

# **Sicherheitsrecht des Bundes – Recht der Nachrichtendienste in Deutschland**

von

**Prof. Dr. Kurt Graulich**  
**Richter am Bundesverwaltungsgericht a.D.**

Humboldt-Universität zu Berlin – Sommersemester 2018

Raum UL9 E 25

Donnerstag, d. 31.05.2018 von 10.00 bis 12.00 Uhr

Schwerpunkt 5

Veranstaltungsnummer 10727

## **Skizze und Materialien**

**fff) Speicherung, Veränderung und Nutzung personenbezogener Daten  
nach § 10 ff. BVerfSchG**

**ggg) Verwendung und Berichtigung personenbezogener Daten in Akten nach  
§ 13 BVerfSchG**

**hhh) Auskunft an den Betroffenen nach § 15 BVerfSchG**

**iii) Berichtspflicht des BfV nach § 16 BVerfSchG**

### **bb) Übermittlungsvorschriften**

**aaa) Zulässigkeit von Ersuchen (§ 17 BVerfSchG)**

**bbb) Übermittlung von Informationen an die Verfassungsschutzbehörden  
(§ 18 BVerfSchG)**

**ccc) Übermittlung von personenbezogenen Daten durch das BfV  
(§ 19 BVerfSchG)**

**a1) Übermittlung an Staatsanwaltschaften, Finanzbehörden, Polizeien, die  
Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen  
(Abs. 1)**

**b1) Übermittlung an Dienststellen der Stationierungstreitkräfte (Abs. 2)**

**c1) Übermittlung an ausländische öffentliche Stellen sowie an über- und  
zwischenstaatliche Stellen (Abs. 3)**

**d1) Übermittlung an andere Stellen, wenn dies zum Schutz der fdGO, des  
Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur  
Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen  
Einrichtungen nach § 1 Abs. 4 SÜG erforderlich ist (Abs. 4)**

**e1) Übermittlung an Dienststellen von denen die Daten erhoben werden  
(Abs. 5)**

**ddd) Übermittlungsverbote (§ 23 BVerfSchG)**

**eee) Minderjährigenschutz (§ 24 BVerfSchG)**

**fff) Pflichten des Empfängers (§ 25 BVerfSchG)**

**ggg) Nachberichtspflicht (§ 26 BVerfSchG)**

**cc) Gemeinsame Dateien**

**aaa) Projektbezogene gemeinsame Dateien (§ 22a BVerfSchG)**

**bbb) Errichtung gemeinsamer Dateien mit ausländischen  
Nachrichtendiensten (§ 22b BVerfSchG)**

**ccc) Teilnahme an gemeinsamen Dateien mit ausländischen  
Nachrichtendiensten (§ 22c BVerfSchG)**

**dd) Anwendung des Datenschutzgesetzes (§ 27 BVerfSchG)**

**fff) Speicherung, Veränderung und Nutzung personenbezogener Daten  
nach § 10 ff. BVerfSchG**

Das BfV darf nach § 10 BVerfSchG zur Erfüllung seiner Aufgaben personenbezogene **Daten in Dateien speichern, verändern und nutzen**, wenn 1. tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG vorliegen, 2. dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG erforderlich ist oder 3. das BfV nach § 3 Abs. 2 BVerfSchG tätig wird. Die Regelung in **§ 10 BVerfSchG** über die Speicherung in Dateien **ergänzt die bereits nach § 8 Abs. 1 Satz 1 BVerfSchG bestehende Befugnis des Bundesamtes für Verfassungsschutz, personenbezogene Daten u.a. zu verarbeiten**, wozu nach allgemeiner datenschutzrechtlicher Terminologie auch das Speichern gehört (§ 3 Abs. 4 Satz 1 BDSG). Entsprechendes gilt für § 4 Abs. 1 BNDG, der durch die Bezugnahme auf § 10 BVerfSchG die dem BND bereits durch § 2 Abs. 1 BNDG eingeräumte Befugnis, personenbezogene Daten zu verarbeiten und damit auch zu speichern, um die Befugnis ergänzt, personenbezogene Daten unter bestimmten Voraussetzungen in Dateien zu speichern (BVerwG, Urteil vom 28. November 2007 – 6 A 2/07 –, BVerwGE 130, 29-39, Rn. 21).

Die Regelung ist in § 10 Abs. 2 BVerfSchG durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes geändert worden. Der neue Abs. 2 ist insbesondere für eine **praktikable Erfassung des Ursprungsdokumentes**, das einer Speicherung zugrunde liegt, erforderlich. Diese **Belegdokumente** sind vor allem in gemeinsamen Datenbanken des Verfassungsschutzverbundes nach § 6 BVerfSchG durchgängig einzustellen, um die Erfassungsvoraussetzungen unmittelbar zu dokumentieren und verfügbar zu machen. Sie können allerdings zugleich auch Daten zu Personen enthalten, die nach § 10 Abs. 1, der nach § 6 Satz 2 (bzw. § 6 Abs. 2 Satz 2 n. F.) ebenso für Verbunddateien gilt, grundsätzlich nicht in Dateien gespeichert werden dürfen (z. B. weitere Daten in Presseartikeln). Die Regelung betrifft ebenso andere Unterlagen, wie z. B. Bild und Tonträger. Entsprechendes gilt auch für Unterlagen, die unter anderem im Fachinformationssystem der Verfassungsschutzbehörden – einer Datenbank mit Grundlagenwissen (Urteile, Gutachten, Berichte, Publikationen, etc.) – eingestellt werden, soweit darauf § 10 zur Anwendung kommt. Daten „Dritter“ sind dabei Daten zu Personen, die nicht dem § 10 Absatz 1 unterfallen. Eine Abfrage dieser Daten ist nach Satz 2 unzulässig. **Eine spezielle Prüfungs- und Lösungsregelung für die Belegdokumente ist nicht erforderlich**, da sich § 10 Absatz 2 auf Belegdokumente zu einer Speicherung auf § 10 Absatz 1 bezieht. Ist die belegte Speicherung nach § 10 Absatz 1 weiterhin erforderlich, dann ist auch die Belegspeicherung nach § 10 Absatz 2 zulässig. Ist diese nach den §§ 12 und 11 nicht mehr erforderlich, erfolgt mit der Löschung der personenbezogenen Daten auch die Löschung des Belegdokuments (BT-Drs. 18/4654 S. 29).

**ggg) Verwendung und Berichtigung personenbezogener Daten in Akten nach  
§ 13 BVerfSchG**

Stellt das BfV fest, daß **in Akten gespeicherte personenbezogene Daten unrichtig** sind oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies gem. § 13 Abs. 1 BVerfSchG in der Akte zu vermerken oder auf sonstige Weise festzuhalten. § 13 Abs. 1 und 2 BVerfSchG betrifft das **Vorgehen bei unrichtigen Akten** sowie die **Sperrung von Akteninhalten**. Die Abs. 3 und 4 sind durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes angefügt worden.

