Bundesamt für Verfassungsschutz hat hierzu besondere Befugnisse nach Maßgabe der folgenden Absätze.

(2) Das Bundesamt für Verfassungsschutz darf bei Personen, die seine Dienststellen, Grundstücke und sonstigen Einrichtungen (Eigensicherungsbereich) betreten oder sich dort aufhalten, und von diesen Personen mitgeführte Taschen und sonstige Gegenstände sowie von diesen Personen genutzte Fahrzeuge

1. verdachtsunabhängig kontrollieren,
2. durchsuchen, wenn tatsächliche Anhaltspunkte für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegen.

(3) Eine Kontrolle nach Absatz 2 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 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 Eigensicherungsbereich befinden, darf das Bundesamt für Verfassungsschutz 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 Eigensicherungsbereich aufhalten, sind verpflichtet an Maßnahmen nach den Absätzen 2 und 4 mitzuwirken. Entziehen sich Personen Maßnahmen nach den Absätzen 2 und 4 im Eigensicherungsbereich, darf das Bundesamt für Verfassungsschutz die Maßnahmen auch noch in unmittelbarer Nähe des Eigensicherungsbereichs vornehmen.

(6) Das Bundesamt für Verfassungsschutz darf optisch-elektronische Einrichtungen zur offenen Überwachung des Eigensicherungsbereichs 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) Das Bundesamt für Verfassungsschutz kann eine nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung unzulässige Benutzung des Luftraums seines Eigensicherungsbereichs durch unbemannte Fluggeräte durch geeignete technische Mittel gegen das unbemannte Fluggerät, dessen Steuerungseinheit oder Steuerungsverbindung aufklären und abwehren.

(8) Das Bundesamt für Verfassungsschutz darf die besonderen Mittel nach den §§ 8a, 8d und 9 Absatz 1 und 4 sowie den §§ 9a und 9b unter den dort genannten Voraussetzungen auch einsetzen, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Aufklärung von sicherheitsgefährdenden Tätigkeiten

1. seiner Beschäftigten oder
2. von Personen, die vom Bundesamt für Verfassungsschutz beauftragt sind
 - a) im Eigensicherungsbereich tätig zu sein oder
 - b) sonstige sicherheitsempfindliche Tätigkeiten wahrzunehmen.

(9) Bei der Durchführung von Maßnahmen nach den Absatz 2 sowie den Absätzen 4 bis 8 hat das Bundesamt für Verfassungsschutz 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.

§ 26c

Verfahren; Kernbereichsschutz

(1) Maßnahmen nach § 26b Absatz 2 Nummer 2 und Absatz 4 bedürfen der Anordnung der für die Eigensicherung zuständigen Abteilungsleitung oder einer von ihr bestimmten Vertretung. Maßnahmen nach § 26b Absatz 6 bedürfen der Anordnung der Amtsleitung oder einer von ihr bestimmten Vertretung.

(2) Ist eine Anordnung nach Absatz 1 Satz 1 aufgrund besonderer Eilbedürftigkeit nicht rechtzeitig zu erlangen, kann die Maßnahme auch ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich erschwert würde. Bei Geräten der Informations- und Kommunikationstechnik darf in diesem Fall lediglich das Gerät sichergestellt werden. Die Anordnung ist unverzüglich nachzuholen. Wird die Anordnung nach Absatz 1 Satz 1 nicht nachgeholt, so

hat das Bundesamt für Verfassungsschutz unverzüglich bereits erhobene Daten zu löschen und sichergestellte Gegenstände an die betroffene Person herauszugeben.

(3) Sichergestellte Gegenstände sind unverzüglich an die betroffene Person herauszugeben, sobald der Zweck der Eigensicherung 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 § 26b Absatz 2 Nummer 2 hat die betroffene Person das Recht, anwesend zu sein. Über eine Durchsichtung nach § 26b Absatz 2 Nummer 2 oder eine Sicherstellung nach § 26b Absatz 4 Satz 1 ist auf Verlangen eine Bescheinigung über die Maßnahme und den Grund der Maßnahme zu erteilen. Maßnahmen nach § 26b 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 § 26b Absatz 4 an die betroffene Person spätestens nach zwei Wochen herauszugeben. Macht die betroffene Person in den Fällen des Satz 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. Das Bundesamt für Verfassungsschutz 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. Das Bundesamt für Verfassungsschutz darf Erkenntnisse, die den Kernbereich privater Lebensgestaltung berühren, nicht verarbeiten, weitergeben oder in anderer Weise nutzen. Das Bundesamt für Verfassungsschutz 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. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach Ablauf von sechs Monaten zu löschen.

(7) Das Bundesamt für Verfassungsschutz kann zur Durchsetzung von Maßnahmen gegenüber Personen, die nach § 26b Absatz 5 mitwirkungspflichtig sind, folgende Mittel anwenden:

1. unmittelbare Einwirkung auf die betroffene Person oder Gegenstände (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 Behördenleitung des Bundesamts für Verfassungsschutz 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 § 26b haben keine aufschiebende Wirkung.“

Artikel 2

Änderung des MAD-Gesetzes

Das MAD-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2977), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. In § 10 wird nach Absatz 1 folgender Absatz 1a eingefügt:

„(1a) Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgabe nach dem Bundespolizeigesetz wahrnehmen, unterrichten den Militärischen Abschirmdienst von sich aus entsprechend § 18 Absatz 1b und 6 des Bundesverfassungsschutzgesetzes.“

2. § 11 wird wie folgt gefasst:

„ § 11

Übermittlung personenbezogener Daten durch den Militärischen Abschirmdienst

Auf die Übermittlung personenbezogener Daten durch den Militärischen Abschirmdienst finden die §§ 19 bis 22, 25a, 25b und 25d des Bundesverfassungsschutzgesetzes entsprechend Anwendung. Für vom Verfassungsschutz übermittelte personenbezogene Daten nach § 18 Absatz 1a Satz 1 des Bundesverfassungsschutzgesetzes gilt § 18 Absatz 1a Satz 2 bis 4 des Bundesverfassungsschutzgesetzes entsprechend.“

3. In § 12 wird die Angabe „§§ 23 bis 26“ durch die Angabe „§§ 23, 25, 25c und 26“ ersetzt.
4. Nach § 14 wird folgender § 15 eingefügt:

„ § 15

Besondere Eigensicherungsbefugnisse

(1) Auf die Befugnisse und Verfahren der Eigensicherung des Militärischen Abschirmdienstes finden die §§ 26b und 26c des Bundesverfassungsschutzgesetzes entsprechend Anwendung. 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.

(2) Das Gesetz über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen bleibt hiervon unberührt.“

5. Der bisherige § 15 wird § 16.

Artikel 3

Änderung des Sicherheitsüberprüfungsgesetzes

In § 36 Absatz 2 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch ... geändert worden ist, wird die Angabe „Nummer 3“ durch die Angabe „Satz 2“ ersetzt.

Artikel 4

Änderung des Artikel 10-Gesetzes

§ 4 Absatz 4 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. Satz 1 werden im Satzteil nach Nummer 3 die Wörter „erforderlich sind“ durch die Wörter „erforderlich sind und in den Fällen der Nummern 1 und 2 daneben die Voraussetzungen der Vorschriften vorliegen, die Übermittlungen der übermittelnden Stelle für die Verhinderung, Aufklärung oder Verfolgung von Straftaten allgemein regeln“ ersetzt.
2. Satz 2 wird aufgehoben.

Artikel 5

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.

(2) In Artikel 1 Nummer 4 tritt § 25c Absatz 1 Satz 2 am 1. Januar 2025 in Kraft.

Begründung

A. Allgemeiner Teil

Der Gesetzentwurf enthält als erster Teil einer umfassenden Reform des Nachrichtendienstrechts die Anpassung der Regelungen zur Übermittlung nachrichtendienstlich gewonnener Informationen. Dieser Teil erfordert eine vorgezogene Umsetzung, da wesentliche Regelungen des Bundesverfassungsschutzgesetzes nach einer Entscheidung des Bundesverfassungsgerichts nur noch längstens bis zum 31. Dezember 2023 fortgelten.

I. Zielsetzung und Notwendigkeit der Regelungen

Der Gesetzentwurf setzt die Vorgaben um, die das Bundesverfassungsgericht zu den Übermittlungsbefugnissen des Bundesverfassungsschutzgesetzes in seinem Beschluss vom 28. September 2022 - 1 BvR 2354/13 - getroffen hat. Nach der Entscheidung gelten wesentliche Übermittlungsvorschriften längstens bis zum 31. Dezember 2023 fort und müssen mithin zuvor durch verfassungskonforme Neuregelungen abgelöst werden.

II. Wesentlicher Inhalt des Entwurfs

Als Teil der auf Systematisierung und Wertungskonsistenz zielenden Reform des Nachrichtendienstrechts ersetzt der Gesetzentwurf nicht lediglich punktuell die außer Kraft tretenden Übermittlungsbefugnisse der Verfassungsschutzbehörden (bisherige § 20 Absatz 1 Satz 1 und 2 und § 21 Absatz 1 Satz 1 in Verbindung mit § 20 Absatz 1 Satz 1 und 2), sondern passt diese Übermittlungsbefugnisse insgesamt an die Vorgaben des Gerichts an. Dazu werden die bisherigen §§ 19 bis 22 und 23 bis 25a insgesamt ersetzt.

Vor dem Hintergrund der mit dem russischen Angriffskrieg auf die Ukraine verschärften internationalen Lage ist im Übrigen besonders vordringlich, die Eigensicherung des Bundesamtes für Verfassungsschutz (BfV) und des Militärischen Abschirmdienstes (MAD) speziell gegenüber Ausforschungsoperationen anderer Nachrichtendienste zu stärken, insbesondere gegenüber Innentätern.

III. Alternativen

Alternativ könnte die Reform des Nachrichtendienstrechts zusammengefasst in einem Gesamtreformgesetz erfolgen. Da angesichts der Fristsetzung des Bundesverfassungsgerichts das Gesetz jedenfalls in Bezug auf die Übermittlungsregelungen noch in 2023 in Kraft treten muss, wären Abstimmung und Beratung eines umfassenden Reformgesetzes allerdings kaum angemessen möglich.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 73 Absatz 1 Nummer 10 Buchstabe b und c des Grundgesetzes und zu Artikel 2 und 4 für die Befugnisse von MAD und BND hinzutretend aus Artikel 73 Absatz 1 Nummer 1 des Grundgesetzes (Verteidigung, auswärtige Angelegenheiten). Die Gesetzgebungskompetenz zu den Regelungen der Eigensicherung bei BfV und MAD folgt aus der Natur der Sache.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf hat keine Bezüge zum Recht der Europäischen Union, da er Regelungen auf dem Gebiet der nationalen Sicherheit trifft, die in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt (Artikel 4 Absatz 2 EUV). Er ist mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar.

VI. Gesetzesfolgen

Die gesetzliche Normierung der vom Bundesverfassungsgericht vorgegebenen Verhältnismäßigkeitsmaßgaben bewirkt keine Änderung im Verwaltungsvollzug, da dieser bereits an die verfassungsgerichtlichen Vorgaben angepasst ist.

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf bezweckt keine Rechts- und Verwaltungsvereinfachung, sondern die Umsetzung der Verfassungsrechtsprechung.

2. Nachhaltigkeitsaspekte

Auf den einleitenden Gesetzesfolgenhinweis wird verwiesen.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

4. Erfüllungsaufwand

Die einmaligen Sachmittelkosten belaufen sich auf insgesamt 3.541.000 €, die auf die Errichtung technischer Einrichtungen etwa im Bereich der Liegenschaftssicherung zurückzuführen sind. Die für die Wartung der Systeme notwendigen jährlichen Sachkosten werden mit 400.000 € kalkuliert. Durch Verwendung der Systeme entstehen jährliche Personalkosten in Höhe von 212.167,70 €.

Eventuelle Mehrausgaben im Bereich des Bundes sind finanziell und (plan-)stellenmäßig im jeweiligen Einzelplan auszugleichen.

5. Weitere Kosten

Keine.

6. Weitere Gesetzesfolgen

Keine.

VII. Befristung; Evaluierung

Die Herstellung einer verfassungskonformen Gesetzeslage bedarf weder einer Befristung noch einer Evaluierung.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundesverfassungsschutzgesetzes)

Zu Nummer 1

Eine verlängerte Aufbewahrung der Protokolldaten dient gleichermaßen dem Datenschutz wie der Datensicherung, speziell zur Eigensicherung, weil hierdurch in Fällen missbräuchlichen Zugriffs verbessert retrograd aufgearbeitet werden kann, welche Verstöße bereits vorausgegangen sind. Gerade im Fall überwordener Innentäter, die andere Nachrichtendienste zur Aufklärung des BfV einsetzen, ist sowohl mit hochprofessionellem Vorgehen wie auch womöglich längerfristigen Beschaffungsoperationen des fremden Nachrichtendienstes zu rechnen. So waren Innentäter in Einzelfällen über Jahre in westlichen Nachrichtendiensten aktiv, bevor sie enttarnt werden konnten. Um in der anschließenden Aufarbeitung bzw. der Feststellung der durch einen Innentäter verursachten Schäden (insbesondere Informationsabflüsse sowie unberechtigte Kenntnisnahme von Verschlusssachen) und der Aufklärung der Arbeitsweise (insbesondere, welche Daten und Speicherungen von Interesse waren) ein möglichst umfassendes Bild zu erhalten, ist eine entsprechend lange Revisionsmöglichkeit der im Nachrichtendienstlichen Informationssystem getätigten Abfragen unabdingbar. Die Verarbeitung der Protokolldaten unterliegt dabei für die gesamten Speicherdauer der engen Zweckbindung des § 6 Absatz 3 Satz 4.

Zu Nummer 2

Es handelt sich um eine Folgeänderung zu Nummer 3.

Zu Nummer 3

Vor seiner Entscheidung vom 28. September 2022 zum Bundesverfassungsschutzgesetz (1 BvR 2354/13) hatte das Bundesverfassungsgericht bereits mit seinem Urteil vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz (1 BvR 1619/17) auch Vorgaben zur verfassungskonformen Gestaltung von Übermittlungsregelungen getroffen. Die Innenministerkonferenz hat hierzu Lösungsansätze erarbeitet (Umlaufbeschluss vom 19. September 2022 - IX B 2.1), auf denen der Gesetzentwurf aufsetzt.

