Bundesrat **Drucksache 31/12**

20.01.12

In - Fz - R

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus

A. Problem und Ziel

Ziel des Gesetzentwurfs ist es, angesichts der Bedrohung durch den gewaltbezogenen Rechtsextremismus den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern.

B. Lösung

Es werden die gesetzlichen Grundlagen für die Errichtung einer gemeinsamen Datei und deren Nutzung durch die Polizeien und Nachrichtendienste geschaffen.

C. Alternativen

Erweiterung der bestehenden Antiterrordatei um den gewaltbezogenen Rechtsextremismus: Eine Erweiterung der Antiterrordatei um den Rechtsextremismus wurde geprüft. Im Gegensatz zum internationalen Terrorismus hat jedoch für den gewaltbezogenen Rechtsextremismus in Deutschland der Bundesnachrichtendienst keinen gesetzlichen Auftrag und soll deshalb keinen Zugriff auf die Datei haben. Weiterhin fordern die Besonderheiten dieses Phänomenbereiches einen von der Antiterrordatei abweichenden Datenkranz und Auswertemöglichkeiten, so dass umfangreiche Anpassungsarbeiten erforderlich wären. Die vorhandene Computerhardware kann nicht für einen weiteren

---

Fristablauf: 02.03.12

Besonders eilbedürftige Vorlage gemäß Artikel 76 Absatz 2 Satz 4 GG.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Personenkreis mit benutzt werden, da sie für den internationalen Terrorismus ausgelegt und vollständig ausgelastet ist.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner

E.2 Erfüllungsaufwand für die Wirtschaft. Davon Bürokratiekosten aus Informationspflichten

Keiner

E.3 Erfüllungsaufwand der Verwaltung

Die Einrichtung einer gemeinsamen standardisierten zentralen Datei führt beim Bundeskriminalamt (BKA) zu einem einmaligen finanziellen Mehraufwand für konzeptionelle und technische Arbeiten in Höhe von rd. 6,2 Mio. Euro. Beim Bundesamt für Verfassungsschutz (BfV) entstehen einmalige Umstellungskosten für die Anpassung der dort eingesetzten Systeme in Höhe von rd. 1 Mio. Euro, bei der Bundespolizei (BPOL) in Höhe von 135 000 Euro und beim Militärischen Abschirmdienst (MAD) in Höhe von 3 000 Euro.

Beim BKA entstehen dauerhaft ein Personalmehrbedarf von 19 Planstellen einschließlich der Personalausgaben in Höhe von rd. 1,1 Mio. Euro sowie laufende Sachkosten von jährlich etwa 0,9 Mio. Euro. Beim BfV entsteht ein personeller Mehrbedarf von einer Planstelle A 9 einschließlich Personalausgaben in Höhe von rd. 45 000 Euro für Administration und Anwenderbetreuung. Bei der Bundespolizei entstehen jährlich laufende Sachkosten von 31 500 Euro.

Der anfallende Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im Einzelplan 06 ausgeglichen werden.

Die Kosten, die bei den Ländern entstehen, werden auf Basis einer Abfrage auf einen einmaligen finanziellen Investitionsaufwand von 2 Mio. Euro sowie auf

laufende Kosten von jährlich etwa 52 500 Euro geschätzt. An personellen Aufwand ist mit 39 Stellen bei den Bundesländern (2 Mio Euro) zu rechnen.

Der Entwurf führt neue Informationspflichten im Sinne des Gesetzes zur Einsetzung eines nationalen Normenkontrollrates (NRK-Gesetz) für die Verwaltung ein. Für die Unternehmen und die Bürgerinnen und Bürger werden keine Informationspflichten eingeführt, vereinfacht oder abgeschafft.

F. Weitere Kosten

Sonstige Kosten für die Wirtschaft, insbesondere die mittelständischen Unternehmen und Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

Bundesrat **Drucksache 31/12**

20.01.12

In - Fz - R

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus

Bundesrepublik Deutschland
Die Bundeskanzlerin

Berlin, den 20. Januar 2012

An den
Präsidenten des Bundesrates
Herrn Ministerpräsidenten
Horst Seehofer

Sehr geehrter Herr Präsident,

hiermit übersende ich gemäß Artikel 76 Absatz 2 Satz 4 des Grundgesetzes den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus

mit Begründung und Vorblatt.

Der Gesetzentwurf ist besonders eilbedürftig, da die Rechtsgrundlage zeitnah benötigt wird, um mit der Datei ein angesichts der aktuellen Lage dringend notwendiges Instrument zur Aufklärung rechtsextremistischer Gewalt zu schaffen.

Fristablauf: 02.03.12
Besonders eilbedürftige Vorlage gemäß Artikel 76 Absatz 2 Satz 4 GG.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage beigefügt.

Mit freundlichen Grüßen

Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G)

§ 1

Datei zur Bekämpfung des gewaltbezogenen Rechtsextremismus

(1) Das Bundeskriminalamt, die in der Rechtsverordnung nach § 58 Absatz 1 des Bundespolizeigesetzes bestimmte Bundespolizeibehörde, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder sowie der Militärische Abschirmdienst führen beim Bundeskriminalamt zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus, insbesondere zur Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund, eine gemeinsame standardisierte zentrale Datei.

(2) Zur Teilnahme an der Datei sind als beteiligte Behörden im Benehmen mit dem Bundesministerium des Innern weitere Polizeivollzugsbehörden berechtigt, soweit

1. diesen Aufgaben zur Bekämpfung des gewaltbezogenen Rechtsextremismus nicht nur im Einzelfall besonders zugewiesen sind,

2. ihr Zugriff auf die Datei für die Wahrnehmung der Aufgaben nach Nummer 1 erforderlich und dies unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Sicherheitsinteressen der beteiligten Behörden angemessen ist.

§ 2

Inhalt der Datei und Speicherungspflicht

Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Absatz 1 in der Datei nach § 1 zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, dass die Daten sich beziehen auf

1. Personen,

   a) bei denen Tatsachen die Annahme rechtfertigen, dass sie einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs mit rechtsextremistischem Hintergrund angehören oder diese unterstützen,

   b) die als Täter oder Teilnehmer einer rechtsextremistischen Gewalttat Beschuldigte oder rechtskräftig Verurteilte sind,

2. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie rechtsextremistische Bestrebungen verfolgen und in Verbindung damit zur Gewalt aufrufen, die Anwendung von rechtsextremistisch begründeter Gewalt als Mittel zur Durchsetzung politischer Belange unterstützen, vorbereiten, oder durch ihre Tätigkeiten vorsätzlich hervorrufen oder bei denen Schusswaffen ohne die erforderlichen waffenrechtlichen Berechtigungen, Kriegswaffen oder Explosivstoffe aufgefunden wurden,

3. Personen, die den Sicherheitsbehörden als Angehörige der rechtsextremistischen Szene bekannt sind, wenn sie mit den in Nummer 1 oder in Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus zu erwarten sind (Kontaktpersonen) oder,

4. a) rechtsextremistische Vereinigungen und Gruppierungen,

   b) Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post,

   bei denen Tatsachen die Annahme rechtfertigen, dass sie im Zusammenhang mit einer Person nach Nummer 1 oder Nummer 2 stehen und durch

sie Hinweise für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus gewonnen werden können,

und die Kenntnis der Daten für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich ist. Satz 1 gilt nur für Daten, die die beteiligten Behörden nach den für sie geltenden Rechtsvorschriften automatisiert verarbeiten dürfen.

§ 3

Zu speichernde Datenarten

(1) In der Datei werden, soweit vorhanden, folgende Datenarten gespeichert:

1. zu Personen

   a) nach § 2 Satz 1 Nummer 1 bis 3 der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Lichtbilder, die Bezeichnung der Fallgruppe nach den vorstehend genannten Kriterien zum Personenkreis und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),

   b) nach § 2 Satz 1 Nummer 1 und 2 sowie zu Kontaktpersonen, bei denen Tatsachen die Annahme rechtfertigen, dass sie von der Planung oder Begehung einer unter § 2 Satz 1 Nummer 1 Buchstabe b genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung rechtsextremistischer Gewalt im Sinne von § 2 Satz 1 Nummer 2 Kenntnis haben, folgende weiteren Datenarten (erweiterte Grunddaten):

      aa) eigene oder von ihnen genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte,

      bb) Adressen für elektronische Post,

      cc) Bankverbindungen,

      dd) Schließfächer,

      ee) auf die Person zugelassene oder von ihr genutzte Fahrzeuge,

      ff) Familienstand,

      gg) besondere Fähigkeiten, die nach den auf bestimmten Tatsachen beruhenden Erkenntnissen der beteiligten Behörden der Vorbereitung und

Durchführung terroristischer Straftaten nach § 129a Absatz 1 und 2 des Strafgesetzbuchs dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,

hh) Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf,

ii) Angaben zu einer gegenwärtigen oder früheren Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Absatz 5 des Sicherheitsüberprüfungsgesetzes oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude,

jj) Angaben zur Gefährlichkeit, insbesondere Waffenbesitz oder zum Gewaltbezug der Person,

kk) Fahrlizenzen und Luftfahrtscheine,

ll) besuchte Orte oder Gebiete, an oder in denen sich die in § 2 Satz 1 Nummer 1 oder 2 genannten Personen treffen,

mm) Kontaktpersonen nach § 2 Satz 1 Nummer 3 zu den jeweiligen Personen nach § 2 Satz 1 Nummer 1 oder 2,

nn) der Tag, an dem das letzte Ereignis eingetreten ist, das die Speicherung der Erkenntnisse begründet,

oo) zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen zu Grunddaten und erweiterten Grunddaten, die bereits in Dateien der beteiligten Behörden gespeichert sind, sofern dies im Einzelfall nach pflichtgemäßem Ermessen geboten und zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus unerlässlich ist,

pp) aktuelle Haftbefehle mit rechtsextremistischem Hintergrund,

qq) besuchte rechtsextremistische Konzerte und sonstige Veranstaltungen,

rr) Angaben über den Besitz oder die Erstellung von rechtsextremistischen Druckerzeugnissen, Handschriften, Abbildungen, Trägermedien wie Bücher und Medienträgern, jeweils in nicht geringer Menge,

ss) Sprachkenntnisse,

tt) aktuelle und frühere Mitgliedschaften sowie Funktionen (Funktionär, Mitglied oder Anhänger) in rechtsextremistischen Vereinen und sonstigen rechtsextremistischen Organisationen,

uu) Zugehörigkeit zu rechtsextremistischen Netzwerken und sonstigen rechtsextremistischen Gruppierungen,

2. Angaben zur Identifizierung der in § 2 Satz 1 Nummer 4 genannten rechtsextremistischen Vereinigungen und Gruppierungen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post, mit Ausnahme weiterer personenbezogener Daten, und
3. zu den jeweiligen Daten nach den Nummern 1 und 2 die Angabe der Behörde, die über die Erkenntnisse verfügt, sowie das zugehörige Aktenzeichen oder sonstige Geschäftszeichen und, soweit vorhanden, die jeweilige Einstufung als Verschlusssache.

(2) Soweit zu speichernde Daten aufgrund einer anderen Rechtsvorschrift zu kennzeichnen sind, ist diese Kennzeichnung bei der Speicherung der Daten in der Datei aufrechtzuerhalten.

§ 4

Beschränkte und verdeckte Speicherung

(1) Soweit besondere Geheimhaltungsinteressen oder besonders schutzwürdige Interessen des Betroffenen dies ausnahmsweise erfordern, darf eine beteiligte Behörde entweder von einer Speicherung der in § 3 Absatz 1 Nummer 1 Buchstabe b genannten erweiterten Grunddaten ganz oder teilweise absehen (beschränkte Speicherung) oder alle jeweiligen Daten zu in § 2 genannten Personen, rechtsextremistischen Vereinigungen und Gruppierungen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post in der Weise eingeben, dass die anderen beteiligten Behörden im Falle einer Abfrage die Speicherung der Daten nicht erkennen und keinen Zugriff auf die gespeicherten Daten erhalten (verdeckte Speicherung). Über beschränkte und verdeckte Speicherungen entscheidet der jeweilige Behördenleiter oder ein von ihm besonders beauftragter Beamter des höheren Dienstes.