Der neue § 13 Abs. 3 BVerfSchG enthält – entsprechend einer Empfehlung des NSU-UA (Nummer 35) – die gesetzliche **Regelung zur Vernichtung von Akten**. Aus Gründen der Aktenvollständigkeit kann eine Vernichtung erst erfolgen, wenn die jeweilige Akte insgesamt nicht mehr zur Aufgabenerfüllung erforderlich ist. Die Regelung umfasst auch die Fälle, in denen eine Akte von Anfang an nicht hätte geführt werden dürfen. Um klare Regelungen zu schaffen und dem Datenschutz Rechnung zu tragen, wird eine Prüffrist für die Erforderlichkeit eingeführt. Ferner wird festgelegt, dass Akten, die zu einer Person im Sinne des § 10 Abs. 1 Nr. 1 geführt werden, analog zur Regelung in § 12 Abs. 3 Satz 2 BVerfSchG zu vernichten sind. Um den Schutz des Persönlichkeitsrechts der Betroffenen zu gewährleisten, enthält die Vorschrift darüber hinaus eine **Sperrregelung** (z. B. im Fall eines laufenden Auskunftsverfahrens). Die Vorschrift macht ferner deutlich, dass sie **keine dem Bundesarchivgesetz (BArchG) vorgehende Rechtsvorschrift ist** und deshalb Akten, die zu vernichten bzw. zu löschen wären, dem Bundesarchiv anzubieten und zu übergeben sind, soweit ihnen ein bleibender Wert im Sinne von § 3 BArchG zukommt. Auch sonstige spezialgesetzliche Lösungsregelungen wie § 4 Absatz 1 G 10 bleiben unberührt (BT-Drs. 18/4654 S. 29 ff.).

Der neue Abs. 4 regelt die **elektronische Aktenführung**. Ihrem Zweck nach sind die Dateiregelungen des BVerfSchG nicht auf Akten, die speziellen Anforderungen der Aktenführung unterliegen, anwendbar, unabhängig von der Form der Aktenführung (in Papier oder elektronisch). Andererseits sind den Dateiregelungen jedoch allgemeine Rechtsgedanken zu entnehmen, die auch auf die Nutzung elektronischer Akten übertragbar sind. Im Interesse der Rechtssicherheit erfolgt deshalb eine ausdrückliche Regelung. Die Regelung geht davon aus, dass **eine in elektronischer Form geführte Akte wie eine herkömmliche Papierakte zu behandeln ist**. Die Vorschrift geht daher insbesondere davon aus, dass die elektronischen Akten den bisherigen Papierakten in Bezug auf die Befugnis zur Speicherung personenbezogener Daten gleichstehen. Die Befugnis zur Speicherung personenbezogener Daten durch das BfV kann bei einer elektronischen Aktenführung schon mit Blick auf den **Grundsatz der Aktenvollständigkeit nicht auf bestimmte Personengruppen beschränkt** sein. Für die elektronische Akte bedarf es somit eines anderen rechtlichen Rahmens als bei einer Datei. Auch bei dieser zeitgemäßen Form der Aktenführung bildet wie bei der Papierakte § 8 Abs. 1 Satz 1 und nicht §§ 10 und 11 Abs. 1 Satz 3 die Grundlage. Andernfalls könnte das BfV beispielsweise nicht aus Pressemeldungen, Jahrbüchern und sonstigen öffentlich zugänglichen Publikationen gewonnenes Hintergrundmaterial zu fremden Nachrichtendiensten und den entsprechenden ausländischen Staaten im Volltext in der elektronischen Akte speichern, da diese in aller Regel auch personenbezogene Daten, z. B. über maßgebliche Personen des dortigen öffentlichen Lebens, enthalten. Auch extremistische Publikationen könnten nicht im Volltext gespeichert werden, wenn sie sich z. B. mit den Auffassungen von namentlich

benannten Politikern, Wissenschaftlern, Künstlern oder sonstigen Personen des öffentlichen Lebens agitatorisch auseinandersetzen. Um den **Schutz der Persönlichkeitsrechte der Mitbetroffenen** wirksam und umfangreich zu gewährleisten, ist nach Satz 3 eine Abfrage personenbezogener Daten mittels automatisierter Verarbeitung nur zulässig, wenn die Voraussetzungen des § 10 Abs. 1 oder § 11 Abs. 1 Satz 3 vorliegen. Sind also – beispielsweise durch das Einscannen von Papierdokumenten – Daten über Personen mitgespeichert worden, deren Kenntnis nur zum Verständnis des Kontexts eines Sachverhalts erforderlich sind, bleibt eine **datenschutzrechtlich relevante automatisierte Abfrage dieser Personen unzulässig**. Da eine Auswertung von Informationen zu diesen Personen grundsätzlich nicht zu den Aufgaben des BfV zählt, bleibt die Erfüllung dieser Aufgaben hiervon unbeeinträchtigt. Darüber hinaus wird der **Minderjährigenschutz** dadurch sichergestellt, dass eine elektronische Abfrage von Daten oder über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres nur unter den engen Voraussetzungen des § 11 Abs. 1 Satz 3 zulässig ist. Diese Regelung zum automatisierten Zugriff auf die elektronische Akte stellt somit sicher, dass **die besonderen Regelungen für Dateien nicht durch die Möglichkeiten des automatisierten Zugriffs auf die elektronischen Akten umgangen werden**. Ferner müssen die Grundsätze der Aktenführung – wie Aktenvollständigkeit – ebenso auf die elektronische Akte Anwendung finden. Demgemäß kommen die speziellen Regelungen der Abs. 1 bis 3 in § 13 zur Berichtigung, Sperrung und Löschung von Daten zur Anwendung und nicht etwa § 12. Soweit zur erleichterten Nutzung von Akteninhalten Auszüge aus Akten in Dateien gespeichert werden, kommen ebenfalls die Aktenregelungen zur Anwendung, weil auch der Aktenauszug weiter als Aktenstück einheitlich zu behandeln ist. Satz 4 lässt einen automatisierten Abgleich von e-Akten mit Dateien nur anwendungsgebietsbegrenzt zu. Damit wird ausgeschlossen, sämtliche Akten als einen verbundenen Datenbestand systematisch für komplexe Suchanfragen im Volltext zu nutzen. Ausgeschlossen wird somit die unspezifische Suche über die Gesamtheit aller Akten, nicht aber ein zielgerichteter Abgleich mit vor diesem Hintergrund ausgewählten Akten. Da auch dieser automatisierte Abgleich wie jede Abfrage nach Satz 3 auf personenbezogene Daten beschränkt ist, die nach § 10 Abs. 1 in Dateien gespeichert werden dürfen (keine Auswertung nach unbeteiligten Dritten), wäre eine solche Aktenauswertung bei fehlerloser Datenpflege im NADIS verzichtbar. Eine vollständig fehlerfreie Bearbeitung ist aber bei Massenvorgängen nicht zu gewährleisten. Speziell im Zuge jüngster Untersuchungsausschüsse bestand deshalb die parlamentarische Forderung, die Informationsrecherche nicht nur über das NADIS, sondern unmittelbar im Aktenbestand vorzunehmen (BT-Drs. 18/4654 S. 30).

Um die Kontrolle der Einhaltung der Nutzungsbeschränkungen verfahrensmäßig zu sichern, gelten besondere **Protokollierungspflichten** (BT-Drs. 18/4654 S. 31).