Das Bundesverfassungsgericht hat seine Verhältnismäßigkeitswürdigung der nachrichtendienstlichen Datenverarbeitung unter Einbezug einer Folgenbetrachtung entwickelt. Weil Verfassungsschutzbehörden lediglich Aufklärungsaufgaben haben, ihnen aber keine polizeilichen Zwangsbefugnisse zustehen, um im Anschluss an eine Überwachungsmaßnahme aufgrund der gewonnenen Informationen selbst konkrete Gefahrenabwehrmaßnahmen oder Strafverfolgungsmaßnahmen gegenüber Einzelnen mit Zwang durchzusetzen, hat es für nachrichtendienstliche Überwachungsbefugnisse abgesenkte Eingriffsschwellen - „Vorfeldaufklärung“ - akzeptiert (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 154, 158 f.; vgl. vorausgegangen bereits zur Differenzierung im Hinblick auf polizeiliche Zwangsbefugnisse BVerfGE 156, 11 - Rn. 102, 106). Andererseits verknüpft es diese erleichterte Datenerhebung komplementär mit Einschränkungen für die Übermittlung an andere Stellen, die den Anforderungen genügen, die von Verfassungs wegen an entsprechende eigene Grundrechtseingriffe der empfangenden Stellen zu richten sind („Kriterium der hypothetischen Datenneuerhebung“ – BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 170). Im Ergebnis gelten bei der Übermittlung nachrichtendienstlich ersterhobener personenbezogener Daten und daraus gewonnener Informationen besonders strenge Anforderungen, wenn der Empfänger über operative Zwangsbefugnisse verfügt (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 235 zu Gefahrenabwehrbehörden, gem. 257 f. aber ergebnisgleich auch für andere Behörden; BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 124). Auch andere Anschlussmaßnahmen können für die betroffene Person allerdings gewichtige, u.U. massive Folgen haben (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 259).

Dem tragen §§ 19 ff. mit gestuften Übermittlungsschwellen und angepassten Anschlussverwendungen Rechnung. Ausgangspunkt ist dabei immer, dass die Übermittlung zum Schutz besonders gewichtiger Rechtsgüter konkret veranlasst ist (§ 22 in Verbindung mit § 19 Absatz 2). Dies eröffnet aber allein die informationelle Anschlussnutzung durch Weiterverarbeitung beim Empfänger, im Ergebnis die Erarbeitung von Erkenntnisprodukten. Für intervenierende – unmittelbar außenwirksame - Anschlussmaßnahmen müssen zusätzlich situative Schwellen hinzukommen. Besteht im Einzelfall ein Risikosachverhalt, eröffnet dies ein Einwirken auf die Risikofaktoren (§ 20), speziell entsprechende Verwaltungsverfahren. Dies schließt unmittelbar außenwirksame Eingriffe ein, jedoch nicht die situativ-operative Zwangsausübung nach vollzugspolizeilicher Typik (§ 20 Absatz 1 a.E.). Solche polizeitypische Befugnis ist erst in den Fällen einer konkretisierten Gefahr (§ 19) oder der Strafverfolgung (§ 21) eröffnet. Welche Eingriffe der Empfänger unter welchen Voraussetzungen vornehmen darf, ergibt sich dabei erst aus dem Fachrecht der Empfängerbehörde. Die Übermittlungsregelungen schaffen nur einen informationellen Rahmen für operative Anschlussnutzung, um das Fehlerrisiko in Ungewissheitssituationen nach Maßgabe einer situativen Gewichtung des Handlungsanlasses angemessen zu begrenzen.

Neben dieser typisierenden Stufenbildung des Gesetzes (konkreter Anlass / Erkenntnisprodukt; bestimmtes Risiko / Verwaltungsakt; konkretisierte Gefahr / Polizeigewalt) verbleibt auch die prinzipiell gleitende Skala der Verhältnismäßigkeitsprüfung (geregelt in § 23 Nummer 2), um auch atypische Sonderfälle angemessen zu behandeln.

Die Verfassungsschutzaufgabe erschöpft sich nicht in der Sammlung und Auswertung von Informationen über bestimmte Bedrohungen, sondern erfüllt sich erst in der Weitergabe dieser Informationen an die Stellen, die zum operativen Schutz vor erkannten Bedrohungen befähigt sind (vgl. BVerfGE 154, 152 - Rn. 217). Solche Übermittlung ist damit originär Aufgabe der Verfassungsschutzbehörde. Deshalb enthalten die Übermittlungsbefugnisse Regelungen zur Ermessensreduktion in Form einer Übermittlungspflicht (§ 19 Absatz 3, § 20 Absatz 2 und § 21 Satz 2). Im Interesse wirksamer Aufgabenwahrnehmung wird die Übermittlungspflicht erweitert, indem der im bisherigen § 20 Absatz 1 enthaltene Behördenbezug auf die Polizei aufgegeben wird.

Die Paragraphen-Gliederung folgt der primär auf den Übermittlungszweck ausgerichteten Rechtsprechung des Bundesverfassungsgerichts und integriert die Übermittlungspflichten (bisheriger § 20) in die jeweiligen Übermittlungsbefugnisse nach §§ 19 bis 22.

Die speziellen Regelungen berücksichtigen, dass Informationen mit nachrichtendienstlichen Mitteln gewonnen werden. Eine erweiterte Übermittlung von sonstigen Informationen öffnet § 25d.

Die Regelungen haben allein die Übermittlung durch das BfV zum Gegenstand, nicht Übermittlungsersuchen an das BfV. Zu Fällen, in denen hierzu besondere notwendig ist, weil die allgemeine Erhebungsbefugnis der erhebenden Behörde dafür nicht ausreicht, ist dies im Fachrecht der Behörde, die mit dem Ersuchen ihre Aufgabe wahrnimmt, zu regeln.

Geregelt werden Eingriffe, da diese dem Vorbehalt des Gesetzes unterliegen, also die Übermittlung personenbezogener Daten. Die Übermittlung von Sachinformationen findet ihre Grundlage in der Aufgabennorm des BfV. Soweit die Eingriffsbefugnisse zur Übermittlung personenbezogener Daten eine Ermessensreduktion in Form einer Übermittlungspflicht vorsehen, ist diese gesetzliche Vorgabe ebenso für die pflichtgemäße Ermessensausübung bei der Übermittlung von Sachinformationen zu beachten.

Zu § 19 (Übermittlung zur Gefahrenabwehr)

§ 19 regelt die Übermittlung zur Gefahrenabwehr im engeren Sinne. § 20 beinhaltet eine weitere Befugnis zum Rechtsgüterschutz durch Beeinflussung bereits von

Risikosachverhalten, für die jedoch keine operativen Zwangsbefugnisse verfügbare sind (§ 20 Absatz 1 am Ende).

Zu Absatz 1

Absatz 1 enthält Zweckbegrenzungen und besondere Übermittlungsschwellen. Konkretisierungen zur Zweckbegrenzung enthält Absatz 2.

Zu Nummer 1

Die Nummer trifft eine Zweckbegrenzung als Folge nachrichtendienstlicher Besonderheiten, nämlich abgesenkter Erhebungsvoraussetzungen und Einsatz nachrichtendienstlicher Mittel sowie weitgehende Freistellung von Transparenzpflichten gegenüber betroffenen Personen (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 240). Deshalb ist eine Übermittlung nur zum Schutz eines besonders gewichtigen Rechtsguts zulässig (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 236, 255). Diese werden in Absatz 2 aufgeführt.

Die Übermittlungsschwelle der wenigstens konkretisierten Gefahr tritt als besonders strenge Voraussetzung hinzu, wenn der Empfänger über operative Zwangsbefugnisse verfügt (s.o. Vorbemerkung zu Artikel 1 Nummer 3). Wegen dieser hohen Schwelle sind bei Übermittlungen nach dieser Norm keine besonderen Beschränkungen zu Folgemaßnahmen (anders bei der Risikointervention gem. § 20 Absatz 6) erforderlich, d.h. Gefahrenabwehr kann hier effektiv, also insbesondere auch durch die operative Anwendung unmittelbaren Zwangs betrieben werden.

Da der Begriff der konkretisierten Gefahr kein Fachbegriff, sondern eine vom Bundesverfassungsgericht gewählte Bezeichnung ist, wird er im Gesetzeswortlaut nicht aufgegriffen, vielmehr wird diese Schwelle in Nummer 1 tatbestandlich näher ausgeführt. Eine konkretisierte Gefahr setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 134), also Anhaltspunkte, die den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Störungsgeschehen zulassen (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 158). Das in Nummer 1 aufgenommene Tatbestandsmerkmal „in bestimmter Art“ umschreibt also, dass das prognostizierte Störungsgeschehen nur der Art nach konturiert sein muss, etwa gegen ein bestimmtes Rechtsgut gerichtet oder phänomenologisch umrissen, beispielsweise als terroristische Tat.

Zu Nummer 2

Nummer 2 dient mit der präventiven Anknüpfung an Straftaten dem Gleichlauf (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 131) mit der Strafverfolgungsregelung in § 21 Satz 1 Nummer 1 und schließt Schutzlücken, die ansonsten etwa bei drohenden Straftaten nach § 97 Absatz 2 AufenthG, §§ 29a ff. BtMG, §§ 19 f. KrWaffG, §§ 243, 250, 267 Absatz 3 und 4 StGB auftreten könnten. Wenn eine Übermittlung zur Strafverfolgung zulässig ist, kann es kein Verfassungsgebot sein, dass die rechtsstaatliche Verwaltung die Straftat sehenden Auges geschehen lässt, um dann – zulässig – die Strafverfolgung zu initiieren, vielmehr muss hier prioritär das Rechtsgut vor der Verletzung geschützt, also die Straftat bereits verhindert werden. Auch im Fall der Übermittlung zur Strafverfolgung nach § 21 ist die Strafverfolgungsbehörde zur Ausübung der strafprozessualen Befugnisse zur operativen Zwangsausübung befugt, auch insoweit stellt die Regelung in § 19 mit der uneingeschränkten Verfügbarkeit auch von Zwangsbefugnissen lediglich den präventiven Gleichlauf bei der Wirksamkeit der Zweckverfolgung her.

Zu Absatz 2

Zu Nummer 1

Nummer 1 enthält die in § 1 Absatz 1 aufgeführten Verfassungsschutzrechtsgüter. Der Aufgabenbereich der Nachrichtendienste ist von vornherein dadurch gekennzeichnet, dass er dem Schutz besonders gewichtiger Rechtsgüter dient (BVerfGE 155, 119 - Rn. 151; BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 150). Angesichts der speziellen Aufgabenregelung in § 3 Absatz 1 Nummer 4 sind der Klarheit halber die dort benannten Schutzziele mit aufgeführt. Auch diese Schutzgüter sind Teilelemente der Kernsubstanz des vom Grundgesetz konstituierten Gemeinwesens, die zur Einbettung in eine internationale Friedensordnung gleichwertig neben den zentralen Prinzipien der inneren Staatsorganisation stehen. Gleiches gilt für den Tatbestand des § 3 Absatz 1 Nummer 3, wenn für das Schutzgut der auswärtigen Belange qualifizierte, nämlich gewaltorientierten Bedrohungen bestehen. Wegen dieses Erfordernisses qualifizierter Angriffsmodalität werden auswärtige Belange in Absatz 2 nicht als gesondertes Schutzgut aufgeführt. Der Schutz vor hiergegen gerichteten Bedrohungen ist bei deren Gewaltausrichtung aber ebenso Essenz der Einbettung in eine internationale Friedensordnung und des Gedankens der Völkerverständigung.

Zu Nummer 2

Nummer 2 ergänzt die Auflistung um weitere Kollektivrechtsgüter von besonderem Gewicht (BVerfGE 120, 274 – Rn. 247; 141, 220 - Rn. 108), sowie von Sachen mit besonderen gemeinwohldienlichen Funktionen. Beim Schutz solcher Sachen ist ein enges Verständnis geboten: Gemeint sind etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 130). Ein praxisbedeutsamer Anwendungsfall der Nummer ist der Schutz kritischer Infrastrukturen, darunter auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.

Zu Nummer 3

Nummer 3 führt besonders gewichtige Individualrechtsgüter auf. Der Katalog ist nicht abschließend. Auch das Bundesverfassungsgericht versteht diese Aufzählung nicht abschließend, sondern hat vorausgegangen beispielsweise auch die Gesundheit als besonders wichtiges Individualrechtsgut anerkannt, sofern es – ebenso wie bei Leib oder Freiheit – um schwerwiegende Verletzungen geht (BVerfGE 133, 277 – Rn. 203). Vergleichbar wichtig sind beispielsweise auch schwerwiegende Verletzungen der sexuellen Selbstbestimmung oder schwere Gefährdungen des Wohls eines Kindes oder Jugendlichen als Kernanliegen der Jugendhilfe.

Zu Absatz 3

Absatz 3 verdichtet die nach Absatz 1 bestehende Übermittlungsbefugnis zur Übermittlungspflicht. Dies betrifft in Nummer 1 und Nummer 2 Buchstabe a Übermittlungen zum Zweck des Verfassungsschutzes (wie im bisherigen § 20 Absatz 1), geht in Nummer 2 Buchstabe b aber auch darüber hinaus.

Bereits die dem Verfassungsschutz dienende Übermittlungspflicht ist gegenüber dem bisherigen Recht erweitert. Sie erfasst einerseits auch die speziellen Verfahren nach Nummer 1 und andererseits nach Nummer 2 Buchstabe a alle Fälle, in denen sich eine von Beobachtungsobjekten ausgehende konkretisierte Gefahr (Befugnischwelle nach Absatz 1) bereits zur konkreten – im Einzelfall bestehenden – Gefahr (Verpflichtungsschwelle nach Absatz 3 Nummer 2) entwickelt hat. Diese erweiterte Ermessensreduktion im Falle verfassungsschutzbezogenen Handlungsbedarfs ist aufgabenadäquat, da die Verfassungsschutzaufgabe sich erst in der Weitergabe der Erkenntnisse an die Stellen erfüllt, die zum operativen Schutz vor erkannten Bedrohungen befähigt sind (vgl. BVerfGE 154, 152 - Rn. 217).

Zudem wird die Übermittlungspflicht erweiternd mit Nummer 2 Buchstabe b auch verfassungsschutzabgelöst auf den Schutz anderer herausragender Rechtsgüter erstreckt, sofern die Gefahr bereits gegenwärtig ist.

Nummer 1

Nummer 1 regelt besondere Verfahren, die der Beseitigung einer bereits eingetretenen Störung der Verfassungsschutzgüter dienen. Das Bundesverfassungsgericht hat als verhältnismäßigkeitswahrende Übermittlungsschwelle für die Verknüpfung nachrichtendienstlicher Vorfelderkenntnisse mit Anschlussmaßnahmen operativer Zwangsausübung die (wenigstens) konkretisierte Gefahr benannt. Erst Recht bleibt dann die Verhältnismäßigkeit gewahrt, wenn anlassgebend für die Übermittlung eine bereits eingetretene Störung ist, die es zu beseitigen gilt. Übermittlungsveranlassend sind dabei jeweils tatsächliche Anhaltspunkte, allgemein in § 19 zum Gefahrenverdacht (einer konkretisierten Gefahr), bei den Störungstatbeständen des Absatz 3 Nummer 1 zum Störungsverdacht.