(2) Sind Daten, auf die sich eine Abfrage bezieht, verdeckt gespeichert, wird die Behörde, die die Daten eingegeben hat, automatisiert durch Übermittlung aller Abfragedaten über die Abfrage unterrichtet und hat unverzüglich mit der abfragenden Behörde Kontakt aufzunehmen, um zu klären, ob Erkenntnisse nach § 8 übermittelt werden können. Die Behörde, die die Daten eingegeben hat, sieht von einer Kontaktaufnahme nur ab, wenn Geheimhaltungsinteressen auch nach den Umständen des Einzelfalls überwiegen. Die wesentlichen Gründe für die Entscheidung nach Satz 2 sind zu dokumentieren. Die übermittelten Anfragedaten sowie die Dokumentation nach

Satz 3 sind spätestens zu löschen oder zu vernichten, wenn die verdeckt gespeicherten Daten zu löschen sind.

§ 5

Zugriff auf die Daten

(1) Die beteiligten Behörden dürfen die in der Datei nach § 1 gespeicherten Daten im automatisierten Verfahren nutzen, soweit dies zur Erfüllung der jeweiligen Aufgaben zur Aufklärung oder Bekämpfung des gewaltbezogen Rechtsextremismus erforderlich ist. Im Falle eines Treffers erhält die abfragende Behörde Zugriff

1. a) bei einer Abfrage zu Personen auf die zu ihnen gespeicherten Grunddaten

   oder

   b) bei einer Abfrage zu rechtsextremistischen Vereinigungen und Gruppierungen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post nach § 2 Satz 1 Nummer 4 auf die dazu gespeicherten Daten, und
2. auf die Daten nach § 3 Absatz 1 Nummer 3.

Auf die zu Personen gespeicherten erweiterten Grunddaten kann die abfragende Behörde im Falle eines Treffers Zugriff erhalten, wenn die Behörde, die die Daten eingegeben hat, dies im Einzelfall auf Ersuchen gewährt. Die Entscheidung hierüber richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

(2) Die abfragende Behörde darf im Falle eines Treffers unmittelbar auf die erweiterten Grunddaten zugreifen, wenn dies aufgrund bestimmter Tatsachen zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann (Eilfall). Ob ein Eilfall vorliegt, entscheidet der Behördenleiter oder ein von ihm besonders beauftragter Beamter des höheren Dienstes. Die Entscheidung und ihre Gründe sind zu dokumentieren. Der Zugriff ist unter Hinweis auf die Entscheidung nach Satz 3 zu protokollieren. Die Behörde, die die Daten eingegeben hat, muss unverzüglich um nachträgliche Zustimmung ersucht werden. Wird die nachträgliche Zustimmung verweigert, ist die weitere Verwendung dieser Daten unzulässig. Die abfragende Behörde hat die Daten unverzüglich zu löschen oder nach § 12 Absatz 3 zu sperren. Sind die Daten einem Dritten übermittelt worden, ist dieser unverzüglich darauf hinzuweisen, dass die weitere Verwendung der Daten unzulässig ist.

(3) Innerhalb der beteiligten Behörden erhalten ausschließlich hierzu ermächtigte Personen Zugriff auf die Datei.

(4) Bei jeder Abfrage müssen der Zweck und die Dringlichkeit angegeben und dokumentiert werden und erkennbar sein.

§ 6

Weitere Verwendung der Daten

(1) Die abfragende Behörde darf die Daten, auf die sie Zugriff erhalten hat, zur Prüfung, ob der Treffer der gesuchten Person oder der gesuchten Angabe nach § 2 Satz 1 Nummer 4 zuzuordnen ist, für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus und zu den Zwecken nach § 7 nutzen. Eine Nutzung zu einem anderen Zweck als zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus ist nur zulässig, soweit

1. dies zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person erforderlich ist, und
2. die Behörde, die die Daten eingegeben hat, der Verwendung zustimmt.

(2) Im Eilfall darf die abfragende Behörde die Daten, auf die sie nach § 5 Absatz 2 Satz 1 Zugriff erhalten hat, nur nutzen, soweit dies zur Abwehr der gegenwärtigen Gefahr nach § 5 Absatz 2 Satz 1 im Zusammenhang mit der Bekämpfung des gewaltbezogenen Rechtsextremismus unerlässlich ist.

(3) Im Falle einer Verwendung nach Absatz 1 Satz 2 oder Absatz 2 sind die Daten zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten; Gleiches gilt für Kennzeichnungen nach § 3 Absatz 2.

(4) Soweit das Bundeskriminalamt, die Landeskriminalämter oder weitere beteiligte Polizeivollzugsbehörden nach § 1 Absatz 2 auf Ersuchen oder im Auftrag der das strafrechtliche Ermittlungsverfahren führenden Staatsanwaltschaft die Datei nach § 1 nutzen, übermitteln sie dieser die Daten, auf die sie Zugriff erhalten haben, für die Zwecke der Strafverfolgung. Sie darf die Daten für Ersuchen nach Absatz 1 Satz 1 verwenden. § 487 Absatz 3 der Strafprozessordnung gilt entsprechend.

§ 7

Erweiterte Datennutzung

(1) Die beteiligten Behörden dürfen zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten erweitert nutzen, soweit dies im Rahmen eines bestimmten Projekts zur Sammlung und Auswertung von Informationen über konkrete rechtsextremistische Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten, oder zur Verfolgung gewaltbezogener rechtsextremistischer Straftaten im Einzelfall erforderlich ist, um weitere Zusammenhänge aufzuklären. Satz 1 gilt entsprechend für Projekte zur Verhinderung gewaltbezogener rechtsextremistischer Straftaten, soweit Tatsachen die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll. Projekte zur Verfolgung oder Verhinderung von Straftaten nach Satz 1 oder Satz 2 dürfen sich nur auf Straftaten nach §§ 88 bis 89b, 91, 102, 105, 106, 108, 125a bis 129a, 211, 212, 224, 226, 227, 239a, 239b, 306 bis 306c, 308, 310 StGB beziehen.

(2) Eine erweiterte Nutzung ist das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. Hierzu dürfen die beteiligten Behörden Daten auch mittels

a) phonetischer oder unvollständiger Daten,

b) der Suche über eine Mehrzahl von Datenfeldern,

c) der Verknüpfung von Personen, Institutionen, Organisationen, Sachen oder

d) der zeitlichen Eingrenzung der Suchkriterien

aus der Datei abfragen sowie räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darstellen sowie die Suchkriterien gewichten.

(3) Die Zugriffsberechtigung ist im Rahmen der projektbezogenen erweiterten Nutzung auf die Personen zu beschränken, die unmittelbar mit Arbeiten in diesem Anwendungsgebiet betraut sind. Die projektbezogene erweiterte Nutzung der Datei ist auf höchstens zwei Jahre zu befristen. Die Frist kann zweimalig um jeweils bis zu einem Jahr verlängert werden, wenn das Ziel der projektbezogenen erweiterten Nutzung bei Projektende noch nicht erreicht worden ist und diese weiterhin für die Erreichung des Ziels erforderlich ist.

(4) Die projektbezogene erweiterte Nutzung darf nur auf Antrag angeordnet werden. Der Antrag ist durch den Behördenleiter oder seinen Stellvertreter schriftlich zu stellen und zu begründen. Er muss alle für die Anordnung erforderlichen Angaben ent-

halten. Zuständig für die Anordnung ist die die Fachaufsicht über die antragstellende Behörde führende oberste Bundes- oder Landesbehörde. Die Anordnung ergeht schriftlich. In ihr sind der Grund der Anordnung, die für die projektbezogene erweiterte Datennutzung erforderlichen Datenarten nach § 3, der Funktionsumfang und die Dauer der projektbezogenen erweiterten Datennutzung anzugeben. Der Funktionsumfang der projektbezogenen erweiterten Datennutzung ist auf das zur Erreichung des Projektziels erforderliche Maß zu beschränken. Die Anordnung ist zu begründen. Aus der Begründung müssen sich die in den Absätzen 1 bis 3 genannten Voraussetzungen ergeben, insbesondere, dass die projektbezogene erweiterte Nutzung erforderlich ist, um weitere Zusammenhänge aufzuklären. Die anordnende Behörde hält Antrag und Anordnung für datenschutzrechtliche Kontrollzwecke zwei Jahre, mindestens jedoch für die Dauer der projektbezogenen erweiterten Nutzung vor. Für Verlängerungen nach Absatz 3 Satz 3 gelten die Sätze 1 bis 10 entsprechend.

(5) § 6 Absatz 4 Satz 1 gilt für aus einem Projekt nach Absatz 1 gewonnene Erkenntnisse entsprechend.

§ 8

Übermittlung von Erkenntnissen

Die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Absatz 1 Satz 1 oder von erweitert genutzten Daten nach § 7 zwischen den beteiligten Behörden richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

§ 9

Datenschutzrechtliche Verantwortung

(1) Die datenschutzrechtliche Verantwortung für die in der Datei gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten trägt die Behörde, die die Daten eingegeben hat. Die Behörde, die die Daten eingegeben hat, muss erkennbar sein. Die Verantwortung für die Zulässigkeit der Abfrage trägt die abfragende Behörde. Die Verantwortung für die erweiterte Datennutzung nach § 7 trägt die Behörde, die die Daten zu diesen Zwecken verwendet.

(2) Nur die Behörde, die die Daten eingegeben hat, darf diese Daten ändern, berichtigen, sperren oder löschen.

(3) Hat eine Behörde Anhaltspunkte dafür, dass Daten, die eine andere Behörde eingegeben hat, unrichtig sind, teilt sie dies umgehend der Behörde, die die Daten ein-

gegeben hat, mit, die diese Mitteilung unverzüglich prüft und erforderlichenfalls die Daten unverzüglich berichtigt.

§ 10

Protokollierung, technische und organisatorische Maßnahmen

(1) Das Bundeskriminalamt hat bei jedem Zugriff für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Behörde und den Zugriffszweck nach § 5 Absatz 4 oder § 7 zu protokollieren. Die Protokolldaten dürfen nur verwendet werden, soweit ihre Kenntnis für Zwecke der Datenschutzkontrolle, der Datensicherung, zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage oder zum Nachweis der Kenntnisnahme bei Verschlusssachen erforderlich ist. Die ausschließlich für Zwecke nach Satz 1 gespeicherten Protokolldaten sind nach 18 Monaten zu löschen.

(2) Das Bundeskriminalamt hat die nach § 9 des Bundesdatenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen zu treffen.

§ 11

Datenschutzrechtliche Kontrolle, Auskunft an den Betroffenen

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 24 Absatz 1 des Bundesdatenschutzgesetzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die datenschutzrechtliche Kontrolle der Eingabe und der Abfrage von Daten durch eine Landesbehörde richtet sich nach dem Datenschutzgesetz des Landes.

(2) Über die nicht verdeckt gespeicherten Daten erteilt das Bundeskriminalamt die Auskunft nach § 19 des Bundesdatenschutzgesetzes im Einvernehmen mit der Behörde, die die datenschutzrechtliche Verantwortung nach § 9 Absatz 1 Satz 1 trägt und die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Rechtsvorschriften prüft. Die Auskunft zu verdeckt gespeicherten Daten richtet sich nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften.

§ 12

Berichtigung, Löschung und Sperrung von Daten

(1) Unrichtige Daten sind zu berichtigen.

(2) Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus, insbesondere zur Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund, nicht mehr erforderlich ist. Sie sind spätestens zu löschen, wenn die zugehörigen Erkenntnisse nach den für die beteiligten Behörden jeweils geltenden Rechtsvorschriften zu löschen sind.

(3) An die Stelle einer Löschung tritt eine Sperrung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen eines Betroffenen beeinträchtigt würden. Gesperrte Daten dürfen nur für den Zweck abgerufen und genutzt werden, für den die Löschung unterblieben ist; sie dürfen auch abgerufen und genutzt werden, soweit dies zum Schutz besonders hochwertiger Rechtsgüter unerlässlich ist und die Aufklärung des Sachverhalts ansonsten aussichtslos oder wesentlich erschwert wäre oder der Betroffene einwilligt.

(4) Die eingebenden Behörden prüfen nach den Fristen, die für die Erkenntnisdaten gelten, und bei der Einzelfallbearbeitung, ob personenbezogene Daten zu berichtigen oder zu löschen sind.

§ 13

Errichtungsanordnung

Das Bundeskriminalamt hat für die gemeinsame Datei in einer Errichtungsanordnung im Einvernehmen mit den beteiligten Behörden Einzelheiten festzulegen zu:

1. den Bereichen des erfassten gewaltbezogenen Rechtsextremismus,
2. den weiteren beteiligten Polizeivollzugsbehörden nach § 1 Absatz 2,
3. der Art der zu speichernden Daten nach § 3 Absatz 1,
4. der Eingabe der zu speichernden Daten,
5. den zugriffsberechtigten Organisationseinheiten der beteiligten Behörden,
6. den Einteilungen der Zwecke und der Dringlichkeit einer Abfrage
7. Umfang und Verfahren der erweiterten Datennutzung nach § 7 und
8. der Protokollierung.