### **hhh) Auskunft an den Betroffenen nach § 15 BVerfSchG**

Nach der Regelung in § 15 BVerfSchG hat die Behörde dem Betroffenen über zu seiner Person gespeicherte Daten **auf Antrag unentgeltlich Auskunft** zu erteilen, soweit er hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer

Auskunft darlegt, sofern keiner der in der Vorschrift genannten Gründe vorliegt, aus denen die Auskunftserteilung zu unterbleiben hat. § 15 BVerfSchG gehört zu den auf dem Volkszählungsurteil beruhenden gesetzlichen Ausgestaltungen von Auskunftsrechten und -pflichten, mit denen das Gesetz dem in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG enthaltenen Grundrecht auf informationelle Selbstbestimmung Rechnung trägt und es den Bürgern ermöglicht, gegebenenfalls gerichtlichen Rechtsschutz gegen einen unrechtmäßigen Umgang mit Daten in Anspruch zu nehmen (BVerfG, Kammerbeschluss vom 10. Oktober 2000 - BvR 586/90 u.a. - a.a.O. Rn. 6 - 8). Da § 7 BNDG auf die Regelung in § 15 BVerfSchG für den Fall der Datenspeicherung Bezug nimmt, ist dem vom Bundesverfassungsgericht aus dem informationellen Selbstbestimmungsrecht abgeleiteten Anspruch - mindestens - auf einen Auskunftsanspruch nach Maßgabe einer Abwägung dadurch zu entsprechen, dass diese Vorschrift ungeachtet der missverständlichen Verweisung auf die Aufgabenerfüllung nach § 4 BNDG und der dortigen Weiterverweisung auf §§ 10 und 11 BVerfSchG im Wege der verfassungskonformen Auslegung auf den gesamten Anwendungsbereich des § 15 BVerfSchG und damit auch auf solche personenbezogenen Daten erstreckt wird, die sich in Akten befinden. Die Abwägung von Auskunftsinteressen und Geheimhaltungsbedürfnissen geschieht dann in dem von § 15 BVerfSchG vorgezeichneten Rahmen (BVerwG, Urteil vom 28. November 2007 – 6 A 2/07 –, BVerwGE 130, 29-39, Rn. 30).

### iii) Berichtspflicht des BfV nach § 16 BVerfSchG

Das BfV unterrichtet nach § 16 Abs. 1 BVerfSchG das BMI über seine Tätigkeit. Diese interne Berichtspflicht ist Ausfluss des Behördenaufbaus und der **Minister-Verantwortlichkeit gegenüber dem Parlament**, die nicht ohne substantielle Information ausgefüllt werden kann. Die Unterrichtung des BMI durch das BfV über dessen Tätigkeit gemäß § 16 Abs. 1 BVerfSchG schließt auch die Unterrichtung über die Befassung des Bundesamts mit Fällen des bloßen Verdachts verfassungsfeindlicher Bestrebungen im Sinne von § 3 Abs. 1 BVerfSchG ein, die ausweislich von § 4 Abs. 1 Satz 3 BVerfSchG von seinem Tätigkeitskreis mit umfasst ist. § 16 Abs. 1 BVerfSchG ist keine Eingrenzung dahingehend zu entnehmen, dass insoweit die Tätigkeit des Bundesamtes von der Unterrichtung des BMI auszunehmen wäre. Eine solche Eingrenzung wäre mit der umfassenden **Ressortverantwortung des BMI für das BfV** (vgl. § 2 Abs. 1 Satz 2 BVerfSchG) auch nicht in Einklang zu bringen (BVerwG, Urteil vom 26. Juni 2013 – 6 C 4/12 –, Rn. 16, juris)

**Die Unterrichtung nach § 16 Abs. 1 BVerfSchG dient gem. § 16 Abs. 2 Sätze 1 und 2 BVerfSchG auch der Aufklärung der Öffentlichkeit durch das BMI über Bestrebungen und Tätigkeiten nach § 3 Abs. 1 BVerfSchG, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. Dabei dürfen auch personenbezogene Daten bekanntgegeben werden, wenn die Bekanntgabe für das Verständnis des Zusammenhanges oder der Darstellung von Organisationen oder unorganisierten Gruppierungen erforderlich ist und die Interessen der Allgemeinheit das schutzwürdige Interesse des Betroffenen überwiegen. Die Auslegung, wonach diese Norm das BMI auch zur Unterrichtung über den bloßen Verdacht verfassungsfeindlicher Bestrebungen im Sinne von § 3 Abs. 1 Nr. 1 BVerfSchG**

ermächtigt, überschreitet zwar in materieller Hinsicht nicht den verfassungsrechtlich gesteckten Rahmen. Nach dem Beschluss des BVerfG aus dem Jahr 2005 in dem Verfahren über die Verfassungsbeschwerde der "Junge Freiheit" stehen bei entsprechender gesetzlicher Ermächtigung verfassungsrechtliche Bedenken einer Unterrichtung der Öffentlichkeit über Verdachtsfälle nicht entgegen, sofern die tatsächlichen Anhaltspunkte für verfassungsfeindliche Bestrebungen hinreichend gewichtig sind, um die Veröffentlichung in Verfassungsschutzberichten auch angesichts der nachteiligen Auswirkungen auf die Betroffenen zu rechtfertigen (BVerfG, Beschluss vom 24. Mai 2005 - 1 BvR 1072/01 - BVerfGE 113, 63 <80 ff.>). § 16 Abs. 2 Satz 1 BVerfSchG lässt sich jedoch nicht mit der gebotenen Bestimmtheit entnehmen, dass er tatsächlich in formeller Hinsicht eine entsprechende Ermächtigung ausspricht, d.h. das BMI über die - eindeutig von der Norm erfassten - Fälle hinaus, in denen Gewissheit über verfassungsfeindliche Bestrebungen besteht, auch zur Berichterstattung in Fällen befugt, in denen tatsächliche Anhaltspunkte erst einen dahingehenden **Verdacht** begründen (BVerwG, Urteil vom 26. Juni 2013 - 6 C 4/12 -, Rn. 12, juris). Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I 2015 S. 1938) hat **§ 16 Abs. 2 Satz 1 BVerfSchG mit dem Ziel neugefasst, dass zukünftig auch über Verdachtsfälle berichtet werden kann**. Diese Änderung hat dem voranstehenden Judikat den Boden entzogen.

**Nicht jedes staatliche Informationshandeln und nicht jede Teilhabe des Staates am Prozess öffentlicher Meinungsbildung ist als Grundrechtseingriff zu bewerten** (vgl. BVerfGE 105, 252 <265 ff.> - zu Art. 12 Abs. 1 GG -; 105, 279 <294 ff., 299 ff.> - zu Art. 4 Abs. 1 GG -). Maßgebend ist, ob der Schutzbereich eines Grundrechts berührt wird und ob die Beeinträchtigung einen Eingriff oder eine eingriffsgleiche Maßnahme darstellt. **Das ist bei der Nennung der Beschwerdeführerin im Verfassungsschutzbericht zu bejahen** (BVerfG, Beschluss vom 24. Mai 2005 - 1 BvR 1072/01 -, BVerfGE 113, 63-88, Rn. 50). Der Hinweis im Verfassungsschutzbericht eines Landes auf den Verdacht verfassungsfeindlicher Bestrebungen eines Presseverlags kommt einem Eingriff in die Pressefreiheit gleich und bedarf deshalb der Rechtfertigung durch ein allgemeines Gesetz im Sinne des Art. 5 Abs. 2 GG (BVerfG a.a.O.).