Buchstabe a bezeichnet mit dem Begriff „Verfassungstreupflicht“ gleichermaßen die dienstrechtlichen Pflichten zum jederzeitigen Eintreten für die freiheitliche demokratische Grundordnung (vgl. § 60 Absatz 1 Satz 3 BBG, § 33 Absatz 1 Satz 3 BeamStG, § 8 SG) wie auch die entsprechenden arbeitsrechtlichen Pflichten (speziell § 41 Satz 2 TVöD-BT-V). Im dienstrechtlichen Verhältnis kann die Disziplinarbehörde gegenüber einem Beamten oder Soldaten also auch ihre operativen Zwangsbefugnisse (Beschlagnahmen oder Durchsuchungen nach § 27 BDG, § 20 WDO) einsetzen. Dies ist für Ermittlungen im Disziplinarverfahren wesentlich, weil hier das Direktionsrecht nicht im Wege eines Verwaltungsverfahrens ausgeübt wird, die Alternative des Erlasses eines Verwaltungsaktes mit nötigenfalls anschließender Verwaltungsvollstreckung also nicht eröffnet ist. Unabhängig davon, wären mit solcher Gestaltung auch die Verfahrenszwecke nicht effektiv erreichbar, weil bei solchem Verfahren typischerweise mit Verschleierungshandlungen des beschäftigten Extremisten zu rechnen wäre.

Buchstabe b betrifft ebenso ein Verfahren, die mit der Abwehr einer konkretisierten Gefahr infolge von Sanktionsmaßnahmen der Europäischen Union im Bereich der Gemeinsamen Außen- und Sicherheitspolitik einhergehen. Entsprechende Sanktionen werden im Regelfall ergriffen, wenn das friedliche Zusammenleben der Völker durch völkerrechtswidrige Handlungen gestört wurde (z.B. im Fall des russischen Angriffskrieges auf die Ukraine) oder durch Handlungen, die völkerrechtlichen Verträgen zuwiderlaufen (z.B. im Zusammenhang mit dem Verhalten des Iran, sein Nuklearprogramm betreffend), beeinträchtigt wurde. Die Gefahrenabwehr im Bereich sektoraler Wirtschaftssanktionen durch Maßnahmen der Außenwirtschaftsüberwachung (Verhütung von Straftaten nach dem Außenwirtschaftsgesetz) rechtfertigt – ebenso wie im Bereich der Bekämpfung der Proliferation von Massenvernichtungswaffen – Übermittlungen von mit nachrichtendienstlichen Methoden gewonnenen Erkenntnissen, um außen- und sicherheitspolitisch nicht hinnehmbare Sanktionsverstöße abzuwehren. Gleiches gilt für Sicherstellungsbefugnisse nach dem SanktDG (§§ 2 ff.), in denen auch eine operative Ausübung unmittelbaren Zwangs miteingeschlossen sein kann. Hier liegt die konkretisierte Gefahr bereits generell in der Situation der verhängten wirtschaftlichen Sanktionsmaßnahme mit der resultierenden Verfügungsbeschränkung, da hiernach mit Wahrscheinlichkeit mit Handlungen der sanktionierten Person zu rechnen ist, die darauf zielen, die sanktionsbefangenen Vermögenswerte dem Sanktionsregime zu entziehen. Dient die jeweilige wirtschaftliche Sanktionsmaßnahme (sektorale Sanktion oder Finanzsanktion) – wie oben beschrieben – den Verfassungsschutzgütern, dann droht mit dem Verstoß gegen dieses Unionsrecht diesen Rechtsgütern Gefahr. Allerdings stammen relevante Informationen hier oftmals von ausländischen Nachrichtendiensten, so dass deren Weitergabe dann typischerweise nach § 23 Satz 1 Nummer 4 die „Third Party Rule“ entgegensteht, solange der Nachrichtengeber der Übermittlung nicht zustimmt. Nicht hiervon gehindert ist dagegen die Weitergabe selbst ermittelter Erkenntnisse, auch wenn sie von Spurenansätzen angestoßen worden waren, die von Ausländischen Nachrichtendiensten stammten. Auch insoweit ist zwar das „ob“ der Übermittlung gesetzlich entschieden, es

verbleibt aber (wie auch bei der Polizei) eine ermittlungstaktische Abwägung zum Zeitpunkt der Übermittlung, da die exekutive Sicherstellung weitergehende Aufklärungsinteressen – etwa zu anderen sanktionsverstrickten Vermögensgütern der betroffenen Personen in Deutschland – gefährden kann. Auch hierbei können Interessen eines ausländischen Nachrichtendienstes mit eingehen, wenn Sachverhalte in gemeinsamen Operationen aufgeklärt werden.

Auch bei anderen Sachverhalten ergibt sich gegebenenfalls eine entsprechende Ermessensreduktion. Dies gilt speziell für Verfahren nach Artikel 18 oder 21 Absatz 4 GG. Auf deren Erwähnung wird hier indessen verzichtet, weil in diesen seltenen Sachverhalten – auch unter Würdigung des besonderen Eingriffsgewichts und des speziellen Verfahrens typischerweise nicht isolierte tatsächliche Anhaltspunkte, sondern verfahrensadäquat erst verdichtete Informationen zu übermitteln sind, auch in der Phase einer Verfahrensvorbereitung innerhalb der vollziehenden Gewalt. Deshalb fügen sich diese Verfahren nicht in die Regelungsstruktur dieses Absatzes ein, unbeschadet dessen, dass bei entsprechender Erkenntnislage auch hier dem BfV kein Übermittlungsermessen verbleibt. In den Verfahren hat das Bundesverfassungsgericht Befugnisse zu Beschlagnahme und Durchsuchung (§ 38 Absatz 1 BVerfGG) bzw. zur Vermögensentziehung (§ 46 Absatz 2 Satz 2 BVerfGG).

Entsprechendes gilt auch für Vereinsverbotsverfahren. Nach Artikel 9 Absatz 2 GG sind extremistische Vereinigungen bereits verfassungsunmittelbar verboten. Nach dieser Verfassungsentscheidungen können in den Feststellungsverfahren, die die Frage der Verfassungswidrigkeit klären, auch operative Zwangsbefugnisse etwa bei Ermittlungsmaßnahmen nach § 4 des Vereinsgesetzes oder bei der Sicherstellung von Vereinsvermögen nach § 10 des Vereinsgesetzes angewendet werden, wenn das Vereinsverbotsverfahren mit den Schutzgütern verfassungsmäßige Ordnung oder Völkerverständigung den besonderen Zwecken nach Absatz 2 dient. Auch in solchen Verfahren erfolgt allerdings zunächst eine Informationssammlung durch das BfV als operative Ermittlungsbehörde. In diesen Verfahren ist nicht erforderlich, je einzelne tatsächliche Anhaltspunkte an die Verbotsbehörde zu übermitteln. Deshalb ist dieses Verfahren hier nicht aufgenommen, auch wenn hier ebenso bei Erreichen der kritischen Informationsdichte kein Übermittlungsermessen verbleibt, sondern zu übermitteln ist.

Zu Nummer 2

Die Regelung erstreckt die Übermittlungspflicht im Interesse wirksamen Rechtsgüterschutzes in einem gestuften System der Gefahrennähe auch auf verfassungsschutzfremde Aufgaben (konkretisierte Gefahr: Übermittlungsbefugnis, Absatz 1 / konkrete Gefahr: aufgabenbezogene Übermittlungspflicht, Absatz 4 Nummer 2 Buchstabe a / gegenwärtige Gefahr: aufgabenfremde Übermittlungspflicht).

Im Rahmen der allgemeinen Übermittlungspflichten nach Nummer 2 kann zur Erforderlichkeit auch berücksichtigt werden, ob die Information dem Empfänger auch – rechtzeitig – anderweitig bekannt wird. Praktischer Fall kann beispielsweise sein, dass die Gefahrerforschung bereits in Zusammenarbeit des BfV mit einer Polizeibehörde erfolgt. In solchen Fällen liegt regelmäßig näher, dass auch Übermittlungen an Dritte, etwa gefährdete Personen oder Einrichtungen durch die Polizei im Rahmen polizeilicher Gefahrenabwehr erfolgt.

Zu § 20 (Übermittlung an inländische Stellen zum vorbeugenden Rechtsgüterschutz)

Die Regelung dient gleichermaßen dem wirksamen Schutz besonders gewichtiger Rechtsgüter als Reaktion auf bestimmte Risikofaktoren, die das Gefährdungspotenzial der Bestrebungen oder Tätigkeiten qualifiziert steigern (Absatz 1 Satz 1 Nummern 1 bis 5) wie auch der Beschränkung von Eingriffswirkungen durch Ausschluss operativer Anwendung unmittelbaren Zwangs (Absatz 1, nach der Nummernaufzählung). Letzteres ist unter Verhältnismäßigkeitserwägungen geboten, um der Besonderheit Rechnung zu tragen, dass die zu übermittelnden personenbezogenen Daten abgelöst von der Einsatzschwelle polizeilicher

Gefahrerforschung bereits im Gefahrenvorfeld verdeckt gewonnen worden sind (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 -, Rn. 119 ff.). Die Verhältnismäßigkeitsbetrachtung des Übermittlungseingriffs setzt Folgerisiken und Rechtfertigungsanforderungen in Relation, die empfängerseitige Informationsverwendung wirkt somit auf die Übermittlungsvoraussetzungen vor (vgl. Gusy, RuP 2022, 257/262). Beschränkte Weiterverarbeitung kann mithin erleichterte Übermittlung öffnen.

Verfügt der Empfänger über operative Zwangsbefugnisse, gilt die besonders strenge Anforderung einer konkretisierten Gefahr als Übermittlungsvoraussetzung (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 235, 257 f. und Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 124). Auch mögliche sonstigen Folgen bleiben aber bei der Gewichtung des Übermittlungseingriffs Rechnung zu tragen (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 235, 259), wenn sie intervenierende Außenwirkung gegenüber dem Betroffenen einschließen und damit über die allein informationellen Befugnisse zur Datenverarbeitung hinaus gehen, auf die der ersterhebende Nachrichtendienst seinerseits beschränkt ist.

Maßgeblich sind dabei die unmittelbar möglichen Folgemaßnahmen (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 – Rn. 123), also eine konkrete Betrachtung der Übermittlungsfolgen, die der Gesetzgeber mit einer differenzierenden Befugnisausstattung des Empfängers gestalten kann (so hatte das Bundesverfassungsgericht bereits vorausgegangen das BKA in seiner Zentralstellenfunktion nicht als Behörde qualifiziert, die über operative Befugnisse verfügt: BVerfGE 156, 11 – Rn. 123; ferner Gärditz, GSZ 2022, 161/164 ff.; Unterreitmeier, GSZ 2023, 34/37). Eine solche Gestaltung enthält Absatz 1 mit dem Ausschluss operativer Zwangsmaßnahmen.

Der Ansatz, die Anschlussverwendung verhältnismäßigkeitswährend zu regulieren, um damit die Übermittlung zu eröffnen, entspricht den das Datenschutzrecht prägenden Zweckbindungen, etwa durch Straftatenkataloge. So hat auch das Bundesverfassungsgericht in seiner Entscheidung zum Bayerischen Verfassungsschutzgesetz (Urteil vom 26. April 2022 - 1 BvR 1619/17 – Rn. 251) die Übermittlung zur Strafverfolgung auf besonders schwere Straftaten beschränkt, ohne dies damit zu verbinden, dass nur an Strafverfolgungsbehörden übermittelt werden darf, die ausschließlich solche Straftaten verfolgen. Eine solche verhältnismäßigkeitswährende Weiterverarbeitungsbindung – sei es durch Zweckbindung oder Zwangsausschluss – hat ihren Sachschwerpunkt in der Regelung der Übermittlungsvoraussetzungen und ist danach von der dies betreffenden Gesetzgebungskompetenz eingeschlossen.

Angesichts dieser Folgenbegrenzung bleibt die gegenüber § 19 abgesenkte Übermittlungsschwelle des § 20 verhältnismäßig. Vorausgesetzt ist hier keine bereits konkretisierte Gefahr, vielmehr ist die Übermittlung hier bereits von konkreten Risikofaktoren veranlasst, die das Gefährdungspotenzial der Bedrohung steigern und auf die danach zum vorbeugenden Rechtsgüterschutz administrativ-ordnungsbehördlich einzuwirken ist. Der Ausschluss operativer Zwangsgewalt wahrt dabei die Verhältnismäßigkeit dieser spezifisch risikobezogenen Übermittlungsschwelle. Zwar bleiben hoheitliche Anschlussmaßnahmen mit unmittelbarer Außenwirkung zu Lasten des Betroffenen möglich (und sind womöglich auch intendiert), bei Gewichtung dieser Folgen ist hier aber wesentlich, dass vorheriger Rechtsschutz effektiv verfügbar ist und die Verwaltung in einer Verwaltungstreitsache die Darlegungs- und Beweislast für den Eingriffstatbestand trägt. Bei der operativen, unmittelbar situationsveranlassten Zwangsausübung drohen hingegen irreversible Schäden, die auch mit der Genugtuungs- und zukunftsgerichteten Vorbeugefunktion einer Fortsetzungsfeststellungsklage nicht auszugleichen sind. Dies unterscheidet die situationsbedingt operative Anwendung unmittelbaren Zwangs von einem Verwaltungsvollstreckungsverfahren, das auch bei einer Übermittlung nach § 20 zur Durchsetzung eines Verwaltungsaktes möglich bleibt (Unterreitmeier, GSZ 2023, 34/35).

Zu Absatz 1

Der Absatz 1 setzt als Übermittlungsschwelle besondere Wirkungsfaktoren voraus, die für das Gefährdungspotenzial der Bedrohung steigernd sind und deshalb eine Einwirkung auf sie zum vorbeugenden Rechtsgüterschutz veranlassen. Der Ansatz folgt Grundüberlegungen tertiärer bzw. indizierter und sekundärer bzw. selektiver/situativer Prävention. Die Ansatzpunkte der Intervention sind personenindiziert (Nummer 1), bezogen auf Tatmittel (Nummer 2) und -gelegenheiten (Nummer 3) sowie den Opferschutz (Nummer 4). Da es sich um Risikofaktoren des Gefährdungspotenzials von Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 handelt, werden hierdurch die Schutzgüter nach § 19 Absatz 2 Nummer 1 gesteigert bedroht. Die Übermittlung zur Einwirkung auf solche Risikofaktoren erfolgt also der Sache nach immer zum Schutz dieser Rechtsgüter.

Erforderlich ist eine Übermittlung zur hoheitlichen Einwirkung auf ein Risiko nur, wenn die intendierte Anschlussmaßnahme ergriffen werden kann. Insoweit wirken also auch die Befugnisvoraussetzungen der Anschlussmaßnahme auf die Übermittlungszulässigkeit vor. Der übermittelnden Stelle wird damit keine Vorprüfung der Zulässigkeit des Folgeeingriffs übertragen (sie liefert lediglich einen informationellen Beitrag, besitzt mithin oftmals bereits keinen ausermittelten Erkenntnisstand), wenn der Empfänger jedoch allgemein nicht über eine geeignete Einwirkungsmöglichkeit verfügt, ist die Übermittlung für den intendierten Zweck nicht erforderlich. Entscheidend ist dabei, ob für die übermittelnde Stelle aus ihrer Perspektive absehbar ist, dass die Übermittlung den verfolgten Zweck nicht erreichen kann.