Die Errichtungsanordnung bedarf der Zustimmung des Bundesministeriums des Innern, des Bundesministeriums der Verteidigung und der für die beteiligten Behörden der Länder zuständigen obersten Landesbehörden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass der Errichtungsanordnung anzuhören.

§ 14

Einschränkung von Grundrechten

Die Grundrechte des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt.

§ 15

Außerkrafttreten

§ 7 tritt am 31. Januar 2016 außer Kraft.

Artikel 2
Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I 2954, 2970), das zuletzt durch Artikel 1 des Gesetzes vom 7. Dezember 2011 (BGBl. I S. 2576) geändert worden ist, wird wie folgt geändert:

§ 6 Satz 8 wird wie folgt geändert:

Nach dem Wort „Macht“ werden ein Komma und die Wörter „von rechtsextremistischen Bestrebungen“ eingefügt.

Artikel 3
Inkrafttreten, Evaluierung

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

(2) Die Anwendung des Artikel 1 ist von der Bundesregierung vor dem 31. Januar 2016 unter Einbeziehung eines oder mehrerer wissenschaftlicher Sachverständiger, die im Einvernehmen mit dem Deutschen Bundestag bestellt werden, zu evaluieren. Bei der Untersuchung sind auch die Häufigkeit und die Auswirkungen der mit den Datenerhebungen, -verarbeitungen und -nutzungen verbundenen Grundrechtseingriffe einzubeziehen und in Beziehung zu setzen zu der anhand von Tatsachen darzustellenden Wirksamkeit zum Zweck der Bekämpfung des gewaltbezogenen Rechtsextremismus. Die Sachverständigenauswahl muss dem Maßstab der Evaluierung gemäß Satz 2 Rechnung tragen.

Begründung

A. Allgemeines

I. Anlass und Zielsetzung des Entwurfs

Die aktuelle Bedrohung durch den Rechtsextremismus erfordert den Einsatz neuer Instrumente zur Gewinnung und zum Austausch von Erkenntnissen der Sicherheitsbehörden von Bund und Ländern. Dazu gehört auch die Nutzung moderner Informationstechnologien, einschließlich gemeinsamer Dateien von Polizeien und Nachrichtendiensten, die sich zur Wahrung der Rechtsstaatlichkeit an den verfassungsrechtlichen, allgemeinen Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit zu orientieren hat.

Die Rechtsgrundlagen für die Tätigkeit der Polizeibehörden (BKAG, BPolG) und der Nachrichtendienste des Bundes (BVerfSchG, MADG, Artikel 10-Gesetz (G 10)) sowie der Länder enthalten eine Vielzahl von Vorschriften, die detailliert die Voraussetzungen regeln, unter denen personenbezogene Daten an andere Behörden übermittelt werden dürfen bzw. müssen. Sie enthalten darüber hinaus Regelungen für die jeweiligen Verbunddateien der Polizeien und Verfassungsschutzbehörden von Bund und Ländern. Demgegenüber fehlen Normen, die gemeinsame Dateien zur Bekämpfung des Rechtsextremismus dauerhaft zulassen, an denen sowohl Polizeibehörden als auch Nachrichtendienste beteiligt sind. Mit dem vorliegenden Gesetzentwurf werden die besonderen Rechtsgrundlagen für den Betrieb einer solchen gemeinsamen Datei geschaffen. Die in dem Entwurf vorgesehene gemeinsame Datei dient dazu, den Informationsaustausch zwischen diesen Behörden zur Bekämpfung des gewaltbezogenen Rechtsextremismus effektiver zu gestalten und bewährte Formen der Zusammenarbeit sinnvoll zu ergänzen. Sie verringert zudem das Risiko von Übermittlungsfehlern und steigert die Qualität der zur Verfügung stehenden Daten.

Die Erfahrungen mit der analog aufgebauten Antiterrordatei (Artikel 1, Gemeinsame-Dateien-Gesetz), die bereits seit 2007 in Wirkbetrieb ist und derzeit evaluiert wird, legen nahe, dass eine gemeinsame elektronische Plattform ein sehr wirkungsvolles Instrument bei der Verbesserung der Zusammenarbeit zwischen den an der Aufklärung extremistischer Bestrebungen und der Bekämpfung politisch motivierter Kriminalität beteiligten Behörden sein kann.

Eine Erweiterung der Antiterrordatei um den Rechtsextremismus wurde geprüft. Im Gegensatz zum internationalen Terrorismus fordern die Besonderheiten dieses Phä-

nomenbereiches jedoch einen von der Antiterrordatei abweichenden Datenkranz und eine erweiterte Möglichkeit zur Datennutzung, so dass umfangreiche Anpassungsarbeiten erforderlich wären. Die vorhandene Computerhardware kann nicht für einen weiteren Personenkreis mit benutzt werden, da sie für den internationalen Terrorismus ausgelegt und vollständig ausgelastet ist. Zudem hat der Bundesnachrichtendienst für den gewaltbezogenen Rechtsextremismus in Deutschland keinen gesetzlichen Auftrag und soll deshalb nicht Teilnehmer an der Datei sein.

Ziel des Gesetzes ist die Verbesserung der Bekämpfung des gewaltbezogenen Rechtsextremismus. Rechtsextremismus ist der Oberbegriff für bestimmte verfassungsfeindliche Bestrebungen, die sich gegen die im Grundgesetz konkretisierte fundamentale Gleichheit der Menschen richten und die universelle Geltung der Menschenrechte ablehnen. Rechtsextremisten sind Feinde des demokratischen Verfassungsstaates, sie haben ein autoritäres Staatsverständnis, das bis hin zur Forderung nach einem nach dem Führerprinzip aufgebauten Staatswesen ausgeprägt sein kann. Das rechtsextremistische Weltbild ist geprägt von einer Überbewertung ethnischer Zugehörigkeit, aus der u.a. Fremdenfeindlichkeit resultiert. Dabei herrscht die Auffassung vor, die Zugehörigkeit zu einer Ethnie, Nation oder „Rasse“ bestimme den Wert eines Menschen. Offener oder immanenter Bestandteil der überwiegenden Mehrzahl aller rechtsextremistischen Bestrebungen ist zudem der Antisemitismus. Individuelle Rechte und gesellschaftliche Interessenvertretungen treten zugunsten kollektivistischer „volksgemeinschaftlicher“ Konstrukte zurück.

II. Wesentliche Schwerpunkte des Entwurfs

Durch den Gesetzentwurf wird zum einen die Rechtsgrundlage für die Errichtung einer gemeinsamen standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus geschaffen.

Mit der gemeinsamen standardisierten zentralen Datei wird der Informationsaustausch zwischen dem Bundeskriminalamt (BKA), den Landeskriminalämtern, den Verfassungsschutzbehörden des Bundes und der Länder und dem Militärischen Abschirmdienst (MAD) im Bereich der Bekämpfung des gewaltbezogenen Rechtsextremismus intensiviert und beschleunigt. Einzelne Erkenntnisse, über die eine Behörde bereits verfügt und die bei einer entsprechenden Verknüpfung mit den Erkenntnissen anderer beteiligter Behörden zur Bekämpfung des gewaltbezogenen Rechtsextremismus beitragen können, werden durch die Datei leichter zugänglich. Zu diesem Zwecke werden die beteiligten Behörden verpflichtet, in der Datei Daten zu den relevanten Personen und Objekten zu speichern. Ein Datenabruf aus der Datei führt

zu einer deutlichen Vereinfachung des Verfahrens und damit zu einer Optimierung des Informationsaustauschs. Gleichzeitig bleiben die jeweiligen allgemeinen Datenübermittlungsvorschriften unangetastet und behalten für den weitergehenden Informationsaustausch ihre unmittelbare Geltung.

Das Gesetz sieht vor, dass neben Grunddaten, die der abfragenden Behörde im Falle eines Treffers grundsätzlich immer angezeigt werden und die in erster Linie die Identifizierung einer bestimmten Person oder eines bestimmten Objekts ermöglichen, auch erweiterte Grunddaten zu den Personen gespeichert werden. Diese erweiterten Grunddaten dienen neben der weitergehenden Identifizierung der Personen auch dem ersten Erkenntnisgewinn. Im Gegensatz zu den Grunddaten sind die erweiterten Grunddaten, die in ihrer Gesamtheit eine Gefährdungseinschätzung zulassen, jedoch bei der ersten Abfrage nicht sichtbar. Sie werden der abfragenden Behörde erst auf Ersuchen bei der speichernden Behörde auf der Grundlage der jeweiligen Datenübermittlungsvorschriften oder im Eilfall sofort angezeigt. Ein Eilfall liegt vor, wenn die Kenntnis der erweiterten Grunddaten zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit, der Freiheit einer Person oder bedeutenden Sachwerten unerlässlich ist und eine vorherige Rückkoppelung mit der eingebenden Behörde, die über die weitergehenden Erkenntnisse verfügt, nicht möglich ist.

Von der Speicherung dieser erweiterten Grunddaten kann abgesehen werden, wenn ihr besondere Geheimhaltungsinteressen entgegenstehen (beschränkte Speicherung). Durch diese Regelung wird sichergestellt, dass einer abfragenden Behörde hochsensible Informationen zu einer Person selbst im Eilfall nicht offen gelegt werden, ohne dass die jeweilige Behörde, die über die Informationen verfügt, die Übermittlung der Daten im Einzelfall prüft. Die grundsätzlich wegen des notwendigen Vertrauensverhältnisses zwischen der Quelle und der Ansprechpartnerin oder dem Ansprechpartner im Nachrichtendienst, der vertrauensvollen Zusammenarbeit mit ausländischen Diensten oder der möglichen Gefährdung der Quelle durch polizeiliche Ermittlungen, zu denen die Polizei mit Blick auf das Legalitätsprinzip verpflichtet wäre, unverzichtbare Geheimhaltung einer Quelle wird allerdings in Bezug auf die erweiterten Grunddaten in aller Regel bereits dadurch gewährleistet, dass diese der abfragenden Behörde nicht angezeigt werden, es sei denn, dass die Behörde, die die Daten eingegeben hat, den Zugriff nach § 5 Absatz 1 Satz 3 im Einzelfall gewährt oder ein Eilfall nach § 5 Absatz 2 vorliegt. Anders verhält es sich mit den Grunddaten, die immer zu speichern und im Trefferfall auch sichtbar sind, sofern die Daten nicht nach § 4 Absatz 1 verdeckt gespeichert sind. Um einen vollständigen Quellenschutz zu erreichen, sieht das Gesetz daher auch die Möglichkeit vor, sämtliche Daten zu einer Person so einzugeben, dass sie im Falle eines Treffers nicht angezeigt

werden und die abfragende Behörde den Trefferfall nicht erkennt (verdeckte Speicherung). In diesem Fall erhält die speichernde Behörde eine Treffermeldung, um sich unverzüglich mit der abfragenden Behörde in Verbindung zu setzen und die notwendige Kommunikation sicherzustellen.

Schließlich soll unter den Voraussetzungen des § 7 der Datenbestand im Rahmen von konkreten Projekten zur Sammlung und Auswertung von Informationen über konkrete rechtsextremistische Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten, oder zur Verfolgung bzw. Verhinderung gewaltbezogener rechtsextremistischer Straftaten auch erweitert genutzt werden können. Eine erweiterte Nutzung ist dabei das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten.

III. Gesetzgebungskompetenz des Bundes

Die Zuständigkeit des Bundes zum Erlass dieser Vorschriften ergibt sich aus Artikel 73 Absatz 1 Nummer 10 des Grundgesetzes (GG), soweit die Bundespolizei betroffen ist, aus Artikel 73 Absatz 1 Nummer 5 GG und, soweit der Militärische Abschirmdienst betroffen ist, aus Artikel 73 Absatz 1 Nummer 1 GG.