### **bb) Übermittlungsvorschriften**

Im Dritten Abschnitt des BVerfSchG befinden sich die **Regelungen über die Übermittlung von Daten** unter Einschluss darauf bezogener Regelungen des Datenschutzes (§§ 17 bis 22a BVerfSchG). Sie beinhalten teils die besonderen Prinzipien des Datenschutzes (§§ 23 bis 26 BVerfSchG) und teils bestimmen sie die Anwendbarkeit des BDSG (vgl. § 27 BVerfSchG). Dabei sind anlassbezogene Übermittlungen personenbezogener Daten zwischen je besonderen Behörden (§§ 17 bis 21 BVerfSchG) von der Übermittlung in Form der befristeten Errichtung gemeinsamer projektbezogener Dateien (§ 22a Abs. 1 und 4 BVerfSchG) zu unterscheiden (Mallmann/Bock in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, vor § 17 BVerfSchG). Die Übermittlungsvorschriften im BVerfSchG bleiben noch hinter den Anforderungen zurück, welche das BVerfG am 20.04.2016 in seinem Urteil zu den heimlichen Überwachungsmaßnahmen im BKAG aufgestellt hat. Insbesondere fehlt es an einer Positivierung des aus dem verfassungsrechtlichen

Verhältnismäßigkeitsgrundsatz abgeleiteten Grundsatzes der hypothetischen Datenneuerhebung im Falle der Datenübermittlung. Die dazu maßgeblichen Grundsätze hat das BVerfG in folgende Leitsätze gefasst:

Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung. (Rn.276)

(a) Die Reichweite der Zweckbindung richtet sich nach der jeweiligen Ermächtigung für die Datenerhebung; die Datenerhebung bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren.

b) Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus im Rahmen der ursprünglichen Zwecke dieser Daten erlauben (weitere Nutzung). Dies setzt voraus, dass es sich um eine Verwendung der Daten durch dieselbe Behörde zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter handelt. Für Daten aus Wohnraumüberwachungen oder einem Zugriff auf informationstechnische Systeme müssen zusätzlich für jede weitere Nutzung auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sein. (Rn.279)

(c) Der Gesetzgeber kann darüber hinaus eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung). (Rn.284).

Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung orientieren sich am **Grundsatz der hypothetischen Datenneuerhebung**. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Eine konkretisierte Gefahrenlage wie bei der Datenerhebung ist demgegenüber grundsätzlich nicht erneut zu verlangen; erforderlich aber auch ausreichend ist in der Regel das Vorliegen eines konkreten Ermittlungsansatzes. (Rn.287)

Für Daten aus **Wohnraumüberwachungen** und **Online-Durchsuchungen** darf die Verwendung zu einem geänderten Zweck allerdings nur erlaubt werden, wenn auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sind. (Rn.291)

(BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378)

**Ohne eine gesetzliche Neuregelung ist der verfassungsrechtlichen Anforderung des BVerfG mit dem vorhandenen Gesetz nicht gerecht zu werden.** Die nachfolgenden Ausführungen ignorieren daher zwangsläufig dieses Manko. Es werden einige der Übermittlungsnormen vorgestellt.

#### **aaa) Zulässigkeit von Ersuchen (§ 17 BVerfSchG)**

Wird nach den Bestimmungen des Dritten Abschnittes des BVerfSchG um Übermittlung von personenbezogenen Daten ersucht, dürfen nach § 17 Abs. 1 BVerfSchG nur die Daten übermittelt werden, die bei der ersuchten Behörde bekannt sind oder aus allgemein zugänglichen Quellen entnommen werden können. Es handelt sich bei der Regelung um eine Form der **Zweckbindung** bei der Datenweitergabe. Die Regelung konkretisiert den Rechtsgrundsatz der **Amtshilfe** – angesichts des



Trennungsgebotes – für die Zusammenarbeit der VS-Behörden mit andere Behörden (Bock in Schenke/Graulich/Ruthig BVerfSchG § 17 Rn. 1).

§ 17 Abs. 1 BVerfSchG gilt nach § 17 Abs. 2 Satz 1 BVerfSchG nicht für besondere Ersuchen der Verfassungsschutzbehörden, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes um solche Daten, die bei der **Wahrnehmung grenzpolizeilicher Aufgaben** bekannt werden. Da die Dienstanweisung des Bundesministeriums des Innern auch Ersuchen des MAD und des BND regelt, ist sie im Be nehmen mit Bundeskanzleramt und Bundesministerium der Verteidigung zu erlassen. Die speziellen Regelungen zum MAD und BND bedürfen dabei des Einvernehmens der zuständigen obersten Bundesbehörde. Die Änderung übernimmt zugleich die sächliche Behördenbezeichnung (BT-Drs. 16/2921 S. 16).

Mit der Aufhebung der Personenkontrollen an den Binnen- grenzen des Schengen-Raumes sind grenzüberschreitende Verkehre nur noch begrenzt über die Ausschreibung zur Grenzfehndung gemäß § 17 Abs. 2 BVerfSchG i. V. m. § 31 Abs. 7 des Bundespolizeigesetzes (BPolG) zu erfassen. Die hierdurch entstandene Lücke soll mit der dafür gemein- schaftlich vorgesehenen Ausschreibungsmöglichkeit im Schengener Informationssystem und der damit notwen- dig verbundenen Ausschreibung im nationalen polizeilichen Informationssystem INPOL geschlossen werden.

Dazu wird im neuen § 17 Abs. 3 die entsprechende natio- nale Ausschreibung geregelt. Ein allgemeiner schreibender und lesender Zugriff der Nachrichtendienste auf INPOL ist damit nicht verbunden. Die Ausschreibung im INPOL dient lediglich der Möglichkeit einer Ausschreibung im Schen- gener Informationssystem (SIS). Diese Befugnis ergibt sich auf dieser Grundlage dann aus Artikel 99 Abs. 3 des Schen- gener Durchführungsübereinkommens vom 15. Juli 1993 – SDÜ – (BGBl. 1993 II S. 1010) in der Fassung des Rats- beschlusses 2005/211/JI vom 25. Februar 2005 über die Einführung neuer Funktionen für das SIS, auch im Hinblick auf die Terrorismusbekämpfung (Abl. EG Nr. L 68 S. 44). Danach ist die Ausschreibung auf Veranlassung der für die Sicherheit des Staates zuständigen Stellen zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die gemäß der Ausschreibung zu übermittelnden Informationen zur Abwehr einer von dem Betroffenen ausgehenden erheb- lichen Gefährdung oder anderer erheblicher Gefahren für die innere oder äußere Sicherheit des Staates erforderlich ist. Die Nachrichtendienste sind dabei Sicherheitsbehörden im Sinne dieser Regelung.

Da nur die durch den Wegfall der Binnengrenzkontrollen eingeschränkte Möglichkeit der Grenzfehndung kompen- siert werden soll, wird die Ausschreibung nur bei tatsäch- lichen Anhaltspunkten für grenzüberschreitende Verkehre mit Ausgangs- oder Zielpunkt in Deutschland zugelassen. Die neuen Ausschreibungsmöglichkeiten werden also wei- terhin nur im Hinblick auf die besonderen Gefahren inter- nationaler extremistischer Bestrebungen und Tätigkeiten fremder Nachrichtendienste zur Feststellung grenzüber- schreitender Sachverhalte eingeräumt. Als Komplementäre- lement zur Ausschreibung im SIS wird auch die nationale Ausschreibung zudem nur unter den materiellen Zulässig- keitsvoraussetzungen einer SIS-Ausschreibung eingeräumt.

Nach Artikel 99 Abs. 1 SDÜ, der nach dem neuen § 17 Abs. 3 BVerfSchG zugleich für die nationale Ausschreibung maßgeblich sein soll, ist eine Sachfahndung nach Fahrzeugen, Wasserfahrzeugen, Luftfahrzeugen und Containern möglich.