Satz 1 schließt die operative Zwangsausübung als Anschlussmaßnahme aus, was in Satz 2 dadurch effektiv ausgestaltet wird, dass auch nicht der falsche Eindruck entstehen darf, die Behörde verfüge hier über operative Zwangsbefugnis. Die Regelung berücksichtigt, dass § 20 Übermittlungen für ordnungsbehördliche Verwaltungsverfahren auch an solche Ordnungsbehörden öffnet, die nicht nur die Befugnis besitzen, im Verwaltungsverfahren bindende Regelungen durch Verwaltungsakt zu treffen, sondern grundsätzlich auch zur operativen Ausübung unmittelbaren Zwangs befugt sind. So erfolgen Übermittlungen zur Zuverlässigkeitsüberprüfung nach § 5 WaffG originär zur Durchführung des Verwaltungsverfahrens mit dem Erlass eines Verwaltungsaktes. Bei einer Erlaubnisaufhebung wären allerdings grundsätzlich weitere Maßnahmen unter Anwendung operativer Zwangsbefugnisse zur Sicherstellung oder Durchsuchung (speziell nach § 46 Absatz 4 WaffG) grundsätzlich möglich. Diese werden mit Absatz 1 jedoch ausgeschlossen, im Ergebnis somit an die erhöhten Voraussetzungen des § 19, nämlich die Situation bereits konkretisierter Gefahr gebunden. Liegt solche Gefahr nicht vor, darf diese Befugnis nicht ausgeübt werden. Dass die Behörde institutionell solche Befugnis besitzt, ist für die Verhältnismäßigkeit der Übermittlung unschädlich, wenn sie hierüber im konkreten Verfahren nicht verfügt.

Zu Nummer 1

Nummer 1 betrifft Maßnahmen, die darauf zielen, direkt auf Beteiligte einzuwirken, und zwar sowohl bereits auf ihre Einstellung (Buchstabe a wie jedenfalls deren Umsetzung im Verhalten (Buchstabe b). Dies kann beispielsweise durch individualisierte Deradikalisierungsmaßnahmen erfolgen (Buchstabe a. Solcherart personenindizierte (Tertiär-)Prävention erfolgt ferner etwa bei Gefährdern durch das ganzheitliches Risikomanagement in der hierzu eingerichteten Arbeitsgruppe des Gemeinsamen Terrorismusabwehrzentrums, oder in Strafvollzug und Führungsaufsicht (Buchstabe b). Solche „täterbezogene“ Prävention hat Bezüge sowohl zu § 19 wie auch § 22. Sofern zur betroffenen Person die individuelle Disposition zu der Art nach schon absehbaren Gefährdungen anzunehmen ist, ist der Sachverhalt bereits unter die engeren Voraussetzungen von § 19 subsumierbar, so etwa im Tatbestand des § 55 BKAG (mit der Konsequenz, dass hier die Folgenbeschränkung des Zwangsausschlusses nicht greift). Zielt die Übermittlung hingegen auf keine belastenden Maßnahmen, wie etwa typischerweise bei einer Ausstiegshilfe, wäre dies ein Fall des § 22. Ebenso ist die Zusammenarbeit zur Erstellung allgemeiner Konzepte – auch auf dem Gebiet der Deradikalisierung – ein Anwendungsfall des § 22 (vgl. dessen Absatz 1 Satz 2 Nummer 3). Dagegen können Maßnahmen, die nicht auf der Mitwirkungsbereitschaft der betroffenen Person aufbauen, sondern unabhängig davon subordinativ ansetzen, nicht

unter § 22 gefasst werden. Dies gilt auch für die – auf Resozialisierung zielende – Vollzugsplanung im Strafvollzug, erst recht für gefährdungsbeschränkende Belastungseingriffe im Vollzug oder danach (Nummer 2).

Zu Nummer 2

Die Nummer betrifft Mittel, mit denen die Bestrebungen verfolgt werden. Neben Mitteln unmittelbarer Tatbegehung (Nummer 1, vgl. § 5 WaffG, § 17 BJagdG, § 8a SprengG), sind dies auch Finanzmittel (Buchstabe b), da sie wesentlich für die operative Handlungsfähigkeit des nachrichtendienstlichen Gegenübers sind (vgl. zur Terrorismusfinanzierung § 89c StGB). Das Verfügbarmachen schließt auch darauf gerichtete Transaktionsketten ein, die zur Verschleierung des Finanzierungssachverhalts auch undolose Beteiligte einbeziehen können. Bei Vergabe öffentlicher Fördermittel (Buchstabe c) kommt noch der Missbrauch öffentlicher Mittel sowie die Ansehenssteigerung so unterstützter Aktivitäten hinzu. Auch Reputation ist ein Einsatzmittel, die Wirkungsbreite und -intensität von Bedrohungen zu steigern, weshalb als weiteres Beispiel der Risikofaktoren-Fallgruppe 2 auch eine Ordensverleihung (materiell-rechtlich an unwürdige Personen ausgeschlossen) zu nennen wäre. Die öffentliche Verleihung von Ehrenzeichen wäre gewissermaßen ein öffentlich postuliertes Gütesiegel, das für extremistische Bestrebungen im Hinblick auf Reichweite, Anschlussfähigkeit und Akzeptanz außerordentlich förderlich sein würde.

Zu Nummer 3

Die Nummer betrifft Gelegenheitsstrukturen. Zum Ausschluss von Zuverlässigkeitsrisiken beim Zugang zu sicherheitsrelevanten Orten, Tätigkeiten und Informationen erfolgen vielfältige Verfahren der Eignungsprüfung, die u.a. auch den Bedrohungen nach § 3 Absatz 1 vorbeugen sollen. Neben gesetzlichen Regelungen (vgl. nur SÜG, § 34a GewO, § 7 LuftSiG, § 12b AtG) werden solche organisatorische Sicherungsmaßnahmen auch von der Verwaltung ergriffen, etwa bei der Einrichtung von Sicherheitsbereichen mit Zugangsakkreditierung bei Veranstaltungen mit allgemein gefährdeten Schutzpersonen. Buchstabe a enthält für solche Sachverhalte die Übermittlungsbefugnis.

Buchstaben b bis d betreffen Strukturen, die der extremistischen oder sicherheitsgefährdenden Beeinflussung der Allgemeinheit oder spezieller Zielgruppen dienen oder einer Kontaktabahnung zur Rekrutierung wie auch der innengerichteten Stärkung des Zusammenhalts. Nummer 3 erfasst beispielsweise auch Grundstücksgeschäfte für „Siedlungsprojekte“ (Bildung „nationaler“ Gebiete, vgl. Verfassungsschutzbericht 2022, S. 70). Unter Buchstabe d fallen etwa extremistische Konzert- oder Kampfsportveranstaltungen. Hierbei geht es nicht ausschließlich darum, Tatgelegenheitsstrukturen hoheitlich zu beeinflussen, vielmehr kann auch durch Förderung gesellschaftlicher Wachsamkeit an „hot spots“ des Geschehens präventive Wirkung erzeugt werden. Im Übrigen ist ausreichend, dass die betreffenden Strukturen auch bedrohungsfördernd genutzt werden, es ist nicht vorausgesetzt, dass sie ausschließlich dazu dienen. Dass beispielsweise ein rechtsextremistischer Liederabend auch der Einnahmeerzielung und dem persönlichen Unterhalt des Vortragenden dient, ist mithin unschädlich.

Buchstabe e betrifft Einreise und Aufenthalt als Basisvoraussetzung, um in Deutschland für Zwecke der Bedrohung tätig zu werden (vgl. etwa § 73 AufenthG). Auch hier ist nicht entscheidend, ob der Aufenthalt ausschließlich solchen Bestrebungen und Tätigkeiten dient, es reicht vielmehr, dass er auch hierzu spezifisch förderlich ist. Ebenso ist auch die Ausreise etwa zur Begehung von Terrorakten oder auch extremistischen Kundgebungen im Ausland eingeschlossen (vgl. etwa §§ 7, 8, 10 PaßG). Der in Buchstabe f geregelte Staatsangehörigkeitserwerb verfestigt das Aufenthaltsrecht irreversibel und schafft mit der demokratischen Teilhabe durch aktives und passives Wahlrecht einen Rechtsstatus, dessen extremistischem Missbrauch bereits vorgebeugt werden muss (so komplementär im Staatsangehörigkeitsrecht auch § 37 StAG).

Zu Nummer 4

Die Nummer bietet die Informationsgrundlage für opferbezogene Prävention und auch Nachsorge im Schädigungsfall, wobei in den Buchstaben besonders praxisbedeutsame Fälle aufgeführt werden. Benannt wird dabei der Zweck, nicht der Übermittlungsempfänger. Im Falle des Buchstaben a ist beispielsweise – je nach Sachverhalt – eine direkte Information potenzieller Angriffsziele denkbar, ebenso wie die informationelle Unterstützung des BSI, gemeinsame Beratungsmaßnahmen oder die Zusammenarbeit im Nationalen Cyber-Abwehrzentrum auch mit anderen Behörden. In der Regel intendieren solche Übermittlungen allerdings keine außenwirksamen Eingriffsmaßnahmen. Werden dabei jedoch personenbezogene Daten übermittelt (z.B. im Fall des Buchstaben a eine vom Angreifer genutzte IP), kann dies für diese Zwecke auf diese Befugnis gestützt werden, so dass eine zusätzliche Regelung hierfür in § 22 überflüssig ist.

Zu Nummer 5

Die Nummer verdeutlicht zugleich auch für die vorausgegangenen Nummern das gemeinsame Kriterium der Reduktion des Gefährdungspotenzials durch das Einwirken jeweils auf bestimmte gefährdungssteigernde Risikofaktoren. Die Übermittlung erfolgt also unter einer besonderen situativen Schwelle (besonderer Risikosachverhalt), wobei diese qualifizierte Situation ein administratives Einwirken konkret erfordert (allerdings wird die operative Zwangsanwendung erst mit der Schwelle des § 19 verfügbar). Ein Beispiel wäre bspw. der Zugang zu Giften oder umweltschädliche Substanzen als Tatmittel, die noch nicht speziell in Nummer 2 aufgeführt sind. Kern des Regelungsbedarfs ist, dass zukünftige Lebenssachverhalte nicht abschließend überschaubar sind, so dass insoweit eine gesetzliche Anleitung nötig ist, die die normativ wesentliche Vorgabe für den Verwaltungsvollzug trifft, ohne solche Anwendungsoffenheit zu versperren. Dazu wird das Prinzip der administrativen Intervention zur Beeinflussung besonderer Risikosachverhalte, die das Gefährdungspotenzial der Bedrohung spezifisch steigern, allgemein geregelt.

Zu Absatz 2

Der Absatz verdichtet die Befugnis des Absatzes 1 ermessensreduzierend zur Übermittlungspflicht. Die Übermittlungspflicht ist auf gesetzlich besonders geregelte Verfahren der vorbeugenden Personenüberprüfung bezogen. Solche Überprüfungen sind beispielsweise in § 73 AufenthG, § 12b AtG, § 34a GewO, § 7 LuftSiG, § 37 StAG, § 3 Absatz 2 SÜG, § 5 WaffG geregelt. Daneben bestehen besondere Übermittlungspflichten zu Personal im öffentlichen Dienst nach § 19 Absatz 4 Nummer 1 Buchstabe c.

Wenn eine Behörde im Übrigen im Rahmen ihrer allgemeinen Aufgaben für Schutzzwecke nach § 19 Absatz 2 Informationen benötigt, die das BfV nach § 3 Absatz 1 sammelt, bleibt es grundsätzlich im Ermessen des BfV, wie es auf eine solche Erkenntnis-anfrage verfährt. Allerdings leitet auch die allgemeine Amtshilfepflicht die Ausübung solchen Ermessens in gewisser Weise an. Eine Ermessensreduktion kann sich insbesondere ergeben, wenn der Empfänger die Informationen zu Verfassungsschutzzwecken benötigt. Dies kann beispielsweise der Fall sein, wenn eine Behörde vor einer Projektvergabe im Bereich politischer Bildung die Eignung von Bewerbern überprüft und eine Organisation mit extremistischem Hintergrund darunter ist.

Zu § 21 (Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung)

§ 21 regelt die Übermittlung für Strafverfolgungszwecke. Nach der Verfassungsrechtsprechung ist sie nur bei besonders schweren Straftaten zulässig (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 136) und erfordert eine gewisse Verdachtsverdichtung (BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 - Rn. 137), über einen Anfangsverdacht hinaus (BVerfGE 154, 152 – Rn. 222). Für diese qualifizierende Anforderung zur Aussagekraft der tatsächlichen Erkenntnisgrundlage verwendet der Gesetzentwurf

den Begriff „bestimmte Tatsachen“. Dies stellt keine übersteigerten Anforderungen, sondern meint ein „mehr“ gegenüber den ansonsten übermittlungsleitenden „tatsächlichen Anhaltspunkten“. Eine praktische Faustformel kann die Frage sein, ob bereits weniger gewichtige Erkenntnisse Strafermittlungen zur Sachklärung – etwa auch im Wege von Strukturermittlungen – veranlassen könnten. Bei Übermittlungen zu bereits laufenden Strafverfahren ist dies per se der Fall. Es ist aber keine Voraussetzung, dass bereits justizseitig Strafermittlungen geführt werden, folglich ist auch unmaßgeblich, in welchem Verfahrensstadium sich etwaige staatsanwaltliche Prüfungen befinden oder wie solche Verfahren in der justiziellen Aktenordnung qualifiziert werden. Maßgeblich ist die Einschätzung der übermittelnden Stelle, was allerdings auch Informationen der empfangenden Stelle einbeziehen kann, die von dort etwa im Rahmen der Vorprüfung der Übermittlungsvoraussetzungen übermittelt werden.

Für die Bestimmung besonders schwerer Straftaten gibt der Strafrahmen einen maßgebenden Anhaltspunkt. Das Bundesverfassungsgericht hat dazu in seiner aktuellen Rechtsprechung keine direkten Vorgaben getroffen. Es hat allerdings negativ abgrenzend festgestellt, dass Delikte mit einem Strafrahmen von bis zu 3 Jahren Freiheitsstrafe die verfassungsrechtlichen Anforderungen verfehlen (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 155). Nach dem Darstellungszusammenhang kann hieraus zwar nicht der Umkehrschluss gezogen werden, dass Delikte mit dem höheren Strafrahmen ab 5 Jahren generell einbeziehbar sind. Wäre das Gericht allerdings der Auffassung, dass nicht nur eine Höchststrafe von 3 Jahren, sondern zudem auch eine Höchststrafe von 5 Jahren generell ungenügend ist, hätte nahegelegen, dass es dies in seinen Ausführungen zur Vermeidung von Fehlinterpretationen signalisiert, was aber nicht der Fall ist. Zudem hat das Gericht in seinem Grundsatzurteil zum BayVSG (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 197 a.E.) bereits im Zusammenhang der besonders schweren Straftaten u.a. auch den Deliktskatalog des § 3 Absatz 1 G 10 erwähnt, der für die Strafverfolgungszusammenarbeit wichtige Staatsschutzdelikte enthält, wie etwa Geheimdienstliche Agententätigkeit (§ 99 Absatz 1 StGB), Volksverhetzung (§ 130 StGB) oder mitgliederschaftliche Betätigung in einer kriminellen extremistischen Vereinigung (§ 129 StGB), allesamt Straftaten mit einer Höchststrafe von 5 Jahren. Es wäre rechtsstaatlich schwer erträglich, wenn die Verfassungsschutzbehörden den Strafverfolgungsbehörden keine Informationen über einen enttarnten Spion mitteilen dürften oder über Beteiligte wirkungsbreiter Volksverhetzung oder militante Überfälle organisierter Extremisten etwa auf Asylbewerber oder Synagogenbesucher (wenn es bei Körperverletzungen bleibt).