IV. Erfüllungsaufwand

Durch den Erfüllungsaufwand gem. § 44 Absatz 4 GGO werden Bund und Länder mit Mehrkosten belastet. Die Einrichtung der Datei führt zu einem einmaligen finanziellen Mehraufwand beim Bund und bei den Ländern sowie zu jährlichen Folgekosten für Betrieb und Nutzung der Datei.
U. a. wegen der zu erzielenden Kostenersparnis und Synergien wird die neue Datei zur Bekämpfung des gewaltbezogenen Extremismus zunächst als technisches Abbild der bereits existierenden Antiterrordatei im Bundeskriminalamt errichtet und betrieben. Durch die Nutzung der bestehenden VS-Rechenzentren für die ATD ist zum aktuellen Zeitpunkt nicht von Baumaßnahmen zum Aufbau der Server- und Speicherstrukturen auszugehen. Die bauliche Infrastruktur wie Klimatisierung kann ebenfalls bestehen bleiben. Für die Errichtung einer zweiten Datei auf den bestehenden Systemen der ATD ist die zugrunde liegende Hardware (Speicher-, Server-, Netzwerkkomponenten) allerdings nicht ausgelegt. Die bestehende Hardware wurde unter Maßgabe der Wirtschaftlichkeit und Sparsamkeit für eine einzelne Datei konzipiert. Darüber hinaus gilt zu berücksichtigen, dass es sich dabei um Komponenten aus dem Beschaffungsjahr 2006 handelt. Eine Weiterverwendung gerade im Hinblick

auf rechenintensive Massenabfragen, wie sie im Zuge von Analysen und Recherchen üblich sind, ist daher ausgeschlossen. Hinzu kommt der quantitative Zuwachs an Daten, da die zu erwartenden Datenbestände in diesem Phänomenbereich weitaus größer sind als im Bereich des internationalen Terrorismus.

Aufwand beim Bundeskriminalamt (BKA) für die Errichtung der zentralen Komponente sowie fachliche Betreuung

Die Gesamtinvestitionskosten beim Bundeskriminalamt belaufen sich schätzungsweise auf ca. 6,2 Mio. Euro, die jährlichen Sachkosten auf etwa 0,9 Mio. Euro.

Diese Kosten schlüsseln sich wie folgt auf:

Hardware und Systemkomponenten	1,1 Mio. €
externe Entwicklungsaufwendungen	1,1 Mio. €
Entwicklung Recherche/Analysetool	2,0 Mio. €
Sicherheits-Komponenten	2,0 Mio. €

Darüber hinaus sind folgende 19 Planstellen/Stellen zusätzlich beim Bundeskriminalamt erforderlich, die weitere Kosten in Höhe von jährlich rd. 1,1 Mio. Euro nach sich ziehen:

Planung, Konzepterstellung:	1 x A12
Produktmanagement und Koordinierungsaufgaben:	1 x A12, 3 x A11
Schnittstellenkonzeption, -anpassung und Überwachung der Quellsysteme:	1 x A13, 2 x A10
Qualitätssicherung Quellsysteme:	1 TB EG 8
Schulung und Betreuung:	1 x A13, 1 x A11, 1 x A9, 1 x TB EG 9
Technische Administration:	3 x A11
Softwareentwicklung und –pflege:	1x A9; 1x A10 und 1x A11)

Aufwand bei den übrigen Bundesbehörden

Auch das Bundesamt für Verfassungsschutz (BfV), die Bundespolizei (BPOL) und der militärische Abschirmdienst (MAD) müssen ihrer Systeme anpassen, um Daten für die Datei anzuliefern bzw. abzufragen.

Beim BfV entstehen einmalige Umstellungskosten für die Anpassung der dort eingesetzten Systeme in Höhe von rd. 1 Mio. €, bei der BPOL in Höhe von 135 000 € und beim MAD in Höhe von 3 000 €.

Beim BfV entsteht ein personeller Mehrbedarf von einer Planstelle A 9 einschließlich Personalausgaben in Höhe von rd. 45 000 € für Administration und Anwenderbetreuung. Bei der Bundespolizei entstehen jährlich laufende Sachkosten von 31 500 €.

Der anfallende Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im Einzelplan 06 ausgeglichen werden

Die Kosten, die bei den Ländern entstehen, werden auf Basis einer Abfrage auf einen einmaligen finanziellen Investitionsaufwand von 2 Mio. € sowie laufenden Kosten von jährlich etwa 52 500 Euro geschätzt. An personellen Aufwand ist mit 39 Stellen bei den Ländern (2 Mio €) zu rechnen.

V. Weitere Kosten

Es entstehen keine Kosten für die Wirtschaft, insbesondere für die mittelständischen Unternehmen. Das Gesetz wird keine Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, haben.

VI. Gleichstellungspolitische Gesetzesfolgenabschätzung

Die gleichstellungspolitischen Auswirkungen wurden gemäß § 2 BGleiG und § 2 GGO anhand der Arbeitshilfe „Gender Mainstreaming bei der Vorbereitung von Rechtsvorschriften“ der Interministeriellen Arbeitsgruppe Gender Mainstreaming geprüft. Die in dem Gesetzentwurf vorgesehene Speicherung von personenbezogenen Daten betrifft Frauen wie Männer unmittelbar. Die Maßnahme hat somit gleichstellungspolitisch weder positive noch negative Auswirkungen. Die Regelungen sind entsprechend § 1 Absatz 2 Satz 1 BGleiG geschlechtergerecht formuliert.

VII. Nachhaltigkeit

Der Gesetzentwurf entspricht der Absicht der Bundesregierung an eine nachhaltige Entwicklung im Sinn der nationalen Nachhaltigkeitsstrategie. Die Managementregeln und Indikatoren der nationalen Nachhaltigkeitsstrategie wurden geprüft.

B. Im Einzelnen

Zu Artikel 1 (Rechtsextremismus-Datei-Gesetz – RED-G)

Zu § 1
Zu Absatz 1
Die Vorschrift schafft die Rechtsgrundlage für die Einrichtung der gemeinsamen standardisierten zentralen Datei zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Datei). Sie legt den Kreis der beteiligten Behörden fest und regelt den Standort der Datei beim BKA. Die Wahl des Standortes beim BKA dient der raschen technischen und organisatorischen Errichtung der Datei. Das BKA verfügt bereits über umfassende Erfahrungen sowie über eine entsprechende technische Plattform, einschließlich der dazu notwendigen Software.

§ 1 regelt darüber hinaus den Dateizweck. Die Datei dient dazu, die beteiligten Behörden bei der Erfüllung der ihnen in den jeweiligen gesetzlichen Vorschriften zugewiesenen Aufgaben im Bereich des gewaltbezogenen Rechtsextremismus zu unterstützen, wobei mit den Begriffen der „Aufklärung“ die nachrichtendienstlichen Aufgaben und mit dem Begriff der „Bekämpfung“ die polizeilichen Aufgaben erfasst werden. Zur Bekämpfung des gewaltbezogenen Rechtsextremismus zählt insbesondere die Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund, weshalb diese Strafverfolgungsaufgaben zur Klarstellung zusätzlich angeführt werden.

Die Datei unterstützt die beteiligten Behörden bei ihrer Aufgabenerfüllung, indem sie den Austausch von Erkenntnissen zu relevanten Sachverhalten erleichtert und damit den Informationsaustausch insgesamt beschleunigt.

Neue Aufgaben werden mit dem Gesetz für die beteiligten Behörden nicht geschaffen. Die Festlegung auf den gewaltbezogenen Rechtsextremismus begrenzt den Umfang der in der Datei zu speichernden Informationen. Ein Gewaltbezug erfordert neben einer subjektiven Komponente auch eine objektive Anknüpfung an gewalttätiges Verhalten und ist damit gegenüber der bloß subjektiven „Gewaltbereitschaft“ enger.

Zu Absatz 2
Nach Absatz 2 sind zur Teilnahme an der Datei unter bestimmten Voraussetzungen weitere Polizeivollzugsbehörden berechtigt. In Betracht kommen insoweit nur Polizeivollzugsbehörden, denen Aufgaben zur Bekämpfung des gewaltbezogenen Rechtsextremismus nicht nur im Einzelfall besonders zugewiesen sind. Mit dieser Regelung soll verhindert werden, dass praktisch jede Polizeivollzugsbehörde, die im Rahmen der Gefahrenabwehr im Einzelfall auch Gefahren des gewaltbezogenen Rechtsextremismus abwehrt, angeschlossen werden kann. Für eine Teilnahme in

Betracht kommen daher in erster Linie die Dienststellen des polizeilichen Staatsschutzes der Länder.

Des Weiteren setzt die Teilnahme weiterer Polizeivollzugsbehörden voraus, dass ihr Zugriff auf die Datei für die Wahrnehmung ihrer Aufgaben zur Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich und die Teilnahme unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Sicherheitsinteressen der beteiligten Behörden angemessen ist. Die Festlegung der weiteren beteiligten Behörden erfolgt in der Errichtungsanordnung, die der Zustimmung des Bundesministeriums des Innern, des Bundesministeriums der Verteidigung und der für die beteiligten Behörden der Länder zuständigen obersten Landesbehörden bedarf (§ 13 Satz 1 Nummer 2).

Zu § 2

Die Vorschrift regelt den Inhalt der Datei.

Zu Satz 1

Satz 1 verpflichtet die beteiligten Behörden sowohl zur Speicherung von Daten zu Personen als auch von Daten zu rechtsextremistischen Vereinigungen und Gruppierungen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post sowie die dazugehörigen Fundstellen in der Datei. Es handelt sich hierbei um bestimmte Personen (Satz 1 Nummer 1 bis 3) und rechtsextremistische Gruppierungen oder Sachen etc. (Satz 1 Nummer 4), zu denen bei den beteiligten Behörden polizeiliche oder nachrichtendienstliche Erkenntnisse vorliegen, deren Kenntnis für die beteiligten Behörden bei der Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich ist.

Die Speicherungspflicht nach Satz 1 entsteht, sobald eine beteiligte Behörde entsprechende Erkenntnisdaten erhoben hat und die übrigen Voraussetzungen zur Speicherung der dazugehörigen Daten in der Datei vorliegen. Durch die unverzügliche Speicherung dieser Daten ist die Aktualität der Datei sicherzustellen.

Das Gesetz schafft keine zusätzliche Rechtsgrundlage für die Datenerhebung durch die beteiligten Behörden. In der Datei dürfen nur bereits erhobene Daten gespeichert werden. Hieraus folgt zugleich, dass in der Datei nur Daten zu Erkenntnissen gespeichert werden, über die die beteiligten Behörden auf der Grundlage der für sie geltenden Rechtsvorschriften bereits verfügen. Dies gilt insbesondere für die Speicherung von Daten zu Kontaktpersonen (Satz 1 Nummer 3). Damit sind die bereichsspezifischen Regelungen zur Erhebung und Speicherung von Daten zu Kon-

taktpersonen in den jeweils für die beteiligten Behörden geltenden speziellen Vorschriften zu beachten.

Voraussetzung für die Speicherung von Daten in der Datei ist, dass die bei den Behörden bekannten Tatsachen die Annahme rechtfertigen, dass sich diese Erkenntnisse auf die nachfolgend beschriebenen Personen oder Gruppierungen oder Sachen etc. (Satz 1 Nummer 4) beziehen.

Zu Nummer 1

Nach Nummer 1 a sind Daten zu Personen zu speichern, bei denen Tatsachen die Annahme rechtfertigen, dass sie einer terroristischen Vereinigung nach § 129a Strafgesetzbuch mit rechtsextremistischem Hintergrund angehören oder diese unterstützen. Nach Nummer 1 b sind Daten zu Personen zu speichern, die als Täter oder Teilnehmer einer rechtsextremistischen Gewalttat Beschuldigte oder rechtskräftig Verurteilte sind. Erfasst werden insbesondere auch gewalttätige und gewaltbezogene Einzeltäter oder Einzeltäterinnen.

Zu Nummer 2

Die Regelung stellt auf Personen ab, bei denen Tatsachen die Annahme rechtfertigen, dass sie rechtsextremistische Bestrebungen verfolgen und aus dieser Motivation rechtswidrig zur Gewalt aufrufen, diese als Mittel zur Durchsetzung von politischen Belangen unterstützen, vorbereiten oder durch ihre Tätigkeit vorsätzlich hervorrufen oder bei denen Schusswaffen ohne die erforderliche waffenrechtliche Berechtigung, Kriegswaffen oder Explosivstoffe aufgefunden wurden. Erfasst werden damit insbesondere jene gewaltbezogenen Rechtsextremisten, die polizeilich bisher weder mit einer konkreten Straftat im Sinne der Nummer 1 Buchstabe a in Erscheinung getreten sind, noch als Beschuldigter oder rechtskräftig Verurteilter zu einer rechtsextremistischen Gewalttat beigetragen haben. Es wird eine positive Haltung des Betroffenen zur Gewaltanwendung vorausgesetzt. Ein bloßes Gutheißen von Gewalt ohne objektivierbaren Beitrag zu einer rechtsextremistischen Gewalttat reicht nicht aus; die Datei ist keine Gesinnungsdatei. Vielmehr setzt das Tatbestandsmerkmal des Unterstützens und vorsätzlichen Hervorrufens die aktive Förderung von Gewaltanwendung voraus. Der Begriff des Unterstützens ist hier als Handlung zu verstehen, die für den Einsatz von Gewalt irgendwie vorteilhaft ist.