Von der gemeinschaftsrechtlichen Möglichkeit einer Ausschreibung zur gezielten Kontrolle wird nicht Gebrauch gemacht, es soll vielmehr national und somit auch schengenweit nur eine Ausschreibung zur verdeckten Registrierung möglich sein. Die Ausschreibung veranlasst nicht die Kontrolle, vielmehr setzt die Kontrollmitteilung eine für polizeiliche Aufgaben durchgeführte Kontrolle voraus. Dem nachrichtendienstlichen Erkenntnisbedarf wird lediglich bei Gelegenheit polizeilicher Aufgabenwahrnehmung Rechnung getragen, ohne dass polizeiliche Befugnisse für nachrichtendienstliche Aufgaben ausgeübt werden. § 8 Abs. 3 BVerfSchG bleibt unberührt (BT-Drs. 16/2921 S. 16). Nach dieser speziellen Regelung dürfen auch im Rahmen des Artikels 99 Abs. 4 SDÜ keine polizeilichen Maßnahmen für den ersuchenden Nachrichtendienst vorgenommen werden, die dieser, wäre er bei der polizeilichen Kontrolle vor Ort, nicht auch selbst vornehmen könnte.

Für den Bereich des Verfassungsschutzes wird die Ausschreibungsmöglichkeit wegen des vorausgesetzten Auslandsbezugs lediglich dem Bundesamt, nicht den Landesbehörden eingeräumt, da auch die Pflege von Auslandskontakten Zentralstellenaufgabe ist. Die Ausschreibung erfolgt – ebenso wie bei den polizeilichen Ausschreibungen nach Artikel 99 Abs. 2 SDÜ – unmittelbar durch den Bedarfsträger ohne zusätzlichen Bearbeitungsschritt im BKA.

Satz 2 stellt klar, dass Artikel 99 Abs. 4 SDÜ Grundlage der Übermittlung an die ausschreibende Stelle ist, bei Übermittlungen des BKA – über das als Zentrale für den nationalen Teil des SIS die Meldungen ausländischer Stellen eingehen – in Verbindung mit § 10 Abs. 2 des Bundeskriminalamtgesetzes (BKAG) i. V. m. § 18 Abs. 2 BVerfSchG.

Die Sätze 3 bis 5 treffen Maßgaben, die – auch verfahrensmäßig – gewährleisten, dass die Ausschreibung nur solange erfolgt, wie die Voraussetzungen dazu vorliegen. Satz 6 sieht die parlamentarische Unterrichtung entsprechend § 8a Abs. 6 vor.

Die Benachrichtigung des Betroffenen ist im Vertragsgesetz zum Schengener Durchführungsübereinkommen geregelt. Mit Artikel 7 wird diese Regelung an die neue Ausschreibungsbefugnis der Nachrichtendienste angepasst (BT-Drs. 16/2921 S. 17).

### **bbb) Übermittlung von Informationen an die Verfassungsschutzbehörden (§ 18 BVerfSchG)**

Die Behörden des Bundes, der bundesunmittelbaren juristischen Personen des öffentlichen Rechts, die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen, unterrichten nach **§ 18 Abs. 1 Satz 1 BVerfSchG** von sich aus das BfV oder die Verfassungsschutzbehörde des Landes über die ihnen bekanntgewordenen Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen im Geltungsbereich dieses Gesetzes erkennen lassen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 BVerfSchG genannten Schutzgüter gerichtet sind. Das Gesetz zur Verbesserung der

Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I 2015 S. 1938) sieht eine Erweiterung von § 18 BVerfSchG mit dem Ziel vor, dass künftig Staatsanwaltschaften, Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz (BPolG) wahrnehmen, ohne Beschränkung auf bestimmte Phänomenbereiche verpflichtet werden sollen, Informationen an das BfV oder an die Verfassungsschutzbehörden der Länder zu übermitteln, sofern tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung für die Aufgabenerfüllung der Verfassungsschutzbehörden erforderlich ist. Bisher bestand eine solche Verpflichtung nach § 18 Abs. 1 BVerfSchG nur bei Spionagetätigkeiten und bei gewaltgeneigten Bestrebungen. Im Übrigen lag die Informationsübermittlung bislang bundesrechtlich im Ermessen der Behörden.

**ccc) Übermittlung von personenbezogenen Daten durch das BfV  
(§ 19 BVerfSchG)**

**a1) Übermittlung an Staatsanwaltschaften, Finanzbehörden, Polizeien, die  
Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen  
(Abs. 1)**

Nach § 19 Abs. 1 Satz 1 BVerfSchG darf das BfV **personenbezogene Daten an inländische Behörden übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der fdGO oder sonst für Zwecke der öffentlichen Sicherheit benötigt.** Die mit dieser Vorschrift dem Bundesamt für Verfassungsschutz eingeräumte Befugnis schließt die Verpflichtung ein, die in der Bestimmung genannten **Tatbestandsvoraussetzungen sorgfältig zu prüfen**, da ohne deren Vorliegen die personenbezogenen Daten nicht weitergegeben werden dürfen. Dementsprechend hat das Bundesamt für Verfassungsschutz festzustellen, ob die Daten an eine inländische Behörde übermittelt und von dieser für die in der Vorschrift genannten Zwecke benötigt werden. Die dem Bundesamt für Verfassungsschutz obliegende Sorgfaltspflicht kann im Einzelfall dazu führen, daß es dem Datenempfänger gegenüber klarzustellen hat, in welcher Funktion er die Informationen erhält und zu welchen Zwecken er sie verwenden darf. Die eigene Verantwortung des Datenempfängers nach § 19 Abs. 1 Satz 2 BVerfSchG bleibt davon unberührt (BVerwG, Beschluss vom 06. März 1995 – 1 B 226/94 –, Buchholz 402.7 BVerfSchG Nr 6, Rn. 4, juris).

Das **Urteil des BVerfG vom 24. April 2013 (1 BvR - 1215/07) zum ATDG** enthält auch allgemeine Begründungsausführungen zu Übermittlungen von Nachrichtendiensten an Polizeien. Danach muss eine Übermittlung von Erkenntnissen, die mit besonderen Mitteln nachrichtendienstlich gewonnen worden sind, für ein operatives Tätigwerden der Polizei, das mit schwerwiegenden Grundrechtseingriffen verbunden ist, grundsätzlich einem herausragenden öffentlichen Interesse dienen. Zwar wird das Übermittlungsermessen nach § 19 Absatz 1 Satz 1 BVerfSchG bereits nach geltendem Recht durch die ausdrückliche Übermittlungsschranke in § 23 Nr. 1 BVerfSchG begrenzt angesichts der dort konkret getroffenen Vorgabe, speziell die Art der Informationserhebung als schutzwürdigkeitsbegründenden Umstand zu berücksichtigen und gegen die mit der Übermittlung verfolgten Allgemeininteressen abzuwägen. Im Anschluss daran sieht Das Gesetz zur Verbesserung der

Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I 2015 S. 1938) eine Neuregelung der Übermittlungsregeln für das BfV an die Polizeien vor. Das BVerfG hatte entschieden, dass Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, angesichts dieser Unterschiede gesteigerten verfassungsrechtlichen Anforderungen unterliegen. **Aus dem Grundrecht auf informationelle Selbstbestimmung folgt insoweit ein informationelles Trennungsprinzip.** Danach dürfen Daten zwischen den Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden. Einschränkungen der Datentrennung sind nur ausnahmsweise zulässig. Soweit sie zur operativen Aufgabenwahrnehmung erfolgen, begründen sie einen besonders schweren Eingriff. Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss deshalb grundsätzlich einem herausragenden öffentlichen Interesse dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt. **Dies muss durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein;** auch die Eingriffsschwellen für die Erlangung der Daten dürfen hierbei nicht unterlaufen werden (BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377, Rn. 123)

#### **b1) Übermittlung an Dienststellen der Stationierungstreitkräfte (Abs. 2)**

Das BfV darf nach § 19 Abs. 2 BVerfSchG personenbezogene Daten an Dienststellen der **Stationierungstreitkräfte** übermitteln, soweit die Bundesrepublik Deutschland dazu im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. 1961 II S. 1183, 1218) verpflichtet ist.