Andererseits hatte das Gericht 2004 im Zusammenhang der Wohnraumüberwachung (BVerfGE 109, 279 – Rn. 238) vertreten, von der besonderen Schwere einer Straftat im Sinne des Art. 13 Absatz 3 GG sei nur auszugehen, wenn sie der Gesetzgeber jedenfalls mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat. Dazu ist allerdings einzubeziehen, dass das Gericht in seiner aktuellen Rechtsprechung für die Übermittlung von Informationen aus Wohnraumüberwachung erhöhte Anforderungen stellt (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 248), woraus im Gegenschluss für die Übermittlung von Informationen, die nicht aus einem derart intensiven Eingriff stammen, mindere Voraussetzungen bereits verhältnismäßigkeitssichernd sind. Das Gericht bezieht dies zwar nicht auf den Übermittlungszweck, sondern auf die situative Übermittlungsschwelle zur Gefahrenabwehr. Die Anforderungen zur Straftatenschwere entwickelt es dagegen als gewichtende Anforderungen zum Rechtsgüterschutz (nicht zur Übermittlungsschwelle). Darin liegt jedoch bereits in der Rechtsprechung eine gewisse Inkonsistenz, denn Strafvorschriften bewahren Rechtsgüter, der Deliktstatbestand beschreibt dagegen nicht mehr das Rechtsgut, sondern bereits die situative Konkretisierung der Tathandlung. Der gerichtliche Ableitungsansatz ließe sich dadurch konsolidieren, dass die Klasse der besonders schweren Delikte in sich unterteilt wird und für Informationen, die aus nachrichtendienstlichen Maßnahmen unterhalb der Eingriffsintensität der Wohnraumüberwachung stammen, bereits eine Höchststrafe von 5 Jahren genügt, jedenfalls wenn bei solchem Delikt qualifizierende Umstände hinzutreten, etwa die besondere Rechtsfeindlichkeit einer

politisch motivierten Körperverletzung, deren Unwertgehalt sich eben nicht im Körperverletzungserfolg erschöpft, sondern mit der extremistischen Zielrichtung geprägt wird durch die Bekämpfung der zentralen Grundprinzipien, die für den freiheitlichen Verfassungsstaat schlechthin unentbehrlich sind.

Im Ergebnis regelt der Absatz zwei Grundfälle der Übermittlung zur Strafverfolgung: Zum einen sind dies gemäß Absatz 2 Nummer 1 Delikte, die bereits mit ihrem Strafraumen von mehr als 5, also mindestens 10 Jahren Freiheitsstrafe als besonders schwer qualifiziert sind (wobei der Strafraumen des jeweiligen Tatbestandes maßgeblich ist, so dass z.B. § 267 Abs. 3 StGB erfasst ist, nicht hingegen Absatz 1). Zum anderen sind dies gemäß Nummern 2 bis 5 Delikte, die neben ihrem hohen Strafraumen von 5 Jahren weiterer Qualifikation bedürfen, um eine Übermittlung zu rechtfertigen. Diese zusätzliche Qualifikation folgt einerseits staatschutzspezifisch (Löffelmann, JR 2023, 1/10) aus den Besonderheiten des Delikts (Nummer 2) oder andererseits Besonderheiten der Tatbegehung, nämlich als Mittel der vom BfV nach § 3 Absatz 1 zu beobachtenden Bedrohungen (Nummer 3: Spionageabwehr; Nummer 4: Extremismusaufklärung), bzw. extremismusspezifischen Gefährdungspotenzials (Nummer 5). Taten in Bezug auf fremde Mächte werden dabei - angesichts deren Vorgehenstypik (nicht Einzeltaten zu begehen, sondern strategische Ziele fortgesetzt zu verfolgen) und dem ressourcengestützt herausragenden Gefährdungspotenzial einer fremden Macht - generell erfasst, weshalb auf eine zusätzliche Auflistung der für eine fremde Macht begangenen Staatsschutzdelikte (z.B. § 99 StGB) in Nummer 2 verzichtet werden kann. Ebenfalls nicht in Nummer 2 berücksichtigt, sind Fälle mit einer Höchststrafe von 10 Jahren, da diese bereits in Nummer 1 erfasst sind (weshalb z.B. bei § 96 StGB lediglich dessen Absatz 2 aufgeführt ist, denn dessen Absatz 1 ist bereits ein Fall der Nummer 1). Bei extremistischen Bestrebungen erfolgt dagegen noch eine rechtsgutsbezogene Differenzierung, die die allgemein übermittlungsrechtfertigenden Schutzgüter besonders berücksichtigt. Dabei ist auch hier mit zu gewichten, dass die Tat nicht isoliert als Allgemeinkriminalität, sondern Instrument von Bestrebungen ist, die gegen die zentralen Grundprinzipien, die für den freiheitlichen Verfassungsstaat schlechthin unentbehrlich sind, gerichtet sind.

Bei einer Gesamtwürdigung folgt die fachrechtliche Qualifikation als besonders schwere Straftat also nicht isoliert allein strafrechtlichen Gewichtigungen, sondern bezieht ein, dass die repressive Verfolgung von Straftätern zwangsläufig auch präventiv dem Schutz der Sicherheit dient (BVerfGE 150, 244 – Rn. 72). Dieser Aspekt geht notwendig und legitim in die Gewichtung der übermittlungsrechtfertigenden Gemeinwohlaspekte ein, die dadurch nicht deckungsgleich mit Strafraumen- und -zumessungserwägungen sind, weil diese im Präventionsanliegen schuldlimitiert bleiben müssen.

Die Übermittlung von Informationen, die einen Beschuldigten entlasten (auch bei Strafvorfällen unterhalb der hohen Schwelle nach Satz 1) ist nicht von den vom Bundesverfassungsgericht zur Strafverfolgung aufgestellten strengen Übermittlungsvoraussetzungen erfasst. Dem trägt § 25b bereits querschnittlich Rechnung, so dass es keiner besonderen Strafverfolgungsregelung dazu bedarf.

Die Übermittlungsverpflichtung zu Staatsschutzdelikten nach Absatz 3 greift die bisherige Verpflichtung nach § 20 Absatz 1 BVerfSchG auf. Wie auch in § 19 Absatz 3 führt der Bezug zur originären Verfassungsschutzaufgabe zur Reduktion des Übermittlungsermessens durch eine Übermittlungspflicht. In den Fällen des Absatzes 2 Nummern 2 bis 5 ist das per se der Fall, in den Fällen des Absatzes 2 Nummer 1 wird dies hingegen in Absatz 3 Nummer 1 als Voraussetzung aufgenommen.

Die besonderen Regelungen dieses Paragraphen beziehen sich auf die Übermittlung zur Strafverfolgung im Einzelfall, also zur entsprechenden operativen Verwendung mit personengerichteten Anschlussmaßnahmen. Diese operative Betrachtung der Folgerisiken für die betroffene Person liegt der Verhältnismäßigkeitsbetrachtung des Bundesverfassungsgerichts zugrunde. Übermittlungen an Strafverfolgungsbehörden, die einzelfallgelöst allgemeinen Aufgaben dienen sind von der Spezialregelung nicht erfasst, bemessen sich mithin

nach den Befugnissen in § 22 Absatz 3. Dies betrifft etwa die Bewertung der allgemeinen Gefahrenlage oder auch eine Einsatznachbereitung, die Probleme eines vorausgegangenen Verfahrens auswertet, um die Verfahrensweisen künftig zu optimieren. Solche Optimierung dient der Sicherheit des Bundes, Übermittlungen erfolgen also nach § 22 Absatz 3 Nummer 2. Die Weiterverarbeitung durch den Empfänger ist nach § 25 Absatz 2 beschränkt, d.h. eine Zweckänderung zur individuellen Strafverfolgung ist nach dessen Satz 1 Nummer 2 nur nach Maßgabe der hypothetischen Übermittlungszulässigkeit auch für diesen Zweck – und unter der Voraussetzung der Zustimmung des BfV – zulässig.

§ 21 trifft im Übrigen Spezialregelungen beschränkt auf die Übermittlung an Strafverfolgungsbehörden. Dies schließt die Strafvollstreckung ein. Dagegen nicht erfasst, also ebenso an §§ 19, 20 und 22 zu messen, sind Übermittlungen in Strafvollzugssachen an Justizvollzugsanstalten, etwa zur Vollzugsplanung mit dem Ziel der Resozialisierung des Gefangenen wie auch zur Verhütung radikalisierender Beeinflussung anderer Gefangener.

Zu § 22 (Übermittlung an inländische Stellen ohne operative Anschlussmaßnahmen)

Angesichts der Verhältnismäßigkeitsverknüpfung von Übermittlungsfolgen und -voraussetzungen werden solche Übermittlungen, die nicht auf außenwirksame Folgen für die betroffene Person zielen, erleichtert zugelassen. Voraussetzung ist in der Finalität der Schutz besonders gewichtiger Rechtsgüter (Bezug auf § 19 Absatz 2) und im Sachverhalt die konkrete Veranlassung (im Einzelfall). Erhöhte situative Schwellen sind hier dagegen nicht zu fordern. Allerdings dürfen die übermittelten Daten dann auch nicht zu Lasten der betroffenen Person außenwirksam eingreifend genutzt werden. Im Ergebnis betrifft der Absatz insbesondere einerseits die Nachrichtendienstliche Aufgabenwahrnehmung selbst sowie die informationelle Kooperation zur Erstellung gemeinsamer Erkenntnisprodukte.

Zu Absatz 1

Der Absatz schließt auch den Fall ein, dass Mitwirkungspflichten nach § 2 G 10 oder § 8a unter Einschaltung der Gewerbeaufsicht durchgesetzt werden. Es ist nicht auszuschließen, dass für die Sachverhaltsdarstellung des Pflichtverstoßes auch personenbezogene Daten zu dem Fall zu machen sind, in dem das Unternehmen seine Mitwirkungspflicht verletzt hat. Die so intendierten gewerbeaufsichtlichen Maßnahmen sind jedoch nicht gegen die Person gerichtet, zu der vorausgegangen mit nachrichtendienstlichen Mitteln Daten erhoben worden sind, sondern gegen das mitwirkungspflichtige Unternehmen.

Keiner besonderen Übermittlungsregelung bedarf eine Erkenntnisanfrage, etwa bei der Eingabe eines Abfragedatensatzes beim Datenabruf aus Registern wie dem Bundeszentralregister. Die hierin notwendig eingeschlossene Angabe der Person, zu der Daten erhoben werden, ist von der Erhebungs- bzw. Abrufbefugnis eingeschlossen. Dies gilt ebenso, wenn neben einem Identifizierungssatz weitere Angaben nötig sind, die die angefragte Stelle nicht für eigene Aufgaben, sondern allein zur Bearbeitung des Übermittlungsersuchens benötigt, oder wenn ein Ersuchen dauerhaft gestellt wird, etwa in Form einer „watch list“ oder als Ausschreibung in einem Informationssystem (vgl § 17 Absatz 2 und 3).

Zu Absatz 2

Absatz 2 entspricht dem bisherigen § 20 Absatz 1 Satz 3. Auch der Aufgabenbereich des BND ist von vornherein dadurch gekennzeichnet, dass er dem Schutz besonders gewichtiger Rechtsgüter dient (BVerfGE 155, 119 - Rn. 151). Eine zusätzliche Regelung für den Fall des Übermittlungsersuchens (bisheriger § 20 Absatz 2 Satz 2 – der zugleich Übermittlungsgrundlage ist, vgl. bisherigen § 21 Absatz 2) ist überflüssig. Die informationelle Zusammenarbeit mit den Landesverfassungsschutzbehörden und dem MAD – also innerhalb des Zweigs der Behörden mit den Aufgaben des nachrichtendienstlichen Verfassungsschutzes – ist gesondert in § 3 Absatz 3 MADG und § 6 geregelt, da es hier um dieselbe

Sachaufgabe mit lediglich im Verwaltungszweig gegliederten Zuständigkeiten geht (LfV's in örtlicher Gliederung, MAD in personeller Gliederung).

Zu Absatz 3

Absatz 3 Nummer 1 erfasst Erkenntnisprodukte der Gefahrerforschung, die nicht einzelfallbezogen auf Anschlussmaßnahmen ausgerichtet sind. Die Nummer beschränkt sich nicht auf analytische Projekte der Sicherheitsbehörden, z.B. im Gemeinsamen Terrorismusabwehrzentrum (wie Lagebilder zur abstrakten Beschreibung der allgemeinen Gefährdungslage oder Fallanalysen, zur Ermittlung von Vorgehensmustern sowie zur Erstellung allgemeiner Handlungskonzepte, die auf die allgemeine Lagebewertung, nicht individuelle Anschlussmaßnahmen zielen). Einbezogen sind auch Forschungsvorhaben in Kooperation mit wissenschaftlichen, beispielsweise universitären Forschungseinrichtungen. Auf eine besondere Forschungsregelung kann dabei auch künftig verzichtet werden. Ein eigener Zweck ist Forschung nicht, es ist vielmehr eine Methodik, mit der Erkenntnisziele verfolgt werden. Entscheidend ist also, ob das Forschungsvorhaben für Erkenntnisse erforderlich ist, die dem Schutz nach § 19 Absatz 2 dienen. Wesentliche Inhalte üblicher Forschungsregelungen (wie etwa § 476 StPO) sind im vorliegenden Zusammenhang bereits durch allgemeine Regelungen zum Geheimschutz und zur Zweckbindung der Weiterverarbeitung getroffen. Auf besondere Forschungseinschränkungen (vgl. etwa § 476 Absatz 1 Satz 1 Nr. 3 StPO – „erheblich überwiegt“) wird hingegen bewusst verzichtet, denn für die geistig-politische Auseinandersetzung mit extremistischen Phänomen besteht eine funktionale Äquivalenz einerseits der Behördenforschung im BfV und andererseits der Erforschung solcher Phänomene in externen wissenschaftlichen Einrichtungen. Allerdings setzen bereits allgemeine Geheimschutzanforderungen sowie Sicherheitsinteressen des BfV – speziell Methoden- und Quellenschutz – der Wissenschaftskooperation enge Grenzen.

Nummer 2 erfasst z.B. übliche Einsatznachbereitung nach Großlagen, die der künftigen Prozessoptimierung dienen und dazu fallbezogen – damit auch unter Verwendung personenebezogener Daten – vorausgegangene Defizite der abgeschlossenen Fallbearbeitung aufarbeiten, um bei künftigen vergleichbaren Fällen in den Abläufen optimiert zu handeln. Ebenfalls hierunter fielen Erfahrungsaustausche zur Verbesserung der Methodenkompetenz. Ebenso erfasst sind allgemeine Hinweise – z.B. auf phänomentypische Merkmale – an Stellen wie etwa FIU oder BAMF, die zu spontanübermittlungen an das BfV verpflichtet sind, um diesen zu ermöglichen, Verdachtstatsachen verbessert zu erkennen und gezielter auszusteuern.