Zu speichern sind zudem Personen, die eine entsprechende Gewaltanwendung vorbereiten. Durch das Tatbestandsmerkmal des Vorbereitens werden Personen erfasst, die eine entsprechende künftige Gewaltanwendung planen oder durch ihre Tätigkeit aktiv fördern. Die Einbeziehung des Vorfeldes ist angesichts der zu schützenden hochrangigen Rechtsgüter notwendig, um rechtsextremistische Gefahren umfassend aufzuklären und ihnen möglichst frühzeitig begegnen zu können.

Zu Nummer 3

Nach Nummer 3 sind auch Daten zu Kontaktpersonen von potenziellen rechtsextremistischen Straftätern oder Straftäterinnen und Gewalttätern oder Gewalttäterinnen im Sinne von Nummer 1 und Nummer 2 zu speichern.

Kontaktpersonen sind Personen, die den Sicherheitsbehörden als Angehörige der rechtsextremistischen Szene bekannt sind, bei denen Tatsachen die Annahme rechtfertigen, dass sie mit den in Nummer 1 und Nummer 2 genannten Personen in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus zu erwarten sind. Die konkreten Tatsachen sind hierzu unter Berücksichtigung nachrichtendienstlicher bzw. polizeilicher Erfahrung zu würdigen. Kriterien für eine derartige Verbindung können beispielsweise die nähere persönliche Beziehung, Mitgliedschaft in derselben rechtsextremistischen Gruppierung, die Dauer der Verbindung oder die konspirativen Umstände sein, unter denen die Personen die Verbindung hergestellt haben oder pflegen. Äußerlich flüchtige oder zufällige Alltagskontakte reichen nicht aus.

In der Datei dürfen jedoch nur die Kontaktpersonen erfasst werden, zu denen die beteiligten Behörden bereits nach den für sie geltenden Rechtsvorschriften Erkenntnisse erhoben haben (Satz 1). Soweit für die Erhebung und Speicherung von Daten zu Kontaktpersonen aufgrund spezialgesetzlicher Ausprägungen des Verhältnismäßigkeitsgrundsatzes besondere Anforderungen gelten, sind diese auch im Falle der Speicherung in der Datei zu beachten.

Der unter Nummer 3 erfasste Personenkreis soll auf solche Personen beschränkt werden, die den Verfassungsschutzbehörden als Funktionäre oder Mitglieder rechtsextremistischer Gruppierungen, als einer informellen, nicht vereinsmäßig, sondern nur lose strukturierten Gruppierung wie den „Autonomen Nationalisten“ zugehörig oder sonst als Angehörige der rechtsextremistischen Szene bekannt sind (beispielsweise wegen der häufigen Teilnahme an rechtsextremistischen Konzerten oder sonstiger Veranstaltungen).

Zu Nummer 4

Die Vorschrift regelt die Speicherung von Daten zu rechtsextremistischen Vereinigungen und Gruppierungen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post. Die Aufzählung ist abschließend. Die Regelung betrifft nur rechtsextremistische Gruppierungen, Sachen etc., die mit Personen nach Nummer 1 oder Nummer 2 in Zusammenhang stehen. Eine Verknüpfung zu einer nach Nummer 1 oder 2 gespeicherten Person in der Datei ist nicht vorgesehen. Außerdem müssen die bei den beteiligten Behörden bekannten Tatsachen die Annahme rechtfertigen,

dass gerade durch die Kenntnis der in Nummer 4 aufgezählten rechtsextremistischen Gruppierungen, Sachen etc. Hinweise für die Aufklärung oder die Bekämpfung des gewaltbezogenen Rechtsextremismus gewonnen werden können.
Daten zu Personen und zu Sachen etc. sind getrennt voneinander abzurufen (vgl. § 5 Absatz 1).

Zu Satz 2
Satz 2 enthält eine Einschränkung der in Satz 1 geregelten Speicherungspflicht. In der Datei sind von den beteiligten Behörden nur die Daten zu speichern, die sie automatisiert verarbeiten dürfen. So darf das Bundesamt für Verfassungsschutz beispielsweise Daten von Minderjährigen, die das 16. Lebensjahr noch nicht vollendet haben, grundsätzlich nicht in Dateien speichern (§ 11 Absatz 1 Satz 2 BVerfSchG). Satz 2 stellt sicher, dass derartige Einschränkungen auch für die Speicherung von Daten in der Datei, die nach diesem Gesetz errichtet wird, gelten.

Zu § 3
Zu Absatz 1
Die Vorschrift regelt, welche Datenarten zu den in § 2 genannten Personen und Objekten standardisiert zu speichern sind. Standardisierung der Angaben bedeutet, dass diese, soweit dies nicht aufgrund der zwingenden Individualität der Daten, wie z. B. bei der Bankverbindung, unmöglich ist, nicht freihändig in die Datei eingegeben werden, sondern systemseitig eine bestimmte Auswahl von Angaben angeboten wird, aus denen die eingebende Behörde auswählt. Die Standardisierung dient der Recherchefähigkeit der Datei (und der Vereinheitlichung der Verwaltungspraxis). Da die erweiterten Grunddaten nach § 3 Absatz 1 Nummer 1 Buchstabe b grundsätzlich nicht angezeigt werden, können sie nur dann zur Recherche genutzt werden, wenn mit den gleichen Angaben gesucht wird. Dies ist nur möglich, wenn sich die beteiligten Behörden auf Kataloge verständigen, mit denen die Angaben der erweiterten Grunddaten abgebildet werden. Der einheitliche Sprachgebrauch erleichtert zudem die Kommunikation und den Datenaustausch zwischen den Behörden.

Zu Nummer 1
Nummer 1 bezieht sich auf die zu speichernden Personendaten. Die Aufzählung dieser Datenarten ist abschließend. Zu speichern sind Grunddaten nach Buchstabe a sowie erweiterte Grunddaten nach Buchstabe b. Zu den Grunddaten zählen neben den üblichen Personendaten (vgl. § 5 Absatz 1 Nummer 1 Bundeszentralregistergesetz) andere Namen, Aliaspersonalien und abweichende Namensschreibweisen (vgl. § 3 Nummer 5 Ausländerzentralregistergesetz), die aktuelle und frühere Anschriften,

Angaben zu besonderen körperlichen Merkmalen, Lichtbilder, die Bezeichnung der Fallgruppe nach den in § 2 Nummer 1 bis 4 genannten Kriterien zum Personenkreis.

Angaben zu Identitätspapieren sind nur zu speichern, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen (vgl. § 16 Passgesetz, § 20 Personalausweisgesetz) und dies zur Identifizierung einer Person erforderlich ist.

Die Speicherung dieser Grunddaten ist für einen zielgenauen und schnellen Trefferabgleich, dem zur Vereitelung rechtsextremistischer Taten entscheidende Bedeutung zukommen kann, unverzichtbar (vgl. Erläuterung zu § 6 Absatz 1).

Mit den Fallgruppen sind die jeweiligen Tatbestände des § 2 sowie die dort genannten Tatbestandsalternativen gemeint. Die Angabe der Fallgruppe dient zum einen der Kontrolle der Verwaltung. Zum anderen ermöglicht sie der abfragenden Behörde eine erste Bewertung der Person.

Einer solchen Erstbewertung kommt nicht nur im Eilfall, wenn eine Kontaktaufnahme mit der eingebenden Behörde nicht möglich ist und sofortige Maßnahmen zur Abwehr einer erheblichen Gefahr für hochrangige Rechtsgüter zu treffen sind, erhebliche Bedeutung zu. Sie dient auch stets der Einschätzung, mit welcher Priorität und Dringlichkeit ein Ersuchen zu stellen ist.

Während die Grunddaten nach Buchstabe a zu allen in § 2 genannten Personen gespeichert werden, ist die Speicherung der erweiterten Grunddaten nach Buchstabe b nur hinsichtlich der Personen nach § 2 Satz 1 Nummer 1 und 2 sowie zu Kontaktpersonen, vorgesehen, die von der Planung oder Begehung einer in § 2 Satz 1 Nummer 1 Buchstabe b genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtsextremistischer Gewalt im Sinne von § 2 Satz 1 Nummer 2 Kenntnis haben. Zu anderen Kontaktpersonen werden aus Gründen der Verhältnismäßigkeit keine erweiterten Grunddaten erfasst. Dies können z.B. Kontaktpersonen sein, derer sich Personen nach § 2 Satz 1 Nummer 1 Buchstabe b und Nummer 2 zur Planung oder Begehung einer in § 2 Satz 1 Nummer 1 Buchstabe b genannten Straftat oder zur Ausübung, Unterstützung oder Vorbereitung von rechtsextremistischer Gewalt im Sinne von § 2 Satz 1 Nummer 2 bedienen, die aber selbst hiervon keine Kenntnis haben.

Im Gegensatz zu den Grunddaten, die der abfragenden Behörde im Falle eines Treffers grundsätzlich immer angezeigt werden, sind die erweiterten Grunddaten grundsätzlich im Trefferfall nicht sichtbar. Sie werden der abfragenden Behörde erst auf Nachfrage bei der speichernden Behörde oder im Eilfall angezeigt (§ 5). Die erweiterten Grunddaten ermöglichen eine fachliche Erstbewertung im Sinne einer zuverlässigen Gefährdungseinschätzung. Zu den erweiterten Grunddaten zählen Angaben zu eigenen und genutzten Telekommunikationsanschlüssen und -endgeräten, Adressen

für elektronische Post, Angaben zu Bankverbindungen, Schließfächern, auf die Person zugelassenen sowie sonstigen genutzten Fahrzeugen, zum Familienstand, Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf, zu einer Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Absatz 5 des Sicherheitsüberprüfungsgesetzes (SÜG) oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude, zu besonderen Fähigkeiten, zur Gefährlichkeit der Person, insbesondere zur Bewaffnung und Gewaltbezogenheit, zu Fahr- und Fluglizenzen, zu besuchten Orten oder Gebieten, an oder in denen sich einschlägige Personen treffen, zu Kontaktpersonen zu den Personen nach § 2 Satz 1 Nummer 1 Buchstabe a und b oder Nummer 2, die Bezeichnung der konkreten Vereinigung oder Gruppierung nach § 2 Satz 1 Nummer 4 Buchstabe a und die Angabe des Tages, an dem das letzte Ereignis eingetreten ist, das die Speicherung der Erkenntnisse begründet.

Anders als bei den anderen erweiterten Grunddaten, für die eine Pflicht zur Speicherung besteht, von der nur ausnahmsweise aus Gründen der Geheimhaltung abgesehen werden kann (beschränkte Speicherung nach § 6 Absatz 1), liegt die Speicherung von zusammenfassenden besonderen Bemerkungen, ergänzenden Hinweisen und Bewertungen im pflichtgemäßen Ermessen der speichernden Behörde. Die Speicherung ist nur dann zulässig, wenn und soweit dies zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus unerlässlich ist.

Die Möglichkeit, neben den standardisierten Angaben individuelle Bemerkungen, Hinweise und Bewertungen eingeben zu können, dient dazu, auch rechtsextremismusrelevante Angaben zu erfassen, die sich nicht über einen Katalog standardisiert erfassen lassen. Die grundsätzliche Pflicht zur Standardisierung darf hierdurch jedoch nicht umgangen werden.

Die einzelnen Datenkategorien, die nach § 2 Satz 1 Nummer 4 zum Teil auch isoliert gespeichert werden können, weil häufig noch kein Personenbezug erkennbar ist, orientieren sich an den schon in den bisherigen Dateien der beteiligten Behörden gespeicherten Daten und den spezifischen Bedürfnissen der Bekämpfung und Aufklärung des gewaltbezogenen Rechtsextremismus. Ihnen kommt nach den Erfahrungen der beteiligten Behörden bei der Bekämpfung des Rechtsextremismus ebenso wie den Grunddaten nach Buchstabe a eine herausragende Bedeutung zu.