#### **c1) Übermittlung an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen (Abs. 3)**

Das BfV darf nach § 19 Abs. 3 BVerfSchG personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Die Übermittlung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Die Übermittlung ist aktenkundig zu machen. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden, und das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

#### **d1) Übermittlung an andere Stellen, wenn dies zum Schutz der fdGO, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 SÜG erforderlich ist (Abs. 4)**

Personenbezogene Daten dürfen nach § 19 Abs. 4 BVerfSchG an andere Stellen nur übermittelt werden, wenn dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 des Sicherheitsüberprüfungsgesetzes erforderlich ist. Übermittlungen nach Satz 1 bedürfen der vorherigen Zustimmung durch das Bundesministerium des Innern. Das Bundesamt für Verfassungsschutz führt einen Nachweis über den Zweck, die Veranlassung, die Aktenfundstelle und die Empfänger der Übermittlungen nach Satz 1. Die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die Verwendung der Daten zu bitten. Die Übermittlung der personenbezogenen Daten ist dem Betroffenen durch das Bundesamt für Verfassungsschutz mitzuteilen, sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist.

#### **e1) Übermittlung an Dienststellen von denen die Daten erhoben werden (Abs. 5)**

Nach § 19 Abs. 5 BVerfSchG findet § 19 Abs. 4 BVerfSchG keine Anwendung, wenn personenbezogene Daten zum Zweck von Datenerhebungen nach § 8 Absatz 1 Satz 2 an Stellen übermittelt werden, von denen die Daten erhoben werden, oder die daran mitwirken. Hiervon abweichend findet Absatz 4 Satz 5 und 6 in Fällen Anwendung, in denen die Datenerhebung nicht mit den in § 8 Absatz 2 bezeichneten Mitteln erfolgt. Durch die Fassung des bisherigen § 19 Abs. 4 Satz 8 BVerfSchG als neuer Abs. 5, der auf den gesamten Absatz 4 bezogen wird, wird ein redaktionelles Versehen bereinigt. Mit Artikel 1 Nr. 7 des Terrorismusbekämpfungsgesetzes sollte klargestellt werden, dass die einschränken- den Bestimmungen des § 19 Abs. 4 BVerfSchG nicht auf die Fälle der Datenerhebung nach § 8 Abs. 1 Satz 2 BVerfSchG anzuwenden sind. Die ergänzte Regelung bezieht sich dabei auf die insofern zuvor strittigen Bestimmungen des § 19 Abs. 4 BVerfSchG. Diese Teilregelung könnte allerdings Umkehrschlüsse in Bezug auf die übrigen Regelungen des § 19 Abs. 4 BVerfSchG veranlassen. Dies ist ersichtlich nicht gemeint. Beispielsweise ist die Anwendung des Satzes 6 (Hinweis auf Verwendungsbeschränkungen) in Gesprächen, die Vertrauensleute zur Informationsbeschaffung führen, evident sinnwidrig. Die klarstellende Zielrichtung der Änderung wird in einer redaktionell klareren Fassung umgesetzt (BT-Drs. 16/2921 S. 17 ff.).

#### **ddd) Übermittlungsverbote (§ 23 BVerfSchG)**

Die Übermittlung nach den Vorschriften des Dritten Abschnitts des BVerfSchG unterbleibt nach § 23 BVerfSchG, wenn (Nr. 1.) für die übermittelnde Stelle erkennbar ist, daß unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen, (Nr. 2.) überwiegende Sicherheitsinteressen dies erfordern

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

#### **eee) Minderjährigenschutz (§ 24 BVerfSchG)**

(1) Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger dürfen nach den Vorschriften dieses Gesetzes übermittelt werden, solange die Voraussetzungen der Speicherung nach § 11 Abs. 1 Satz 1 erfüllt sind; nach § 11 Abs. 1 Satz 1 darf das BfV unter den Voraussetzungen des § 10 BVerfSchG Daten über Minderjährige vor Vollendung des 14. Lebensjahres in zu ihrer Person geführten Akten nur speichern, verändern und nutzen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass der Minderjährige eine der in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat. (2) Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig, wenn sie zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist.

(2) Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres dürfen nach den Vorschriften dieses Gesetzes nicht an ausländische sowie über- oder zwischenstaatliche Stellen übermittelt werden. (2) Abweichend hiervon dürfen Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger, die das 14. Lebensjahr vollendet haben, übermittelt werden, wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass die Übermittlung zur Abwehr einer erheblichen Gefahr für Leib oder Leben einer Person erforderlich ist oder tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung zur Verfolgung einer der in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftaten erforderlich ist.

#### **fff) Pflichten des Empfängers (§ 25 BVerfSchG)**

(1) Der Empfänger prüft, ob die nach den Vorschriften dieses Gesetzes übermittelten personenbezogenen Daten für die Erfüllung seiner Aufgaben erforderlich sind. (2) Ergibt die Prüfung, daß sie nicht erforderlich sind, hat er die Unterlagen zu vernichten. (3) Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unververtretbarem Aufwand möglich ist; in diesem Fall ist die Verarbeitung der Daten einzuschränken.

#### **ggg) Nachberichtspflicht (§ 26 BVerfSchG)**

Erweisen sich personenbezogene Daten nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig, so sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, es sei denn, daß dies für die Beurteilung eines Sachverhalts ohne Bedeutung ist.

#### **cc) Gemeinsame Dateien**

Die Regelungen über gemeinsame Dateien sind zu unterschiedlichen Zeitpunkten in das Gesetz aufgenommen worden und weisen daher nicht unerhebliche Unterschiede auf.