Die in Absatz 3 aufgeführten Nummern sind nicht abschließend. Ein weiteres Beispiel betrifft etwa die analytische und informationelle Kooperation bei der Vorsorge zur Bewältigung künftiger Schadenslagen, etwa zum Bevölkerungsschutz nach einem Einsatz gemeingefährlicher Tatmittel, zu dem möglicherweise mit Erkenntnissen aus allgemeinen Tatvorbereitungen, z.B. allgemeinen Anleitungsunterlagen, die für die Bestrebungen genutzt werden („Terrorhandbücher“) beigetragen werden kann. Typischerweise wird solche Kooperation ohne eine Übermittlung personenbezogener Daten auskommen.

Ein weiteres Beispiel ist im Übrigen die Regelung des § 16. Die Aufgabe des Verfassungsschutzes durch Aufklärung der Öffentlichkeit erschöpft sich dabei nicht in der Veröffentlichungen, sondern kann z.B. auch die Zusammenarbeit mit zivilgesellschaftlichen Einrichtungen bei der Sensibilisierung der Öffentlichkeit oder auch bestimmter Zielgruppen einschließen, was die informationelle Grundlage in § 22 findet.

Bei einwilligungsbasierten Maßnahmen wie der Ausstiegshilfe für extremismusverstrickte Personen, beruht die Datenverarbeitung auf deren Einwilligung, so dass hierfür nicht auf § 22 zurückgegriffen werden muss.

Zu Nummer 4

Zu § 23 (Übermittlungsverbote)

Die Regelung greift den bisherigen § 23 auf, verbessert aber die Bestimmtheit der Norm speziell bei den Regelungen zur Verhältnismäßigkeit (Satz 1 Nummer 2 und Satz 2) sowie zur Abwägung kollidierender Sicherheitsinteressen (Satz 1 Nummer 3). Hier werden jeweils abwägungsleitende Vorgaben präzisiert.

Zu Nummer 1

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 § 19 Absatz 1 bzw. § 21 begrenzend. Zudem bleiben die Erhebungsumstände im Rahmen der konkreten Verhältnismäßigkeitswürdigung im Einzelfall zu betrachten (Nummer 2 Buchst. c).

Zu Nummer 2

In Satz 1 Nummer 2 sind mit 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 Persönlichkeitsreife. 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 Befugnisausgestaltung – Eingriffe bereits mit Verdachtserkenntnissen zu rechtfertigen – bewältigt wird).

Zu Nummer 3

Die Nummern 3 und 4 konkretisieren die im bisherigen § 23 Nummer 2 lediglich allgemein getroffene Vorgabe, zwischen Übermittlungszweck und kollidierenden Sicherheitsinteressen abzuwägen. Nummer 3 regelt die Kollision mit besonders wichtigen Individualrechtsgütern. Diese sollen besonders geschützt werden. Deshalb erfolgt hier eine Abwägung nur, wenn die Übermittlung ebenso dem Individualrechtsgüterschutz dient.

Zu Nummer 4

Gegenüber dem bisherigen § 23 Nummer 2 enthält die neue Nummer 4 im neuen zweiten Halbsatz zusätzlich eine abwägend gewichtende Vorstrukturierung zur Relevanz von Sicherheitsbelangen. Dies reagiert auch auf Kritik zur gegenwärtigen Regelung, über diese Übermittlungsschranke würden in der Verwaltungspraxis – der Dienstleisterrolle eines Nachrichtendienstes zuwider – behördliche Eigeninteressen gegenüber Bedarfsträgerinteressen sachwidrig übergewichtet. Solche Kritik ist bereits in der gegenwärtigen Praxis unbegründet, eine gesetzliche Regelung kann aber das Vertrauen in die dienstleisterorientierte Aufgabenwahrnehmung stärken.

Zu § 24 (Minderjährigenschutz)

Die Regelung knüpft am bisherigen § 24 Absatz 1 an (Auslandsübermittlungen sind in § 25a Absatz 4 Satz 2 speziell geregelt). Die bisherige Regelung bezieht sich auf

Speicherungen nach § 11 Absatz 1 Satz 1, also Daten über Minderjährige vor Vollendung des 14. Lebensjahres. Dies wird nunmehr normenklarer formuliert. Der bisherige § 24 Absatz 1 Satz 2, der Übermittlungen einschränkt, wenn die Speicherschwelle nach § 11 Absatz 1 Satz 1 nicht mehr vorliegt, wird nochmals enger gefasst. Die Befugnis nach § 19 wird dann rechtsgutsbezogen begrenzt und ist nach Nummer 1 nur bei konkretisierter Gefahr für besonders gewichtige Individualrechtsgüter zulässig. An sonstige Hoheitsverwaltung sind Übermittlungen nach § 20 nicht bereits wegen besonderer Risiken, auf die einzuwirken ist, zulässig, vielmehr müssen Anhaltspunkte für schädigendes Verhalten zur Person bestehen, die allerdings nicht die Prognosequalität einer konkretisierten Gefahr erreichen müssen.

Zu § 25 (Weiterverarbeitung durch Empfänger)

Zu Absatz 1

Absatz 1 entspricht dem bisherigen § 25, wobei die dort noch auf Dokumente ausgerichtete Formulierung („Unterlagen zu vernichten“) allgemeiner auf – auch elektronische – Datenverarbeitung bezogen wird.

Zu Absatz 2

Absatz 2 greift den bisherigen § 19 Absatz 1 Satz 3 auf, regelt die Zweckbindung verbreitert und ergänzt sie mit sichernden Verfahrensregelungen.

Die Zweckbindung schließt insbesondere auch die Nutzung der übermittelten Daten für eine Strafverfolgung für andere als in § 21 bezeichnete Straftaten nach § 160 Absatz 4 StPO aus (diese strafprozessuale Regelung ermöglicht zugleich die entsprechende Strafverfolgungsbeschränkung in den Landesverfassungsschutzgesetzen). Unbenommen bleibt indes die strafrechtliche Würdigung einer Tat, die die Voraussetzungen nach § 21 erfüllt, unter allen rechtlich einschlägigen Gesichtspunkten. Wenn die mitgliedschaftliche Beteiligung an einer kriminellen - extremistischen – Vereinigung (§ 129 StGB – Fall des § 21 Absatz 2 Nr. 4 Buchst. a) im Wege einer Sachbeschädigung erfolgt (§ 303 StGB – kein Fall des § 21), kann und muss dies Tateinheitlich in die Strafzumessung eingehen.

§§ 20, 22 enthalten ebenfalls besondere Bindungen, die eine Weiterverarbeitung zur operativen Zwangsanzuwendung bzw. sonstigen Belastungsakten mit unmittelbarer Außenwirkung ausschließen. Entstehen nachträglich die solche Anschlussmaßnahmen rechtfertigenden situativen Voraussetzungen (konkretisierte Gefahr im Sinne von § 19 Absatz 1 bzw. konkretes Risiko im Sinne von § 20 Absatz 1) oder werden diese Voraussetzungen nachträglich bekannt, kann mithin im Wege der Zustimmung nach § 25 Absatz 2 Satz 1 Nummer 2 der Ausschluss einer Weiterverarbeitung zur Zwangsausübung oder anderen Belastungsakten aufgehoben werden.

Zu Absatz 3

Absatz 3 gewährleistet Transparenz, wenn die betroffenen Person aufgrund einer Übermittlung verfassungsschutzrelevanter Erkenntnisse Nachteile im Rahmen einer vorbeugenden Personenüberprüfung erleidet, etwa keine Akkreditierung zum Zugang zu Sicherheitsbereichen erhält (die beispielsweise bei internationalen Veranstaltungen mit besonders gefährdeten Personen zu deren Schutz eingerichtet werden) oder mangels Eignung keine Projektförderung im Rahmen von Programmen der Extremismusprävention. Die Regelung betrifft Übermittlungen im Rahmen der allgemeinen nachrichtendienstlichen Aufgabe nach § 3 Absatz 1. Soweit das BfV an Personenüberprüfungen nach § 3 Absatz 2 mitwirkt, ergeben sich Informationsrechte der betroffenen Personen auch aus den speziellen Fachgesetzen, beispielsweise aus § 23 SÜG.

Soweit im Ergebnis des Verfahrens ein Verwaltungsakt ergeht, der in Rechte der betroffenen Person eingreift, sind die tragenden Gründe in einer Verwaltungsstreitsache ohnehin offen zu legen, einschließlich der Quelle entscheidungserheblicher Informationen. Die Regelung des Absatzes 3 betrifft im Ergebnis vornehmlich nachteilige Entscheidungen der Leistungsverwaltung, speziell wenn auf den begehrten Vorteil kein Anspruch besteht.

Zu § 25a (Auslandsübermittlungen)

Die Regelung passt den bisherigen § 19 Absatz 3 BVerfSchG bei den Übermittlungszwecken an die Verfassungsrechtsprechung an (BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17 - Rn. 260 ff., 379 f.). Dabei wird die Auslandsübermittlung in den Voraussetzungen grundsätzlich mit den Inlandsübermittlungen synchronisiert. Da sich die Auslandszusammenarbeit vornehmlich zwischen Nachrichtendiensten vollzieht, also grundsätzlich auf ausschließlich informationelle Anschlussnutzung gerichtet ist, bildet dabei § 22 die Basisreferenz, speziell auch mit dem allgemeinen Ausschluss exekutiver Verwendung (in Absatz 1 und 3). Liegen die Schwellen-Voraussetzungen der §§ 19, 20 (also konkretisierte Gefahr bzw. konkrete Risikosachverhalte) vor, kann nach Absatz 4 die Übermittlung auch für exekutive Maßnahmen erfolgen, bzw. die Informationsnutzung dafür nachträglich auf Anfrage zugelassen werden.

Zu Absatz 1

Satz 1 bezeichnet die zulässigen Zwecke, zu denen die Übermittlung im Einzelfall erforderlich sein muss, wobei die Erforderlichkeit allein auf eine informationelle Nutzung ohne intervenierende Außenwirkung bezogen wird, da der Empfänger hierauf grundsätzlich beschränkt ist (Absatz 3 Satz 1 Nummer 2). Nummer 1 korrespondiert dem § 22. Das Schutzgut der Sicherheit eines anderen Staates korrespondiert dabei der Sicherheit des Bundes, erfasst mithin nicht jedwedes Schutzinteresse der inneren Sicherheit, sondern die Funktionsfähigkeit des Staates (vgl. § 4 Absatz 1 Satz 1 Buchstabe b). Nummer 2 führt zusätzlich die Aufklärung von Straftaten auf. Dies bezieht sich gemäß Satz 2 nicht auf justizielle Strafverfolgung, sondern mit dem Ausschluss exekutiver Anschlussmaßnahmen allein die Aufklärung (auch dies ohne exekutive Eingriffe). Die Weitergabe an die Justiz zur Strafverfolgung bleibt mit Absatz 4 Satz 1 Nummer 3 an die Verdachtsverdichtung entsprechend § 21 gebunden. Dies betrifft lediglich die empfängerseitige Weiterverwendung. Eine Direktzusammenarbeit des BfV mit Justizstellen des Empfängerstaates findet grundsätzlich nicht statt und darf auch nicht die Rechtshilfeverfahren unterlaufen (Satz 3).

Satz 4 entkoppelt die grundsätzliche Synchronisierung insoweit, als Staatsschutzzwecke dann nicht übermittlungsrechtfertigend sein können, wenn es um die Sicherheit eines anderen Staates geht, diese im Lichte der grundgesetzlichen Werteordnung aber nicht schützenswert ist. Diese Beschränkung ist unabhängig davon, ob im konkreten Übermittlungsfall zusätzlich auch noch Risiken für den Übermittlungsbetroffenen entstehen (die Schutznorm dazu enthält Absatz 3 Nummer 2 Buchstabe b). Die tatbestandliche Beschreibung dieser Anforderungen folgt der Staatspraxis entsprechender Regelungen (etwa § 22b Absatz 1 Nummer 2 BVerfSchG oder § 28 Absatz 2 Nummer 4 und Absatz 3 Nummer 1 BKAG), wobei im vorliegenden Regelungszusammenhang zusätzlich das Demokratieprinzip hinzutritt (da es nicht lediglich um die Gewährleistung von Individualrechten, sondern die Schutzwürdigkeit der Staatsordnung geht).

Zu Absatz 2

Der Übermittlungsausschluss berücksichtigt bei Konkretisierung des in Nummer 3 geregelten Betroffenen schutzes durch Satz 2 und 3 sowohl die bereits nach dem BKAG-Urteil (BVerfGE 141, 220 – Rn. 325 ff.) angepasste Praxis der Bundesgesetzgebung (etwa in § 28 Absatz 2 BKAG) wie auch die aktuelle Entscheidung des Bundesverfassungsgerichts zum Bay. Verfassungsschutzgesetz (Urteil vom 26. April 2022 - 1 BvR 1619/17), wonach dessen Art. 25 Absatz 3 Satz 2 verfassungsrechtlich nicht zu beanstanden ist.

Zu Absatz 3

Absatz 3 begrenzt entsprechend dem Übermittlungszweck die Übermittlungsfolgen mit Satz 1 Nummer 2 durch grundsätzlich generellen Ausschluss exekutiver Anschlussmaßnahmen (nicht nur Zwangsausübung). Die Übermittlung erfolgt mithin nicht nur zu diesem Zweck, sondern auch unter dieser Bedingung. Dies ist für die Zusammenarbeitspraxis unschädlich, da typischerweise der Empfänger auf ausländischer Seite ebenso ein Nachrichtendienst ist und solche Übermittlung in der Zusammenarbeitspraxis grundsätzlich entsprechend § 22 lediglich zur informationellen Nutzung unter Ausschluss exekutiver Anschlussmaßnahmen erfolgt. Die im nationalen Recht getroffene Regelung bindet den Empfänger zwar nicht rechtlich. Internationale Zusammenarbeit im nachrichtendienstlichen Bereich beruht aber auf Vertrauen und Verlässlichkeit. Ist der Partner bei der Einhaltung auch lediglich informeller Regelungen unzuverlässig, riskiert er, dass die Zusammenarbeitsbeziehung beendet wird. Dies schafft faktisch in der Zusammenarbeitspraxis eine wirksame informelle Bindung an die Grundlagen der Zusammenarbeit. Im Übrigen ist eine etwaige Unzuverlässigkeit bei der Beachtung der Verwendungsbeschränkung auch in der Folgenabschätzung nach Absatz 2 Nummer 3 zu berücksichtigen.

Zu Absatz 4

Sofern die Belange nach Absatz 2 nicht entgegenstehen (Satz 3), eröffnet Satz 1 Ausnahmen von der allgemeinen Weiterverarbeitungsbeschränkung des Absatzes 3 unter den dazu für die entsprechende inländische Verwendung mit §§ 19 bis 21 geregelten Schwellenvoraussetzungen. Die exekutive Anschlussnutzung nach Nummer 3 bezieht sich auf die Verwendung als konkreter Ermittlungs- und Spurenansatz im Ermittlungsverfahren, etwa für einen Durchsuchungsbeschluss. Eine Verwendung zu Beweis Zwecken für ein Strafurteil bliebe im Rechtshilfeverfahren zu klären.