Bei den Telekommunikationsanschlüssen ist es unverzichtbar, dass nicht nur die eigenen, sondern allgemein die von den betreffenden Personen genutzten erfasst werden. Eine wesentliche polizeiliche und nachrichtendienstliche Erkenntnis ist, dass die Täter in aller Regel nicht ihre eigenen Mobilfunkgeräte nutzen, sondern sich unter Verwendung von Aliaspersonalien bzw. der unerlaubten Nutzung echter Personalien Zugang zu Telekommunikationsendgeräten bzw. -anschlüssen verschaffen. Mobilte-

lefone werden zu Zwecken der Verschleierung bei der Tatvorbereitung oder Tatdurchführung regelmäßig gewechselt oder auch innerhalb einer Tätergruppierung getauscht. Darüber hinaus ist die Feststellung von Anschlussinhabern bei ausländischen Mobiltelefonen, Satellitentelefonen oder auch der Nutzung von Prepaid-Telefonkarten nicht selten schwierig oder unmöglich. Die tatsächlichen Nutzungsverhältnisse sind dagegen häufig bereits durch polizeiliche oder nachrichtendienstliche Maßnahmen festgestellt worden oder Teil des Hinweisaufkommens.

Aus diesem Grunde ist es erforderlich, auch Telekommunikationsanschlüsse von Personen zu speichern, die möglicherweise selbst nicht unter § 2 Absatz 1 Satz 1 Nummer 1 oder 2 fallen und nicht wissen, dass ihr Telefon von entsprechenden Personen genutzt wird.

Die Angabe von Bankverbindungen ist erforderlich, weil der Vorbereitung und Durchführung rechtsextremer Anschläge finanzielle Transaktionen vorausgehen können, zu denen den beteiligten Behörden häufig Hinweise vorliegen. Gelder, die für rechtsextremistische Zwecke benötigt werden, werden überwiegend durch Spenden sowie durch legale oder illegale wirtschaftliche Tätigkeiten beschafft. Hierzu werden neben den inoffiziellen Überweisungssystemen auch die offiziellen Zahlungs- und Geldtransfersysteme der Banken genutzt.

Mit Schließfächern sind Post- und Bankschließfächer sowie Schließfächer gemeint, die auf Bahnhöfen, Flughäfen und anderen öffentlichen Orten gemietet werden können.

Die Speicherung von eigenen und genutzten Fahrzeugen ist, ähnlich wie bei den Telekommunikationsanschlüssen, erforderlich, da die betreffenden Personen bei der Tatvorbereitung, z. B. bei Fahrten zu bestimmten Treffpunkten, in der Regel nicht ihre eigenen Fahrzeuge nutzen.

Als besondere Fähigkeiten, die der Vorbereitung oder Durchführung einer rechtsextremistisch motivierten Gewalttat nach den Erkenntnissen der beteiligten Behörden besonders dienlich sein können, gelten insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen. Diese können sich zum Beispiel aus der Teilnahme an Wehrsport- oder Wehrertüchtigungsaktivitäten, aus der Mitgliedschaft in Schützenvereinen und Reservistenverbänden oder einer aktuellen oder früheren Tätigkeit für Sicherheitsdienstleister ergeben.

Den Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung, zu der insbesondere das Studium und der erlernte Beruf zählen, sowie dem ausgeübten Beruf kommt nach den bisherigen Erfahrungen insbesondere in Bezug auf bestimmte Ausbildungs- und Studiengänge besondere Bedeutung zu (z.B. aktuelle oder ehema-

lige Angehörige von Sicherheitsfirmen und der damit verbundene Erwerb von Kampfsportkenntnissen oder waffenrechtlichen Erlaubnissen/Kenntnissen).

Den Angaben zu einer Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Absatz 5 SÜG oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude kann für die erste Gefährdungseinschätzung im Zusammenhang mit unerlässlichen Sofortmaßnahmen eine entscheidende Bedeutung zukommen.

Die standardisierten Angaben zur Gefährlichkeit der Person beziehen sich insbesondere darauf, ob die betreffende Person Waffen besitzt oder als gewaltbezogen einzustufen ist. Rückschlüsse auf den Gewaltbezug können sich unter anderem aus der Zugehörigkeit zu oder der Rolle innerhalb einer bestimmten gewaltbezogenen Gruppierung oder Vereinigung sowie der Selbstcharakterisierung der Person ergeben. Den Angaben zur Gefährlichkeit einer Person kommt im Eilfall eine besondere Bedeutung zu, da bei Personen, die als gefährlich einzustufen sind, entsprechende Eigensicherungsmaßnahmen getroffen werden müssen.

Die Angabe von Fluglizenzen ist für die Einschätzung, ob von der Person eine gemeine Gefahr für die Allgemeinheit ausgehen kann, notwendig. Eine ähnliche Bedeutung können auch Fahrerlaubnisse, insbesondere für Lastkraftwagen oder Schiffe, erlangen.

Die Angabe von besuchten Orten oder Gebieten, an oder in denen sich die in § 2 Satz 1 Nummer 1 und 2 genannten Personen treffen, oder der Besuch von rechtsextremistisch Konzerten und sonstige Veranstaltungen ist erforderlich, weil gerade die Information, dass eine Person an einschlägigen Orten verkehrt, häufig Bestandteil eines ansonsten bruchstückhaften, aber höchst rechtsextremismusrelevanten, Hinweises ist. Über diese Angaben lassen sich insbesondere Netzwerke abbilden und feststellen, ob zwischen Straftaten und bestimmten Veranstaltungen ein Zusammenhang besteht. Zu diesen Orten zählen im Bereich des gewaltbezogenen Rechtsextremismus unter anderem bekannte Treffpunkte. Dabei gilt auch hier wieder, dass im Hinblick auf die verfassungsrechtlich gewährleistete Versammlungsfreiheit nach Artikel 8 GG und die politische Parteienfreiheit aus Artikel 21 Absatz 1 GG, unter dem Tatbestandsmerkmal „sonstige Veranstaltungen“ nicht die Teilnahme an rechtmäßigen Versammlungen und Kundgebungen oder rechtmäßigen Parteiveranstaltungen erfasst ist.

Als erweitertes Grunddatum zu Personen nach § 2 Satz 1 Nummer 1 und 2 werden auch deren Kontaktpersonen gespeichert. Kontaktpersonen zu Kontaktpersonen werden hingegen nicht gespeichert. (Die Bezeichnung der konkreten Gruppierung oder Vereinigung nach § 2 Satz 1 Nummer 4 Buchstabe a ist nur bei denjenigen Per-

sonen zu speichern, die einer solchen Gruppierung oder Vereinigung mutmaßlich angehören oder diese unterstützen.)

Anhand der Angabe des Tages, an dem das letzte Ereignis eingetreten ist, das die Speicherung der Erkenntnisse begründet, lässt sich feststellen, welche Behörde über die neuesten Erkenntnisse zu einer Person verfügt. Dieser Angabe kommt nicht nur für die Erstbewertung im Eilfall Bedeutung zu. Über diese Angabe kann beim Datenabruf gezielt nach denjenigen Behörden gesucht werden, die über die neuesten Erkenntnisse verfügen.

Angaben zu aktuellen Haftbefehlen mit rechtsextremistischem Hintergrund sollen dazu dienen, Erkenntnisse zu gewaltbezogenen Rechtsextremisten, die sich im Zuge eines Ermittlungsverfahrens den Sicherheitsbehörden entziehen und durch Haftbefehl gesucht werden, schneller im Verbund der Sicherheitsbehörden allen zugänglich zu machen. Dies dient letztlich dazu, das Umfeld dieser Rechtsextremisten aufzuklären und neue Ansatzpunkte für Aufenthaltsermittlungsmaßnahmen zu schaffen.

Die Speicherung von Sprachen, die der Betroffene beherrscht, kann bedeutsam sein für Erkenntnisse über seine Vernetzung mit ausländischen Rechtsextremen.

Angaben über aktuelle und frühere Mitgliedschaften sowie Funktionen (Funktionär, Mitglied oder Anhänger) in rechtsextremistischen Vereinen und sonstigen rechtextremistischen Organisationen dient dem Erkenntnisgewinn über das rechtsextremistische Gefährdungspotential der Person. Zugleich gibt sie Aufschluss über ihren Grad der Vernetzung in der Szene.

Gespeichert werden können auch Angaben über den Besitz oder die Erstellung von Druckerzeugnissen, Handschriften, Trägermedien sowie Abbildungen in jeweils nicht geringer Menge. Damit können ggf. Autoren, Verantwortliche im Sinne des Pressegesetzes, Hersteller, Verbreiter, Verlage oder Institutionen nachgewiesen werden, so dass die Behörden die Verbreitung dieser Gegenstände im Falle ihrer Rechtswidrigkeit ggf. bereits im Vorfeld unterbinden oder relevante Erkenntnisse für Maßnahmen der Strafverfolgungsbehörden gewinnen können.

Zu Nummer 2

Nach Nummer 2 sind die zur Identifizierung der Sachen etc. erforderliche Angaben zu speichern. Zu den Angaben nach § 2 Satz 1 Nummer 4 selbst, also beispielsweise der Nummer eines Telekommunikationsanschlusses, die möglicherweise geeignet ist, einen Bezug zu einer bestimmten natürlichen Person herzustellen und damit gegebenenfalls bereits als personenbezogenes Datum anzusehen wäre, dürfen keine weiteren personenbezogenen Daten zu den Sachen etc. gespeichert werden. Einzelheiten sind in der Errichtungsanordnung festzulegen (vgl. § 13 Satz 1 Nummer 3).

Zu Nummer 3

Zu den Personendaten und den Angaben nach § 2 Satz 1 Nummer 4 sind nach Nummer 3 die jeweiligen Behörden, die über die weitergehenden Erkenntnisse verfügen, sowie die dazugehörigen Aktenzeichen oder sonstigen Geschäftszeichen und, soweit vorhanden, die Einstufung als Verschlusssache zu speichern. Die Einstufung als Verschlusssache richtet sich nach § 4 Absatz 2 SÜG.

Zu Absatz 2

Die Regelung stellt klar, dass Vorschriften, die eine Kennzeichnung von Daten im Falle von Übermittlungen vorschreiben, auch bei einer Speicherung der Daten in der Datei zu beachten sind. Dies gilt insbesondere für Kennzeichnungen nach § 4 Absatz 2 und § 6 Absatz 2 Artikel 10-Gesetz. Die Kennzeichnungen müssen auch nach einer Übermittlung der Daten aufrechterhalten werden (§ 6 Absatz 3 Satz 2).

Zu § 4

Die Vorschrift regelt die Möglichkeiten der beschränkten und verdeckten Speicherung. Die Regelungen stellen sicher, dass im Einzelfall überwiegenden Sicherheitsinteressen Rechnung getragen werden kann.

Zu Absatz 1

Die Vorschrift regelt Begriffe und Voraussetzungen der beschränkten und verdeckten Speicherung. Im Falle einer beschränkten Speicherung kann die jeweilige Behörde ganz oder teilweise von einer Speicherung der in § 3 Nummer 1 Buchstabe b genannten erweiterten Grunddaten absehen. Im Falle einer verdeckten Speicherung kann sie sämtliche Daten zu einer Person oder Sache etc. in der Weise eingeben, dass die anderen Behörden keinen Zugriff auf die gespeicherten Daten erhalten. Diese können dann auch nicht erkennen, dass zu den von ihnen abgerufenen Personen oder Sachen etc. Daten verdeckt gespeichert sind. In diesem Fall erhält die speichernde Behörde eine Treffermeldung, um mit der abfragenden Behörde Kontakt aufzunehmen (Absatz 2).

Eine beschränkte und verdeckte Speicherung ist nur zulässig, wenn sie aufgrund besonderer Geheimhaltungsinteressen erforderlich ist. Die Ausnahmevorschrift ist, vor allem in Bezug auf verdeckte Speicherungen, eng auszulegen. Solche besonderen Geheimhaltungsinteressen sind etwa denkbar bei Informationen, die von ausländischen Partnerdiensten kommen und mit einer Verwendungsbeschränkung versehen sind oder bei Informationen, die polizeiliche oder nachrichtendienstliche Quellen betreffen und aus Gründen des Quellenschutzes nicht oder insgesamt nicht offen gespeichert werden können.

Nach Satz 2 entscheidet über beschränkte und verdeckte Speicherungen der jeweilige Behördenleiter. Der Behördenleiter kann einen Beamten des höheren Dienstes als Vertreter beauftragen. Die Regelung dient dazu, dass beschränkte und verdeckte Speicherungen auf das unbedingt notwendige Maß beschränkt bleiben.