### aaa) Projektbezogene gemeinsame Dateien (§ 22a BVerfSchG)

Die Vorschrift ist durch das TBG eingefügt worden und schafft eine Rechtsgrundlage dafür, dass das BfV für die Dauer und zur Unterstützung einer **befristeten projektbezogenen Zusammenarbeit mit anderen Sicherheitsbehörden eine gemeinsame Datei (Projektdatei)** einrichten kann. Die anderen Sicherheitsbehörden sind die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden der Länder, der MAD, der BND und das ZKA. Die konkrete Ausgestaltung der Projektdatei hängt davon ab, welche der genannten Sicherheitsbehörden an der jeweiligen projektbezogenen Zusammenarbeit teilnehmen. Dies können, müssen aber nicht alle in Satz 1 genannten Behörden sein. Satz 2 enthält eine detaillierte Regelung des Dateizwecks. Voraussetzung der Errichtung einer gemeinsamen Projektdatei ist, dass sie der Unterstützung einer „projektbezogenen Zusammenarbeit“ zwischen dem BfV und den anderen beteiligten Behörden dient, in deren Rahmen Erkenntnisse im Hinblick auf die abschließend genannten Aufgabenbereiche nach § 3 Abs. 1 Nr. 1 bis 4 BVerfSchG ausgetauscht werden. Die Möglichkeiten zur Errichtung einer Projektdatei werden durch den Projektbezug begrenzt. Eine gemeinsame Projektdatei kommt nur bei einem klar definierten Projektauftrag in Betracht. Projektauftrag, Projektziele sowie die Verfahrensweisen der beteiligten Sicherheitsbehörden müssen zu Beginn des Projekts zwischen den beteiligten Behörden konkret vereinbart werden. Die Zusammenarbeit muss dem Austausch von Erkenntnissen im Hinblick auf die im Einzelnen genannten Bestrebungen und Tätigkeiten nach § 3 Abs. 1 Nr. 1 bis 4 BVerfSchG dienen. Diese müssen durch die Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gekennzeichnet sein. Diese in Anlehnung an § 18 Abs.1 BVerfSchG gewählte Formulierung stellt den inhaltlichen Bezug zum Terrorismus her. Nach Satz 2 sind die beteiligten Behörden beim Austausch und der gemeinsamen Auswertung von Erkenntnissen an ihre jeweiligen Aufgaben und Befugnisse gebunden. Mit dem Begriff der Erkenntnisse sind alle polizeilichen und nachrichtendienstlichen Erkenntnisse, einschließlich sog. Vorfelderkenntnisse gemeint, die im Rahmen geltender Ermittlungsvorschriften zwischen den beteiligten Behörden ausgetauscht werden können. Die in einer Projektdatei gespeicherten personenbezogenen Daten dürfen nur durch die an der Projektarbeit beteiligten Behörden und nur im Rahmen ihrer jeweiligen Befugnisse verwendet werden (Satz 3). Die Daten aus der gemeinsamen Datei dürfen nur verwendet werden, soweit sie im Zusammenhang mit der projektbezogenen Zusammenarbeit für die Erfüllung der jeweiligen Aufgaben der Behörden erforderlich sind. Satz 4 regelt darüber hinaus, dass die für die beteiligten Behörden jeweils geltenden Vorschriften auch für die weitere Verwendung der Daten gelten. Dies gilt insbesondere für Kennzeichnungen nach § 4 Abs.2 Artikel-10-Gesetz, die auch nach einer Übermittlung der Daten aufrechterhalten werden müssen (BT-Drs. 16/2950 S. 23).

**bbb) Errichtung gemeinsamer Dateien mit ausländischen Nachrichtendiensten (§ 22b BVerfSchG)**

Die Regelungen ist eingefügt worden durch das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 26. Juli 2016 (BGBl. I 2016 S. 1818). Das Gesetz enthielt spezielle Rechtsgrundlagen für gemeinsame Dateien von BfV mit wichtigen ausländischen Partnerdiensten, insbesondere der Nachbarstaaten und anderer EU- bzw. NATO-Mitgliedstaaten. Zudem wird bereits national die technische Unterstützung der Informationszusammenführung und -pflege fortentwickelt, indem Projektdateien mit polizeilichen und nachrichtendienstlichen Teilnehmern etwas länger eingerichtet werden können (BT-Drs. 18/8702 S. 12).

Die **transnationale Zusammenarbeit von Nachrichtendiensten** ist insbesondere durch die jihadistischen Anschläge in Europa – am 13. November 2015 in Paris und am 22. März 2016 in Brüssel – angeregt worden und hat zu Gesetzesänderungen in der Bundesrepublik geführt. Diese Gefährdungslage gebietet nach den Ausführungen der Bundesregierung zum Schutz der Menschen vor terroristischen Anschlägen dringend eine verbesserte Zusammenarbeit der Sicherheitsbehörden bei der Zusammenführung und Auswertung von Informationen. Hierzu ist bereits im Vorfeld polizeilicher Maßnahmen eine verbesserte internationale nachrichtendienstliche Zusammenarbeit geboten. In Europa ist dazu die Counter Terrorism Group (CTG) als informeller Zusammenschluss von 30 Nachrichtendiensten eingerichtet. Vertreten sind die Inlandsdienste aller EU-Staaten sowie von Norwegen und der Schweiz. Sie richtet aktuell eine **operative „Plattform“** ein. Verbindungsbeamte der CTG-Dienste arbeiten dort zum vereinfachten und beschleunigten Austausch von Erkenntnissen über den islamistischen Terrorismus zusammen. Technisch unterstützt werden soll die Zusammenarbeit auch durch eine gemeinsame Datei. Eine solche Datei könnte derzeit in Deutschland beim Bundesamt für Verfassungsschutz (BfV) nicht geführt werden, da es bislang rechtlich gehindert ist, ausländischen Nachrichtendiensten einen automatisierten Abruf darauf einzurichten. Das Gesetz soll insoweit die Kooperationsfähigkeit Deutschlands in einem internationalen Analyseverbund zum Schutz der Freiheit und Sicherheit der Menschen verbessern (BT-Drs 18/8702 S. 12).

**§ 22b BVerfSchG schafft eine spezielle Rechtsgrundlage für die Errichtung von gemeinsamen Dateien unter Federführung des BfV mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind.** In vielen Bereichen ist das BfV zur Erfüllung seiner Aufgaben nach § 3 BVerfSchG auf die Kooperation mit ausländischen Nachrichtendiensten angewiesen. Insbesondere mit Partnerdiensten in den Nachbarstaaten und darüber hinaus in der EU und der NATO besteht ein besonderes Zusammenarbeitsbedürfnis und damit auch die Notwendigkeit, relevante Informationen zeitnah zu teilen. Dies gilt gerade auch für den Bereich der Terrorismusbekämpfung. Dementsprechend sieht § 22b Abs. 1 BVerfSchG vor, dass das BfV für die Zusammenarbeit mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind (**ausländische Nachrichtendienste**), zur Erforschung von Bestrebungen oder Tätigkeiten, die sich auf bestimmte Ereignisse oder Personenkreise beziehen, **gemeinsame Dateien einrichten kann**, wenn 1. die Erforschung von erheblichem Sicherheitsinteresse für die Bundesrepublik Deutschland



und den jeweils teilnehmenden Staat ist, 2. in den teilnehmenden Staaten die Einhaltung grundlegender rechtsstaatlicher Prinzipien gewährleistet ist, 3. die Festlegungen und Zusagen nach Absatz 5 Satz 1 verlässlich sind und 4. das BMI zugestimmt hat.

Der Nachrichtendienst eines Staates, der weder unmittelbar an die Bundesrepublik Deutschland angrenzt noch Mitgliedstaat der Europäischen Union oder des Nordatlantikvertrages ist, kann darüber hinaus nur teilnehmen, wenn besondere Sicherheitsinteressen dies erfordern (§ 22b Abs. 2 Satz 1 BVerfSchG).