Satz 2 enthält in Anlehnung an den bisherigen § 25 Absatz 2 eine Regelung zum Minderjährigenschutz bei einer belastenden Anschlussnutzung, die einerseits tatbestandlich restriktiver ist, indem die Übermittlung im Einzelfall für die besonders wichtigen Zwecke erforderlich sein muss (bisher: wenn solches Erfordernis nicht ausgeschlossen werden kann), auf dieser Grundlage angesichts der herausragenden Schutzgüter (konkrete Gefahr für Leib oder Leben einer Person) auf eine Mindestalterregelung (bisher: 14 Jahre) jedoch verzichtet.

Zu Absatz 5

Absatz 5 ermöglicht die ausnahmsweise Übermittlung auch an nichtöffentliche Stellen. Dafür ist die Zustimmung der Amtsleitung nach § 27 Absatz 3 Satz 1 erforderlich.

Zu Absatz 6

Absatz 6 trägt dem Umstand Rechnung, dass einer Auslandsübermittlung womöglich eine inländische Abklärung vorausgehen muss, etwa im informationellen Austausch mit dem BND.

Zu § 25b (Übermittlungen zum Schutz betroffener Personen)

Die Formulierung lehnt sich an § 23 Absatz 1 Nummer 1 BDSG an.

Die neue Regelung soll dem Schutz betroffener Personen auch in atypischen - insofern von den vorausgegangenen 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 Betroffenen zum Schutz 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 § 8 Absatz 1 Satz 1, 2. Halbsatz die Übermittlungsgrundlage. Typischerweise wird dem BfV jedoch 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.

Zu § 25c (Weitere Verfahrensregelungen)

Zu Absatz 1

Die 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, Kontrollen zu erleichtern, Rechnung. Sie greift hierzu über die bereits im geltenden Recht enthaltenen speziellen Dokumentationspflichten hinaus (bisherige § 19 Absatz 3 Satz 1 und § 19 Absatz 4 Satz 3) und ermöglicht damit gezielte Kontrollen u.a. auch zu den nach der Verfassungsrechtsprechung sensiblen Übermittlungen nach §19, an die 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, die die Regelung des § 6 Absatz 3 Satz 5 aufgreift, 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. Für solche Daten, wie etwa die Dokumentation von Ausgängen im Vorgangsbearbeitungssystem des BfV oder Vorgangsvermerke in Sachakten, gelten keine besonderen Zweckbindungs- oder Lösungsregelungen, vielmehr gelten die jeweiligen Regelungen für die Fachverarbeitung, dies auch soweit Annotationen (Angabe der Rechtsgrundlage) zu Kontrollzwecken erfolgen. Einer speziellen Kontrollregelung bedarf es nicht, da solche Sekundärnutzung immer (nicht nur zu Protokolldaten) zulässig ist.

Zu Absatz 2

Der Absatz greift die Regelung des § 29 Absatz 14 BNDG auf (komplementär auch zur entsprechenden Speicherungsregelung in § 10 Absatz 2 und der Vernichtungsausnahme des bisherigen § 25a Satz 3 bzw. neuen § 25 Absatz 1 Satz 2). Ein Bedarfsfall ist etwa die

Weitergabe technischer Aufzeichnungen, etwa der Videodatei einer Observation, die typischerweise auch unbeteiligte Dritte im öffentlichen Raum erfasst, die unter Umständen bestimmbar wären, so dass 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, u.U. auch für das Forschungsvorhaben methodisch unzutraglich.

Zu Absatz 3

Absatz 3 behält ein besonderes Entscheidungsverfahren für Übermittlungen an nichtöffentliche Stellen bei (bisher § 19 Absatz 4 Satz 2) bei, sieht dafür aber künftig die Zuständigkeit der Behördenleitung (Präsident/Präsidentin und Vizepräsidenten/Vizepräsidentinnen) vor, da es sich um operative Verwaltungsentscheidungen handelt, die nicht sachgerecht (auch nicht besser) auf ministerieller Ebene zu treffen sind. Die Ausübung von Fachaufsicht bleibt hiervon unberührt. Das BfV ist angewiesen, für die Aufgabenwahrnehmung bedeutsame Dienstvorschriften vorzulegen. Dies schließt auch künftige allgemeine Regelungen für gleichgelagerte Übermittlungsfälle nach Absatz Satz 2 ein.

Satz 3 übernimmt die Mitteilungsregelung des bisherigen § 19 Absatz 4 Satz 7. Die Regelung findet keine Anwendung bei Übermittlungen zum Zwecke der Datenerhebung (so ausdrücklich bisheriger § 19 Absatz 5). Dies ergibt sich bereits aus der annexen Verbindung mit dem Erhebungsvorgang und erfordert keine besondere gesetzliche Regelung.

Zu § 25d (Nicht nachrichtendienstlich erhobene Informationen)

Die besonderen Übermittlungsvoraussetzungen und Maßgaben der vorausgehenden Vorschriften sind Folgeregelungen zur Datenerhebung mit nachrichtendienstlichen Mitteln, die den Besonderheiten solcher heimlichen Eingriffe spezifisch Rechnung tragen. Für anderweitig gesammelte Informationen sind sie mithin nicht sachlich einschlägig. Dazu trifft § 25d einerseits eine offenere Übermittlungsregelung, stellt dabei aber zugleich klar, dass etwaige besondere Weiterverarbeitungsvorschriften zu beachten sind. Dies betrifft gleichermaßen vom BfV erhobene Daten (speziell § 8b Absatz 2 Satz 7) wie auch zuvor von anderen Stellen übermittelte Daten (z.B. § 25 Absatz 6 BKAG).

Zu Nummer 5

Der neue § 26a knüpft an den bisherigen § 21 an. Eine Regelung zu Übermittlungen an den MAD ist im Bundesverfassungsschutzgesetz überflüssig, da dies – sachnäher – bereits in § 3 Absatz 3 MADG geregelt ist. Die Übermittlung zwischen den Verfassungsschutzbehörden ist in § 6 Absatz 1 BVerfSchG geregelt.

Zu Nummer 6

Zu § 26b (Besondere Eigensicherungsbefugnisse)

Zu Absatz 1

§ 26b fasst speziell für den Eigenschutz des BfV erforderliche Befugnisse zusammen. Absatz 1 enthält hierzu eine allgemeine Zweckbestimmung. Der behördliche Eigenschutz ist als Funktionssicherung in der Fachaufgabe der Natur der Sache nach eingeschlossen (ebenso wie z.B. Personalgewinnung). Zuständigkeiten und Befugnisse, die sich bereits allgemein aus der Ausübung des Hausrechts ergeben, bleiben durch die Regelung spezieller Befugnisse in § 26b unberührt. Hierzu zählen insbesondere die räumliche Sicherung der Dienststellen, Grundstücke und sonstigen Einrichtungen (Eigensicherungsbereich) gegen unbefugten Zugang und Ausspähung sowie die vorbeugende Personenüberprüfung anlässlich der Zutrittskontrolle oder der Kontrolle der Berechtigung zum Aufenthalt auch

innerhalb der Einrichtungen. Ebenso gehört hierzu die Kontrolle von Diensträumen. Müssen Gegenstände in den Diensträumen durchsucht werden, ist dies nicht mehr vom Hausrecht gedeckt, sondern bedarf einer gesonderten Regelung (Absatz 4). Die Befugnis zur Eigensicherung erstreckt sich auch auf die unmittelbare Umgebung der Dienststellen und Einrichtungen.

In den nachfolgenden Absätzen werden spezifische Befugnisse ergänzend gesetzlich geregelt. Der Bedarf nach verbesserter Eigensicherung ist auch Konsequenz von Spionagefällen, in denen es ausländischen Nachrichtendiensten gelang, Beschäftigte eines deutschen Nachrichtendienstes anzuwerben und zur Ausforschung des Dienstes einzusetzen. Die Verarbeitung personenbezogener Daten ist im für die Funktionssicherung der Fachaufgaben des BfV erforderlichen Umfang nach den allgemeinen Vorschriften des BVerfSchG zulässig. Der Begriff der „sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten“ entspricht hier der Verwendung in § 9 Absatz 1 Satz 1 Nummer 2 BVerfSchG, nicht jedoch der Bedrohung nach § 3 Absatz 1 Nummer 2 BVerfSchG, denn hier bezieht sich der Normgegenstand nicht ausschließlich auf den Schutz vor fremden Mächten. Sicherheitsgefährdend sind im Zweckzusammenhang der Eigensicherung solche Tätigkeiten, die geeignet sind, die Funktionsfähigkeit des Bundesamtes für Verfassungsschutz zu beeinträchtigen, also insbesondere auch solche, die den Geheimschutz gefährden. Einerseits soll verhindert werden, dass Personen, die Zugang zu Verschlusssachen haben oder diesen im Zusammenhang mit dem Zutritt zu einer Dienststelle, einem Grundstück oder einer sonstigen Einrichtung des BfV haben, geheimhaltungsbedürftige Informationen entgegen den rechtlichen Bestimmungen außerhalb der in Absatz 2 näher bestimmten Gelände verbringen können. Andererseits soll auch Gefahren durch das Einbringen gefährlicher Gegenstände begegnet werden, mit denen beispielsweise Anschläge gegen Personen oder Sachen durchgeführt werden können oder die dazu dienen können, Tätigkeiten auf dem Gelände zu überwachen.

Zu Absatz 2

Absatz 2 regelt die Befugnis zur vorbeugenden Personenüberprüfung bei Gewährung des Zutritts zum oder des Aufenthalts im Eigensicherungsbereich (einschließlich des Verlassens) unter Einbezug mitgeführter Gegenstände. Im Eigensicherungsbereich des BfV ist beispielsweise das Mitführen von Kameras (auch Smartphones mit Kamera) oder anderer Datenträger zum Schutz vor sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten oder die Mitnahme von Verschlusssachen außerhalb des Eigensicherungsbereichs untersagt. Nach Maßgabe der Nummer 1 kann dies routinemäßig oder stichprobenhaft auch verdachtsunabhängig – auch unter Einsatz technische Mittel, wie etwa eines Mobilfunkdetektors – kontrolliert werden. Da nicht in jeder Dienststelle des BfV die Durchführung der verdachtsunabhängigen Kontrollen an den Ein- und Ausgängen, z.B. aufgrund baulicher Gegebenheiten, möglich und hinreichend ist, kann die Kontrolle auch auf dem Gelände der Dienststellen erfolgen, soweit dies zum Eigenschutz erforderlich ist.

Eine weitergehende Durchsuchung ist nach Nummer 2 nur bei Vorliegen tatsächliche Anhaltspunkte für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten zulässig. Die Maßnahmen stehen auch dann zur Verfügung, wenn Personen sich im Eigensicherungsbereich aufhalten, insbesondere auch beim Verlassen.

Zu Absatz 3

Absatz 3 enthält Begriffsbestimmungen zu Kontrollen und Durchsuchungen von Personen und Gegenständen nach § 26 b Absatz 2 und dient der Abgrenzung und Begrenzung der jeweiligen Befugnisse. Die Befugnisse zur Kontrolle und Durchsuchung nach Gegenständen schließen Gegenstände, die von einer Person mitgeführt werden, wie beispielsweise auch Taschen und mitgeführte Koffer sowie die Kontrolle oder Durchsuchung mit Hilfe von technischen Mitteln mit ein. Eine weitergehende körperliche Untersuchung der betroffenen Person selbst ist in jedem Fall unzulässig; eine solche kann nur durch die Polizei nach den hierfür geltenden Vorschriften vorgenommen werden.

Zu Absatz 4

Absatz 4 regelt zum Schutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten notwendige Befugnisse zur Sicherstellung oder Durchsuchung oder sonstigen Untersuchung von Gegenständen, die in den Eigensicherungsbereich eingebracht wurden. Nach der Vorschrift können potenzielle Tatmittel wie beispielsweise eine Kamera oder ein Smartphone, die auf das Gelände wegen der allgemeinen Ausforschungsfahr nicht mitgebracht werden dürfen, in Besitz genommen und untersucht werden, ob sie zu einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit genutzt worden sind. Soweit die Befugnis nicht bereits gegenständlich anknüpft (Gegenstände, die keiner bestimmten Person zugeordnet werden können, nach Nummer 2), sondern einen Verdacht aufgrund tatsächlicher Anhaltspunkte im Einzelfall voraussetzt (Nummer 1), können die verdachtsbegründenden Informationen auch mit nachrichtendienstlichen Mitteln gewonnen worden sein, da hier zwar als Anschlussmaßnahme auch die zwangsweise Sicherstellung droht, Anlass aber die im Befugnistatbestand bezeichnete, situativ konkretisierte Gefahr ist. Gegenstände, die vom Dienstherrn ausschließlich zur dienstlichen Nutzung überlassen worden sind, wie etwa dienstliche Behältnisse oder dienstliche Informations- und Kommunikationstechnik, müssen nicht sichergestellt werden, da der Dienstherr bereits aufgrund des Eigentums berechtigt ist, die Herausgabe zu verlangen.

Die Befugnis schließt auch die verdachtsabhängige Durchsuchung verschlossener Gegenstände, die zur privaten Nutzung überlassen wurden, mit ein. Verschlossene Gegenstände, die zur privaten Nutzung überlassen wurden, sind insbesondere Kleiderschränke, sowie Schreibtischfächer, sowie sonstige verschlossene Behältnisse, in welchen z.B. elektronische Speichermedien aufbewahrt werden könnten. Bereits die Kontrolle ist nur unter der Voraussetzung zulässig, dass tatsächliche Anhaltspunkte dafür vorliegen, dass diese Gegenstände für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten genutzt werden und muss durch die Amtsleitung angeordnet sein (§ 26c Absatz 1).

Zu Absatz 5

Absatz 5 Satz 1 regelt eine Mitwirkungspflicht bei Kontrollen und Durchsuchungen nach Absatz 2 für die Personen, die sich im Eigensicherungsbereich des BfV aufhalten sowie Sicherstellungsmaßnahmen nach Absatz 4. Die Vorschrift trägt damit der besonderen Risikosituation des Aufenthalts im Eigensicherungsbereich des BfV Rechnung, die eine vorbeugende Überprüfung zum Erkennen und zur Abwehr von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten rechtfertigt. Weitere Mitwirkungspflichten können sich aus besonderen Rechtsverhältnissen heraus auch bereits beim Betreten ergeben.