Zu Absatz 2

Absatz 2 regelt das weitere Verfahren im Falle einer Abfrage von verdeckt gespeicherten Daten. Da der Anfragende den Trefferfall nicht erkennen kann, legt Satz 1 fest, dass die Behörde, die die Daten eingegeben hat, automatisiert durch die Übermittlung aller Anfragedaten über die Abfrage unterrichtet wird. Zugleich ist sie verpflichtet, unverzüglich mit der abrufenden Stelle Kontakt aufzunehmen. Durch die Übermittlung aller Anfragedaten wird der Behörde, die die Daten verdeckt gespeichert hat, ermöglicht, den Trefferfall zu verifizieren.

Nur in engen Ausnahmefällen, bei überwiegenden Geheimhaltungsinteressen nach den Umständen des Einzelfalls, darf die Behörde, die die Daten verdeckt gespeichert hat, gemäß Satz 2 von einer Rückmeldung bei der anfragenden Stelle absehen. Sie wird damit verpflichtet, unverzüglich eine Abwägung vorzunehmen, ob mit der anfragenden Stelle Kontakt aufgenommen werden kann, wobei gegebenenfalls die Erkenntnisdaten zu einem späteren Zeitpunkt nach den geltenden Übermittlungsvorschriften übermittelt werden. Ein unverzügliches Handeln ist geboten, da wegen der Unkenntnis der anfragenden Stelle über den Trefferfall die verfolgte Spur zur Abwehr eines terroristischen Anschlags verloren gehen könnte. Zur Vornahme dieser Interessenabwägung und deren Eilbedürftigkeit benötigt die Behörde, die die Daten verdeckt gespeichert hat, Informationen über die Dringlichkeit bzw. Wichtigkeit der Abfrage.

Die Informationen über die Dringlichkeit bzw. Wichtigkeit der Abfrage werden der Behörde, die die Daten verdeckt gespeichert hat, mit der Abfrage automatisiert und für die abfragende Behörde nicht erkennbar übermittelt (vgl. § 6 Absatz 3). Nach Satz 3 sind die wesentlichen Gründe für die nach Satz 2 zu treffende Entscheidung über eine Kontaktaufnahme zu dokumentieren. Die Dokumentationspflicht dient dem Datenschutz und der Kontrolle der Verwaltung. Die übermittelten Anfragedaten sowie die Dokumentation sind nach Satz 4 spätestens mit der Löschung der verdeckt gespeicherten Daten zu löschen oder zu vernichten. Die Löschung der verdeckt gespeicherten Daten richtet sich nach § 12 Absatz 2; sie erfolgt spätestens mit der Löschung der dazugehörigen Erkenntnisdaten.

Zu § 5

Zu Absatz 1

Die Vorschrift regelt, dass die beteiligten Behörden die Datei im automatisierten Verfahren nutzen dürfen, soweit dies zur Erfüllung der jeweiligen Aufgaben zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich ist. Satz 2 legt fest, auf welche der gespeicherten Daten die abfragende Behörde im Trefferfall Zugriff erhält, d. h. welche Daten für die abfragende Behörde sichtbar werden.

Im Falle einer Abfrage von Daten zu Personen sind dies neben der Fundstelle und der etwaigen Einstufung als Verschlusssache (§ 3 Absatz 1 Nummer 3), sofern nicht die Voraussetzungen des Satzes 2 oder Absatzes 2 vorliegen, nur die gespeicherten Grunddaten. Aus der Verbindung des Satzes 2 Nummer 1 Buchstabe a mit Satz 2 Nummer 1 Buchstabe b durch das Wort „oder“ ergibt sich, dass eine kombinierte Abfrage von Daten nach Nummer 1 Buchstaben a und b nicht zulässig ist.

Auf die zu Personen gespeicherten erweiterten Grunddaten erhält die abfragende Behörde demgegenüber im Falle eines Treffers grundsätzlich keinen Zugriff, d. h. sie sind für die abfragende Behörde nicht sichtbar. Die Nichtanzeige der erweiterten Grunddaten, aus denen sich insgesamt eine Erstbewertung der jeweiligen Person ergibt, dient dem Grundrechtsschutz der Betroffenen. Die Behörde, die die Daten eingegeben hat, kann jedoch auf Ersuchen Zugriff auf die erweiterten Grunddaten im automatisierten Verfahren gewähren, wobei sie hierbei die geltenden Übermittlungsvorschriften zu beachten hat (Freischaltung). Eine solche Freischaltung der erweiterten Grunddaten auf Nachfrage sehen Satz 3 und 4 vor. Zur Übermittlung an eine Polizeibehörde bzw. zur entsprechenden Freischaltung sind beispielsweise Nachrichtendienste nach den geltenden Übermittlungsvorschriften verpflichtet, wenn die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist (vgl. § 20 Absatz 1 BVerfSchG, § 11 Absatz 2 MADG) und keine Übermittlungsverbote eingreifen.

Umgekehrt sind Polizeibehörden aufgrund bestehender Übermittlungsvorschriften verpflichtet, die Dienste über sicherheitsgefährdende Tätigkeiten im Bereich des Staatsschutzes zu unterrichten (vgl. § 18 Absatz 1 BVerfSchG). Eine konventionelle Übermittlung von erweiterten Grunddaten aufgrund eines Ersuchens nach § 6 Absatz 1 Satz 1 ist damit nicht ausgeschlossen.

Zu Absatz 2

Die abfragende Behörde kann im Falle eines Treffers auch unmittelbar, d. h. ohne vorherige Entscheidung der speichernden Behörde, auf die erweiterten Grunddaten zugreifen, wenn dies aufgrund bestimmter Tatsachen zur Abwehr einer gegenwärti-

gen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist und keine rechtzeitige Entscheidung nach Absatz 1 Satz 4 eingeholt werden kann (Eilfall). In diesem Falle überwiegt das Interesse an der Gefahrenabwehr gegenüber dem Grundrechtsschutz des Betroffenen. Zur Verfahrenssicherung entscheidet der jeweilige Behördenleiter, ob die Voraussetzungen des Eilfalls vorliegen. Der Behördenleiter kann einen Beamten des höheren Dienstes als Vertreter beauftragen. Die Entscheidung und ihre Gründe sind schlüssig zu dokumentieren. Der Zugriff auf die erweiterten Grunddaten aufgrund eines Eilfalls ist zu protokollieren. Die Behörde, die die Daten eingegeben hat, muss unverzüglich um nachträgliche Zustimmung ersucht werden. Wird die nachträgliche Zustimmung verweigert, ist die weitere Verwendung dieser Daten unzulässig und die Daten sind unverzüglich zu löschen. An die Stelle der Löschung tritt die Sperrung der Daten, soweit die Voraussetzungen nach § 12 Absatz 3 vorliegen. Sind die Daten an einen Dritten übermittelt worden, ist dieser davon zu unterrichten, dass die weitere Verwendung der Daten unzulässig ist.

Zu Absatz 3

Nach Absatz 3 erhalten nur Personen Zugriff auf die Datei, die hierzu ermächtigt sind. Die Ermächtigung nach Absatz 3 ist nicht identisch mit der Ermächtigung zum Verschlusssachenzugang nach dem Sicherheitsüberprüfungsgesetz. Der Zweck der Regelung besteht vielmehr darin, den Nutzerkreis auch innerhalb der Organisationseinheiten, die in den beteiligten Behörden mit den entsprechenden Aufgaben nach § 1 betraut und nach § 13 Satz 1 Nummer 5 in der Errichtungsanordnung festzulegen sind, auf das erforderliche Maß zu beschränken. Hierdurch wird neben Datenschutzinteressen auch insbesondere den Geheimhaltungsinteressen der teilnehmenden Behörden Rechnung getragen. Nur diejenigen Personen, die für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus oder diesen unterstützende Bestrebungen zuständig sind, sollen Zugriff auf die Datei erhalten. Eine sachwidrige Streuung der Zugriffsbefugnis soll verhindert werden. Dies schließt jedoch eine besondere Ermächtigung aller Mitarbeiterinnen und Mitarbeiter einer Organisationseinheit, die für die genannten Bereiche zuständig ist, nicht aus.

Zu Absatz 4

Die Vorschrift verpflichtet die abfragende Stelle, bei jeder Abfrage den Zweck und die Dringlichkeit der Abfrage zu dokumentieren. Mit dieser Angabe soll die Behörde, die die Daten verdeckt gespeichert hat, im Trefferfall nach § 4 Absatz 2 Satz 2 die erforderliche Abwägung vornehmen können. Die Angabe des Zwecks und der Dringlichkeit kann standardisiert erfolgen. Sie wird der Behörde, die die Daten verdeckt ge-

speichert hat, elektronisch durch das System übermittelt und dokumentiert. Die Einteilungen der Zwecke und der Dringlichkeit einer Abfrage sind nach § 13 Satz 1 Nummer 6 in der Errichtungsanordnung festzulegen.

Zu § 6

Zu Absatz 1

Während § 5 die Verwendung der Daten nur im Hinblick auf den Datenzugriff zum Inhalt hat, regelt § 6 die weitere Verwendung der Daten, auf die eine abfragende Behörde zugegriffen hat. Als weitere Verwendung der Daten sind nach Satz 1 zunächst der Trefferabgleich und das Stellen eines Ersuchens zulässig. Diese Verwendungsbeschränkung gilt unbeschadet des Absatzes 4, der unter bestimmten Voraussetzungen die Übermittlung der Trefferdaten nach Absatz 4 an die das strafrechtliche Ermittlungsverfahren führende Staatsanwaltschaft zulässt. Darüber hinaus ist eine Verwendung der Daten zu Zwecken der erweiterten Datennutzung nach § 7 zulässig.

Eine Prüfung, ob ein Treffer der gesuchten Person oder Sache etc. zuzuordnen ist, kann dann erforderlich werden, wenn bei einer Abfrage mehrere Treffer als Ergebnis erzielt werden, aber anhand vorliegender Zusatzerkenntnisse, so genannter weicher Daten, erkennbar wird, dass nicht alle Treffer zu der gesuchten Person oder Sache etc. passen. Anhand der bei der abfragenden Behörde vorhandenen „weichen“ Erkenntnisse ist eine Negativselektion möglich. Beispiel: Die abfragende Behörde weiß, dass es sich bei dem Betreffenden, von dem im Übrigen nur ein viel gebräuchlicher Name bekannt ist, um eine ältere Person handelt. Aus den im Trefferfall angezeigten Daten zu den Personen gleichen Namens kann die abfragende Behörde von vornherein diejenigen aussondern, die jüngere Personen betreffen. Auf diese Weise können überflüssige Ersuchen und die damit verbundenen weiteren Übermittlungen personenbezogener Daten vermieden werden.

Die Ersuchen um Übermittlung müssen der Wahrnehmung der jeweiligen Aufgaben der beteiligten Behörden zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus dienen.

Eine Verwendung der Daten zu anderen Zwecken als nach Satz 1 ist nur zulässig, wenn dies zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist und die Behörde, die die Daten eingegeben hat, der Verwendung zustimmt.

Bei der Erteilung der Zustimmung sind geltende Übermittlungsverbote zu beachten (vgl. § 23 BVerfSchG, § 27 BKAG). Stimmt die Behörde, die die Daten eingestellt

hat, auf die im Eilfall Zugriff genommen wurde, nicht zu (vgl. § 5 Absatz 2), dürfen die Daten für die Gefahrabwehr nicht weiter verwendet werden.

Zu Absatz 2

Liegen die Voraussetzungen eines Eilfalls nach § 5 Absatz 2 Satz 1 vor, so darf die abfragende Behörde die Daten, auf die sie Zugriff erhalten hat, nach Absatz 2 verwenden, soweit dies zur Abwehr der gegenwärtigen Gefahr nach § 5 Absatz 2 Satz 1 im Zusammenhang mit der Bekämpfung des gewaltbezogenen Rechtsextremismus unerlässlich ist. Verweigert die Behörde im Nachhinein ihre Zustimmung nach § 5 Absatz 2 Satz 5, so darf die Maßnahme nicht fortgesetzt werden. Die bis dahin bereits getroffene Maßnahme wird jedoch im Falle einer verweigerten Zustimmung nicht nachträglich rechtswidrig.

Die Begrenzung sowie die weiteren Voraussetzungen der über die Ersuchensstellung hinausgehenden weiteren Verwendung der Daten nach Absatz 1 Satz 2 und Absatz 2 trägt dem besonderen Zweck der Datei sowie dem Umstand Rechnung, dass die beteiligten Behörden im Übrigen teilweise sehr unterschiedliche Aufgaben wahrnehmen.