#### **ccc) Teilnahme an gemeinsamen Dateien mit ausländischen Nachrichtendiensten (§ 22c BVerfSchG)**

**Das BfV darf gem. § 22c Abs. 1 BVerfSchG an gemeinsamen Dateien, die von ausländischen Nachrichtendiensten errichtet sind, teilnehmen.** § 22b Absatz 1 bis 4 und 6 BVerfSchG gilt entsprechend. Dabei gilt § 22b Absatz 1 Nr. 3 BVerfSchG mit der Maßgabe, dass verlässlich zuzusagen ist, dass 1. die vom BfV eingegebenen Daten ohne dessen Zustimmung nicht an Dritte übermittelt werden dürfen und nur zu dem Zweck verwendet werden dürfen, zu dem sie in die Datei eingegeben wurden, und 2. das BfV auf Ersuchen Auskunft über die vorgenommene Verwendung der Daten erhält. § 22c BVerfSchG regelt die Teilnahme des BfV an Dateien ausländischer öffentlicher Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind. Insoweit geht es zwar nicht darum, dass das BfV anderen Stellen zu einer eigenen Datei automatisierten Abruf einräumt, gleichwohl erscheint eine dem § 22b BVerfSchG entsprechende Regelung angemessen, wenn der Inlandsdienst sich im Ausland an gemeinsamer Datenhaltung beteiligt. Die Vorgaben beziehen sich dabei allein auf das BfV und die von ihm eingegebenen Daten. **Ob der federführende ausländische Nachrichtendienst seinerseits eine Dateianordnung erstellt und Festlegungen zwischen den Partnern abspricht, bleibt ihm überlassen.** Für die vom BfV eingegebenen Daten müssen aber die Zusagen entsprechend Abs. 5 Satz 1 Nr. 4 erfolgen (vergleiche § 19 Abs. 3 Satz 4 BVerfSchG) (BT-Drs. 18/8702 S. 15).

#### **dd) Anwendung des Datenschutzgesetzes**

Durch Art. 2 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 20197) sind die §§ 26a und 27 BVerfSchG an die Stelle des alten § 27 BVerfSchG getreten. Dieses Gesetz ist vorbehaltlich des Absatzes 2 am 25. Mai 2018 in Kraft getreten. Gleichzeitig ist das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 7 dieses Gesetzes geändert worden ist, außer Kraft getreten.

#### **§ 26a Unabhängige Datenschutzkontrolle**

(1) Jedermann kann sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der

Verarbeitung seiner personenbezogenen Daten durch das Bundesamt für Verfassungsschutz in seinen Rechten verletzt worden zu sein.

(2) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert beim Bundesamt für Verfassungsschutz die Einhaltung der Vorschriften über den Datenschutz. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) Das Bundesamt für Verfassungsschutz ist verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren. Dies gilt nicht, soweit das Bundesministerium des Innern im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(4) Die Absätze 1 bis 3 gelten ohne Beschränkung auf die Erfüllung der Aufgaben nach § 3. Sie gelten entsprechend für die Verarbeitung personenbezogener Daten durch andere Stellen, wenn diese der Erfüllung der Aufgaben von Verfassungsschutzbehörden nach § 3 dient. § 16 Absatz 1 und 4 des Bundesdatenschutzgesetzes findet keine Anwendung.

#### § 27 Anwendung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 3 durch das Bundesamt für Verfassungsschutz findet das Bundesdatenschutzgesetz wie folgt Anwendung: 1. § 1 Absatz 8, die §§ 4, 16 Absatz 1 und 4 und die §§ 17 bis 21 sowie § 85 finden keine Anwendung, 2. die §§ 46, 51 Absatz 1 bis 4 und die §§ 52 bis 54, 62, 64, 83, 84 sind entsprechend anzuwenden

## Gesetzgebung, Literatur und Rechtsprechung

### 1. Gesetze und Materialien:

Entwurf der Bundesregierung vom 06.04.1989 eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (BT-Drs. 11/4306)

Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 21. Tätigkeitsbericht – (BT-Drs. 16/4950)

Terrorismusbekämpfungsergänzungsgesetz (TBEG) vom 5. Januar 2007 (BGBl. I S. 2)

Entwurf der Bundesregierung vom 06.09.2011 eines Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes (BT-Drs. 17/6925)

Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20.06.2013 – BGBl. I S. 1602

Beschlussempfehlung und Bericht des 2. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes (sog. NSU-Untersuchungsausschuss) v. 22.08.2013 (BT-Drs. 17/14600)

Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus vom 30. April 2013, Hrsg. vom BMI und der Ständigen Konferenz der Innenminister und -senatoren der Länder

Unterrichtung durch das Parlamentarische Kontrollgremium Bericht zu den Maßnahmen nach dem Terrorismusbekämpfungsgesetz für das Jahr 2012 v. 19.12.2013 (BT-Dr. 18/216)

Entwurf der Bundesregierung vom 20.04.2015 eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes (BT-Drs. 18/4654)

### 2. Rechtsprechung

BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377 –  
Gemeinsame Antiterrordatei der Polizeibehörden und Nachrichtendienste in ihrer Grundstruktur verfassungsrechtlich unbedenklich, in ihrer Ausgestaltung jedoch teilweise verfassungswidrig - informationelles Trennungsprinzip verbietet grundsätzlich Datenaustausch zwischen Polizeibehörden und Nachrichtendiensten

BVerfG, Beschluss vom 24. Mai 2005 – 1 BvR 1072/01 –, BVerfGE 113, 63-88, Verletzung von GG Art 5 Abs 1 S 2 durch Aufnahme einer Wochenzeitung in Verfassungsschutzberichte eines Bundeslandes ohne hinreichende Begründung des Verdachts verfassungsfeindlicher Bestrebungen

BVerfG, Urteil vom 14. Januar 1986 – 2 BvE 14/83, 2 BvE 4/84 –, BVerfGE 70, 324-388 –  
Zur Frage, ob die Bewilligung der Haushaltsmittel für vier dem Geheimschutz  
unterliegende Aufgabenbereiche durch die Haushaltsgesetze 1984 und 1985  
verfassungsmäßige Rechte einer Fraktion bzw einzelner Abgeordneter verletzt  
hat

BVerfG, Entscheidung vom 15. Dezember 1970 – 2 BvF 1/69, 2 BvR 629/68, 2 BvR 308/69  
–, BVerfGE 30, 1 – G 10 – Abhör-Urteil

BVerwG, Urteil vom 26. Juni 2013 – 6 C 4/12 – Buchholz 402.7 BVerfSchG Nr 15 =  
NVwZ 2014, 233-235 -, Verfassungsschutzbericht des Bundes; Bürgerbewegung  
pro Köln; Verdachtsfall; Unterlassungsanspruch; Folgenbeseitigungsanspruch;  
tatsächliche Anhaltspunkte

BVerwG, Urteil vom 24. März 2010 – 6 A 2/09 – Buchholz 402.71 BNDG Nr 2 –  
Bundesnachrichtendienst; Auskunftsanspruch; Geheimhaltungsbedürfnis;  
personenbezogene Daten

BVerwG, Beschluss vom 06. März 1995 – 1 B 226/94 –, Buchholz 402.7 BVerfSchG Nr 6,  
Rn. 4, juris - Sorgfaltspflicht bei Weitergabe personenbezogener Daten durch das  
Bundesamt für Verfassungsschutz; Klarstellungspflicht

### **3. Literatur:**

Bock in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BVerfSchG

Graulich, Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-  
Fernmeldeaufklärung und internationale Datenkooperation, in KriPoZ 2017, 43

Gröpl, Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung,  
Berlin 1993

Gusy, Geheimdienstliche Aufklärung und Grundrechtsschutz, Wiesbaden 2011

Gusy, Anmerkung zur Entscheidung des BVerwG vom 26.06.2013 (6 C 4/12; VR 2013,  
432) - Zur Aufnahme einer Vereinigung in den Verfassungsschutzbericht des  
Bundes , in NVwZ 2014, 236-237 Abkürzung Fundstelle

Gusy in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BNDG

Mallmann in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BVerfSchG

Roggan/Bergemann, Die neue Sicherheitsarchitektur der Bundesrepublik Deutschland,  
Anti-Terror-Datei, gemeinsame Projektdaten und TBG, in NJW 2007, 876-881