Satz 2 erstreckt komplementär zu Satz 1 die Befugnisse nach Absatz 2 und 4 auch noch auf das unmittelbare Umfeld des Eigensicherungsbereichs, soweit dies erforderlich ist um die Maßnahme bei einer zur Mitwirkung nach Satz 1 verpflichteten Person durchzuführen und abzuschließen. Hierdurch werden Fälle erfasst, in denen eine mitwirkungspflichtige Person sich entgegen der Mitwirkungspflicht nach Satz 1 Maßnahmen nach Absatz 2 und 4 durch Verlassen des Geländes zu entziehen versucht, so dass sicherheitsgefährdende oder geheimdienstliche Tätigkeiten nicht aufgedeckt oder verhindert werden könnten. Die Befugnis ist auf die unmittelbare Nähe des Eigensicherungsbereichs beschränkt und ermöglicht in diesem Bereich die Durchsetzung der Maßnahmen nach § 26c Absatz 7, insbesondere auch das Festhalten der betroffenen Person. Der Begriff der „unmittelbaren Nähe“ wird bereits in den Standardregelungen des Polizeirechts zur Identitätsfeststellung im Umfeld zu schützender Objekte verwendet (z.B. § 23 Absatz 1 Nummer 4 und Absatz 2 Nummer 2 des Bundespolizeigesetzes). Das dortige Begriffsverständnis kann auch hier zur Auslegung und Durchführung der Norm herangezogen werden. Wird eine Person bereits bei dem Versuch des Betretens zurückgewiesen, da ihre Zugangsberechtigung nicht besteht oder nicht nachgewiesen werden kann, stellt dies keinen Fall des Satzes 2 dar; der Sinn der Kontrolle, die Verhinderung des Zutritts, ist in diesem Fall erfüllt.

Zu Absatz 6

Absatz 6 ermöglicht die verdachtsunabhängige offene Überwachung innerhalb des Eigensicherungsbereichs einschließlich von Diensträumen mit optisch-elektronischen Mitteln. Die Überwachung ist offen, wenn auf sie durch geeignete Mittel hingewiesen ist. Die Überwachung muss dem Schutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten dienen und verhältnismäßig sein. Die Überwachung von Arbeitsräumen, die ausschließlich durch eine bestimmte Person genutzt werden und eine permanente Beobachtung dieser Person ermöglichen würden, sowie die Überwachung von Sanitär- oder Umkleideräumen sind nach Satz 3 ausgeschlossen; die Nutzung der Daten zur Leistungskontrolle der Behördenangehörigen ist nicht statthaft. Die Datenspeicherung im Rahmen der Aufzeichnung ist auf den erforderlichen Umfang strikt zu beschränken und eine unverzügliche Löschung vorzusehen, wenn die Daten zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der betroffenen Personen einer weiteren Speicherung entgegenstehen. Bei der Festlegung der Höchstspeicherdauer ist die Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen der Datenschutzkonferenz vom 17. Juli 2020 zu berücksichtigen. Die näheren Voraussetzungen für eine offene Überwachung, insbesondere deren Voraussetzungen, die Festlegung der von einer Überwachung grundsätzlich ausgeschlossenen Räumlichkeiten sowie geeignete Möglichkeiten des Hinweises auf die Überwachung, sind in einer Dienstvorschrift zu benennen. Eine verdeckte Überwachung ist nur nach Maßgabe des Absatzes 8 zulässig.

Zu Absatz 7

Absatz 7 beinhaltet eine spezifische Befugnis zum Schutz vor unbemannten Fluggeräten, die sich in unmittelbarer Nähe zum Eigensicherungsbereich befinden. Für Maßnahmen nach Absatz 7 gelten die allgemeinen und spezifischen Verhältnismäßigkeitsvorgaben in Absatz 9. Ermöglicht werden durch die Befugnis die Detektion und Abwehr (in der Regel durch Übernahme der Steuerung) von unbemannten Fluggeräten. Die Regelung trägt damit dem Umstand Rechnung, dass sicherheitsgefährdende oder geheimdienstliche Tätigkeit bereits jetzt und zukünftig vermehrt nicht nur von Personen, sondern auch konkret von unbemannten technischen Systemen ausgehen können. Deren Nutzung in dem in § 21h Absatz 3 Nummer 4 der Luftverkehrsordnung bezeichneten Bereich ist daher unzulässig.

Zu Absatz 8

Absatz 8 erstreckt besondere Befugnisse, die zur Aufklärung von Bedrohungen nach § 3 Absatz 1 bestehen, auch auf die Aufklärung sicherheitsgefährdender Tätigkeiten von Beschäftigten des BfV und sonstigen Personen, die mit sicherheitsempfindlichen Tätigkeiten (§ 1 Absatz 2 SÜG) betraut oder beauftragt sind, im Eigensicherungsbereich tätig zu sein. Diese Erweiterung des materiellen Befugnistatbestands ist für Sachverhalte nötig, bei denen die sicherheitsgefährdende Tätigkeit tatbestandlich keine Bedrohung im Sinne des § 3 Absatz 1 ist, beispielsweise wenn Außenstehende geschützte Informationen über Beschäftigte für andere Zwecke, etwa für kommerzielle oder allgemein kriminelle Zwecke beschaffen (zum Begriff der „sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten“ s. die Begründung zu Absatz 1). Dass neben Beschäftigten auch Beauftragte einbezogen werden, trägt dem Umstand Rechnung, dass das BfV insbesondere im Bereich seiner Informationstechnik auf externe Dienstleister angewiesen ist, mit deren Zugangsmöglichkeiten zugleich gewichtige Risiken für die operative Sicherheit des BfV entstehen können. Auch insoweit hat die Tätigkeit von Innentätern besonderes Gefährdungspotenzial für die Funktionsfähigkeit der Behörde und das Vertrauen der Bevölkerung darin. Auch bei Anwendung der im materiellen Tatbestand erweiterten Befugnisse sind die jeweiligen speziellen Verfahrensmaßgaben, insbesondere § 8b, zu beachten.

Zu Absatz 9

Maßnahmen der Eigensicherung haben das Verhältnismäßigkeitsgebot nach § 8 Absatz 5 zu beachten. In Absatz 9 wird klarstellend die Verhältnismäßigkeit auch der speziellen Eigensicherungsbefugnisse nach § 26b geregelt.

Zu § 26c (Verfahren; Kernbereichsschutz)

Zu Absatz 1

In Absatz 1 sind querschnittlich Vorgaben zu Anordnungen geregelt. Eine innerbehördliche Einsatzfreigabe ist für die Maßnahmen nach § 26b Absatz 2 Nummer 2, Absatz 4 und Absatz 6 vorgesehen. Dabei wird bezüglich der Anordnungszuständigkeit entsprechend des Gewichts des Eingriffs zwischen der zuständigen Abteilungsleitung und der Amtsleitung differenziert. Die Anordnung hat eine verfahrenssichernde Funktion und dient damit dem Schutz des Betroffenen.

Die Anordnung muss inhaltlich bestimmt sein, d.h. speziell den Anlass der Maßnahme in der Begründung ausführen und ist nach den Grundsätzen der Aktenführung in der Verwaltung zu dokumentieren.

Zu Absatz 2

Absatz 2 enthält eine Eilfallregelung für den Fall, dass der Zweck der Maßnahme bei Einholung einer vorherigen Anordnung vereitelt oder wesentlich erschwert würde, was etwa bei Gefahr im Verzug angenommen werden kann. Diese kann beispielsweise eintreten, wenn das Kontrollpersonal im Rahmen seiner Tätigkeit entdeckt, dass ein Gerät der Informations- und Kommunikationstechnik unbefugt im Eigensicherungsbereich eingesetzt wird. In diesem Fall darf das Kontrollpersonal die erforderlichen Maßnahmen (z.B. Durchsuchung der Person oder Sicherstellung eines Gerätes der Informations- oder Kommunikationstechnik) ohne vorherige Anordnung durchführen.

Nach Satz 2 darf bei Geräten der Informations- oder Kommunikationstechnik ohne vorherige Anordnung jedoch lediglich das Herausgabeverlangen bzw. die Sicherstellung des Gerätes der Informations- oder Kommunikationstechnik erfolgen. Für die Auswertung privater oder privatdienstlicher IT ist in jedem Fall eine Anordnung notwendig. Das Anordnungsverfahren ist unverzüglich nachzuholen.

Zu 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 Herausgaberegung 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 5 Satz 3 bis 5.

Zu Absatz 4

Absatz 4 Satz 1 regelt das Anwesenheitsrecht der betroffenen Person bei Kontrollmaßnahmen nach § 26b Absatz 2 Nummer 2. Weil nach § 26b 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 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 Gefährdungspotential, wobei zusätzlich von einem größere Verbreitungs- und Weitergabepotential 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 § 26b Absatz 4 gewährleistet, nach dem auch die lediglich anlassbezogene Untersuchung sichergestellter mobiler Informations- und Kommunikationstechnik zulässig ist. Der Tatbestand des § 26b Absatz 4 knüpft dabei ausschließlich an Informations- und Kommunikationstechnik an, die auf dem Gelände der Liegenschaften des BfV aufgefunden wurden. Dadurch ist der Anwendungsbereich örtlich begrenzt und inhaltlich strikt auf die Aufgaben und Zwecke der Eigensicherung 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 3 unabhängig vom Abschluss der Untersuchung nach § 26b Absatz 4 spätestens nach zwei Wochen zu erfolgen. Macht die betroffene Person die Notwendigkeit einer früheren Herausgabe geltend, ist dies angemessen zu berücksichtigen. Satz 4 und 5 enthält 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 Geräts aus familiären oder gesundheitlichen Gründen).

Zu Absatz 6

Absatz 6 enthält eine spezifische Regelung zum Kernbereichsschutz. Untersuchungen nach § 26b 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. Satz 5 bis 7 enthalten Kernbereichsschutz-spezifische Dokumentationsvorgaben zu Kontrollzwecken und damit korrespondierende Löschungspflichten.

Zu Absatz 7

Absatz 7 enthält eine spezifische Befugnis zur zwangsweisen Durchsetzung von Maßnahmen nach § 26b Absatz 2 und 4 ausschließlich gegenüber Personen, die nach § 26b Absatz 5 mitwirkungspflichtig sind. Die Zwangsmittel sind auf den spezifischen Sonderbereich der Eigensicherung begrenzt und in Absatz 7 abschließend enumerativ geregelt. Der Begriff der Hilfsmittel der körperlichen Gewalt wird bereits in § 2 UZwG verwendet, nach Absatz 7 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. Das Bundesamt für Verfassungsschutz hat dafür Sorge zu tragen, dass die Beschäftigten entsprechend ausgebildet werden.

Zu Absatz 8

Absatz 8 regelt die sofortige Vollziehbarkeit der Maßnahmen nach § 26b. 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 Artikel 2 (Änderung des MAD-Gesetzes)

Der Artikel trifft Folgeregelungen, die sich aus Artikel 1 für das MAD-Gesetz ergeben. Eine entsprechende Verweisungsanpassung im BND-Gesetz ist durch den parallelen Entwurf eines Gesetzes zur Änderung des BND-Gesetzes obsolet.

Zu Nummer 1

Mit der Regelung wird der bisherige § 22 BVerfSchG systematisch naheliegender in § 10 MADG integriert.

Zu Nummer 2

Es handelt sich um eine Folgeregelung zu Artikel 1 Nummer 3.

Zu Nummer 3

Es handelt sich um eine Folgeregelung zu Artikel 1 Nummer 3.

Zu Nummer 4

Zu § 15 Absatz 1

Aufgrund eines mutmaßlichen Verratsfalls im Jahr 2022 bei einem Nachrichtendienst wurde der Bedarf an Stärkung von Maßnahmen zur Eigensicherung deutlich. Ziel der gesetzlichen Neuregelung ist es, den Militärischen Abschirmdienst vor den Gefahren sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten zu schützen und Informationsabflüsse aus dem Militärischen Abschirmdienst heraus zu verhindern. Aufgrund der gleichen Interessenlage zwischen dem Bundesamt für Verfassungsschutz und dem Militärischen Abschirmdienst bietet sich ein Verweis in die entsprechenden Vorschriften des Bundesverfassungsschutzgesetzes an.

Zu § 15 Absatz 2

Absatz 2 stellt deklaratorisch dar, dass das Gesetz über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen über die besonderen Befugnisse der Eigensicherung hinaus weiter Anwendung findet.

Zu Nummer 5

Es handelt sich um eine Folgeänderung zu Nr. 4.

Zu Artikel 3 (Änderung des Sicherheitsüberprüfungsgesetzes)

Der Artikel trifft die im Sicherheitsüberprüfungsgesetz nötige Folgerung zu Artikel 1 Nummer 3.

Zu Artikel 4 (Änderung des Artikel 10-Gesetzes)

Zu Nummer 1

Die Änderung in Nummer 1 beschränken Übermittlungen zusätzlich auf den nach den neuen Übermittlungsvorschriften vorgegebenen, engeren Rahmen. Im Rahmen der raschen Umsetzung des Beschlusses des Bundesverfassungsgerichts erfolgt die Anpassung des Artikel 10-Gesetzes dabei minimalinvasiv. Dazu wird die Gesetzessystematik klargestellt, wonach § 4 Absatz 4 G 10 nicht selbst Befugnisgrundnorm ist, sondern eine zweckbegrenzende Ergänzungsnorm, die die anderen Vorschriften zu entnehmende Übermittlungsbefugnis speziell einschränkt. Bei der Gesetzesanwendung ist also zunächst unter die eigentliche Übermittlungsbefugnis zu subsumieren und kumulativ dann noch unter die Einschränkungen in § 4 Absatz 4 G 10. Beispielhaft erläutert werden kann dies für Übermittlungen des BfV an Strafverfolgungsbehörden. Die allgemeine Übermittlungsbefugnis ergibt sich dabei aus § 21 BVerfSchG, dessen Voraussetzungen also vorliegen müssen. Dies reicht zur Übermittlung aber noch nicht, wenn die Daten mit dem besonderen nachrichtendienstlichen Mittel der G10-Maßnahme erhoben worden sind. Hier ist dann in einer zweiten Stufe auch die besondere Einschränkung nach § 4 Absatz 4 Nummer 2 G 10 zu prüfen. Erst wenn auch diese ergänzende Voraussetzung erfüllt ist, dürfen die G10-Daten übermittelt werden. Bei einer wertungskonsistenten Gesamtregelung, die mit dem nachfolgenden 2. Reformgesetz erfolgen wird, wäre eine grundlegendere Anpassung angezeigt.

Zu Nummer 2

Bei der Änderung in Nummer 2 handelt es sich um eine Folgeregelung zu Nummer 1. Die danach erfolgende kumulative Anwendung der allgemeinen Vorschriften bezieht u.a. auch den neuen § 25a BVerfSchG sowie speziell dessen Absatz 2 mit ein. Eine besondere Regelung zu Auslandsübermittlungen ist für den Fall des § 4 Absatz 4 Satz 1 Nummer 3 G 10 verzichtbar, da für diesen Zweck ohnehin keine Auslandsübermittlungen erfolgen.

Zu Artikel 5 (Inkrafttreten)

Zu Absatz 1

Das Gesetz soll schnellstmöglich, also am Tag nach seiner Verkündung in Kraft treten.

Zu Absatz 2

Die technische Auswertbarkeit der die Übermittlung protokollierenden Daten setzt eine dies ermöglichende Revision des Datenmanagementsystems voraus, deren Umsetzung eine

Vorlaufzeit erfordert. Die Kapazitätsgrenzen des für die Umsetzung nötigen technischen Dienstleisters des BfV eröffnen keine kurzfristigere Umsetzung.