Zu Absatz 3

Aufgrund der Zweckbindung der nach Absatz 1 Satz 2 oder Absatz 2 weiter verwendeten Daten sind diese zu kennzeichnen und die Kennzeichnungen nach einer Übermittlung durch den Empfänger aufrecht zu erhalten. Die Aufrechterhaltung der Kennzeichnung gilt auch für Daten, die nach § 3 Absatz 2 zu kennzeichnen sind.

Zu Absatz 4

Absatz 4 Satz 1 regelt die Übermittlung der Daten nach § 5 Absatz 1 Satz 2 oder 3 an die das strafrechtliche Ermittlungsverfahren führende Staatsanwaltschaft zu Zwecken der Strafverfolgung.

Die Daten, die das BKA, ein LKA oder weitere beteiligte Polizeibehörden nach § 1 Absatz 2 mittels der Abfrage der Datei erhalten, sollen an die das strafrechtliche Ermittlungsverfahren führende Staatsanwaltschaft übermittelt werden, wenn diese Behörden auf deren Ersuchen oder in deren Auftrag gehandelt haben.

Diese kann die übermittelten Daten für Ersuchen an die zuständigen Behörden und für Zwecke des Strafverfahrens nutzen, was durch den Verweis auf Absatz 1 Satz 1 sichergestellt wird. Der Verweis auf § 487 Absatz 3 StPO betrifft die Verantwortung für die Zulässigkeit der Übermittlung.

Zu § 7

Zu Absatz 1

§ 7 regelt die erweiterte, projektbezogene Nutzung der Datei. Angesichts der Bedrohungen durch den gewaltbezogenen Rechtsextremismus zeigt sich, dass nicht nur die Notwendigkeit besteht, den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern, sondern auch die vorliegenden Daten in systematischer Weise zu nutzen. In der Nachbereitung von Vorfällen (wie z. B. der „Ceska“-Morde bzw. der Morde des „Zwickauer Trios“) zeigt sich regelmäßig nicht ein Defizit an der Informationsbeschaffung, sondern am Informationsfluss und der Informationsbewertung durch die einzelnen Sicherheitsbehörden von Bund und Ländern. Zusätzlich erschweren die nicht einheitlich gestalteten sicherheitsbehördlichen Informationssysteme eine möglichst effiziente Nutzung der vorhandenen Daten. Dadurch wurden beispielsweise im Fall der „Ceska“-Morde umfangreiche und Ressourcen bindende Maßnahmen (z.B. Rechercheanfragen in unterschiedlichen Datenbanken, Mehrfacherfassungen) erforderlich.

Um diesen Defiziten entgegenzutreten und eine effektive, aber rechtsstaatlich ausgestaltete Bekämpfung des gewaltbezogenen Rechtsextremismus sicherzustellen, sollen die in der Datei nach § 1 gespeicherten Daten unter strengen Voraussetzungen für eng umgrenzte Projekte befristet erweitert genutzt werden können. Der Projektcharakter ist dabei wesentliches rechtsstaatliches Element. Durch ihn wird sichergestellt, dass die erweiterte Datennutzung nur aus Anlass konkreter tatsächlicher Erkenntnisse in einem beschränkten zeitlichen und inhaltlichen Rahmen erfolgt. Jedes Projekt nach Absatz 1 ist nur dann zulässig, wenn es im Einzelfall erforderlich ist, um weitere Zusammenhänge zu bestehenden Erkenntnissen aufzuklären.

Projekte in diesem Sinne sind ausschließlich zulässig zur Aufklärung von rechtsextremistischen Bestrebungen, die auf die Anwendung von Gewalt angelegt sind oder Gewalttaten vorbereiten sowie zur Verfolgung oder Verhinderung von gewaltbezogenen rechtsextremistischen Straftaten. Projekte zur Verhinderung von gewaltbezogenen rechtsextremistischen Straftaten sind dabei nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass eine derartige Straftat begangen werden soll (Satz 2). Projekte zu Zwecken der Verfolgung oder Verhütung von gewaltbezogenen rechtsextremistischen Straftaten dürfen sich ausschließlich auf die in Satz 3 abschließend genannten Straftaten beziehen.

Zu Absatz 2

Der Begriff der erweiterten Nutzung wird in Absatz 2 definiert. Satz 1 begrenzt den Zweck der erweiterten Nutzung auf die Herstellung von Zusammenhängen zwischen Personen, Orten und Sachen, die Aggregierung und Verknüpfung der Daten sowie

die statistische Auswertung. Satz 2 beschreibt die technischen Mittel, die hierzu genutzt werden dürfen, insbesondere die erlaubten Suchfunktionen.

Beispiele für eine erweiterte Nutzung sind die kartenmäßige, grafische oder sonstige Darstellung von Tatorten sowie Aufenthaltsorten der Verdächtigen, die Darstellung von Beziehungsgeflechten der Verdächtigen, der räumliche Verteilung sowie von Reiseaktivitäten des rechtsextremistischen Personenpotenzials.

Zu Absatz 3

Zu Satz 1

Durch die Begrenzung des zugriffsberechtigten Personenkreises, der unmittelbar mit Arbeiten in dem Anwendungsgebiet der projektbezogenen Zusammenarbeit betraut ist, soll der besondere Charakter dieser Nutzungsart hervorgehoben werden. Zugleich wird hierdurch die Nutzung auf das für das Projekt Erforderliche beschränkt.

Zu Satz 2

Satz 2 stellt klar, dass die projektbezogene erweiterte Nutzung im Regelfall auf zwei Jahre befristet ist. Lediglich für den Fall, dass das Ziel der projektbezogenen erweiterten Nutzung bei Projektende noch nicht erreicht worden ist und deshalb seine Fortsetzung für die Erreichung des Projektziels erforderlich ist, kann die Frist durch zwei separate Anordnungen um jeweils maximal ein Jahr verlängert werden.

Zu Absatz 4

Absatz 4 enthält verfahrensmäßige Sicherungen, um dem Ausnahmecharakter der Nutzung nach § 7 Absatz 1 Geltung zu verschaffen. So darf ein die erweiterte Nutzung ermöglichendes Projekt nach § 7 Absatz 1 nur auf schriftliche Anordnung der Fachaufsicht führenden obersten Bundes- oder Landesbehörde erfolgen. Die Anordnung muss insbesondere die zu nutzenden Datenarten nach § 3 sowie den für das konkrete Projekt erforderlichen Funktionsumfang im Rahmen von § 7 Absatz 2 beschreiben. Weiter müssen in der Begründung sämtliche Voraussetzungen der projektbezogenen erweiterten Datennutzung dargelegt werden. Satz 7 konkretisiert insoweit das Übermaßverbot im Hinblick auf den angestrebten Funktionsumfang.

Der Anordnung muss ein schriftlicher und begründeter Antrag durch die jeweilige Behördenleitung vorausgehen, der alle für die Anordnung erforderlichen Angaben enthält.

Zu Absatz 5

Absatz 5 regelt die Übermittlung der aus einem Projekt nach Absatz 1 gewonnenen Erkenntnisse an die das strafrechtliche Ermittlungsverfahren führende Staatsanwalt-

schaft zu Zwecken der Strafverfolgung, indem § 6 Absatz 4 Satz 1 für entsprechend anwendbar erklärt wird.

Die Erkenntnisse, die das BKA, ein LKA oder weitere beteiligte Polizeibehörden nach § 1 Absatz 2 aus einer erweiterten Datennutzung nach § 7 Absatz 1 erhalten, sollen an die das strafrechtliche Ermittlungsverfahren führende Staatsanwaltschaft übermittelt werden, wenn diese Behörden auf deren Ersuchen oder in deren Auftrag gehandelt haben. Diese kann die übermittelten Daten für Zwecke des Strafverfahrens nutzen.

Zu § 8

Die Vorschrift regelt, dass die Übermittlung von Erkenntnissen, einschließlich von in der Datei gespeicherten Erkenntnissen, aufgrund eines Ersuchens nach § 6 Absatz 1 Satz 1 oder der projektbezogenen erweiterten Nutzung nach § 7 Absatz 1 nur nach den jeweils geltenden allgemeinen Übermittlungsvorschriften erfolgt, etwa nach § 10 Absatz 1 und 2 BKAG, § 5 Absatz 1 und 3, §§ 18 bis 22 BVerfSchG, § 3 Absatz 3, § 10 Absatz 1, § 11 MADG, § 4 Absatz 4 Nummer 1 und 2, § 7 Absatz 2 und 4 G 10 sowie nach den entsprechenden landesgesetzlichen Regelungen. Eine konventionelle Übermittlung von erweiterten Grunddaten neben den Möglichkeiten eines Zugriffs nach § 5 Absatz 1 Satz 3 oder § 5 Absatz 2 ist damit nicht ausgeschlossen. Hinsichtlich der Erkenntnisdaten wird, im Gegensatz zu den Daten in der Datei, auf die die beteiligten Behörden nach § 5 Absatz 1 Satz 2 oder § 5 Absatz 2 zugreifen, mit dem Gesetz keine neue Übermittlungsbefugnis geschaffen.

Zu § 9

Zu Absatz 1

Die datenschutzrechtliche Verantwortung für die in der Datei gespeicherten Daten liegt nach Satz 1 bei der Behörde, die die Daten eingegeben hat. Diese muss erkennbar sein (Satz 2). Nach Satz 3 liegt die Verantwortung für die Zulässigkeit des Abrufs im automatisierten Verfahren bei der empfangenden Behörde. Nur diese ist in der Lage, die Zulässigkeit des Abrufs zu überprüfen. Die datenschutzrechtliche Verantwortung für die im Rahmen der erweiterten Datennutzung nach § 7 trägt dementsprechend auch die Behörde, die die Daten zu diesem Zweck verwendet.

Zu Absatz 2

Entsprechend der datenschutzrechtlichen Verantwortung der eingebenden Behörde ist nur sie berechtigt, die von ihr eingegebenen Daten zu verändern, zu berichtigen, zu sperren oder zu löschen.

Zu Absatz 3

Die Regelung begründet für den Fall, dass eine Behörde Anhaltspunkte dafür hat, dass Daten, die eine andere Behörde gespeichert hat, unrichtig sind, die Pflicht zur umgehenden Mitteilung an die Behörde, die die Daten eingegeben hat.

Zudem wird die Behörde, die die Daten eingegeben hat, verpflichtet, die Mitteilung unverzüglich zu prüfen und erforderlichenfalls die Daten zu berichtigen (vgl. § 12 Absatz 1).

Zu § 10

Zu Absatz 1

Satz 1 verpflichtet das BKA, den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Dienststelle und den Zugriffszweck (§ 5 Absatz 3) für Zwecke der Datenschutzkontrolle zu protokollieren. Die Regelung umfasst eine systemseitige Vollprotokollierung, d. h. eine automatisierte, beweissichere und lückenlose Protokollierung aller Datenbanktransaktionen auf der Grundlage von Auswerteprogrammen.

Zu den Protokolldaten zählt insbesondere die Angabe der abfragenden Person. Einzelheiten sind nach § 13 Satz 1 Nummer 8 in der Errichtungsanordnung festzulegen. Satz 2 enthält eine Verwendungsbeschränkung der Protokolldaten. Sie dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage und, soweit erforderlich, zum Nachweis der Kenntnisnahme bei Verschlusssachen verwendet werden. In Satz 3 wird die Löschungsfrist für Protokolldaten auf 18 Monate festgelegt, sofern diese ausschließlich für Zwecke der Datenschutzkontrolle nach Satz 1 verwendet werden. Eine längere Aufbewahrung zu Zwecken nach Satz 2, insbesondere zum Nachweis der Kenntnisnahme bei Verschlusssachen, ist damit nicht ausgeschlossen.

Zu Absatz 2

Absatz 2 verpflichtet das BKA, die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen zu treffen.

Zu § 11

Die Vorschrift regelt die datenschutzrechtliche Kontrolle sowie die Rechte der Betroffenen.

Zu Absatz 1

Nach Satz 1 obliegt die Kontrolle der Durchführung des Datenschutzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach § 24 Absatz 1

BDSG. Daneben können die Rechtsaufsichtsbehörden und die Gerichte zur Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften die Protokolldaten nach § 10 Absatz 1 Satz 2 nutzen. Für die Eingabe und die Abfrage durch Landesbehörden richtet sich die datenschutzrechtliche Kontrolle nach den jeweils einschlägigen Datenschutzgesetzen der Länder.

Zu Absatz 2

Satz 1 verweist hinsichtlich des Rechts auf Auskunft über die nicht verdeckt in der Datei gespeicherten Daten auf § 19 BDSG. Gemäß Satz 1 ist das BKA im Außenverhältnis gegenüber den Auskunftssuchenden zentrale Auskunftsstelle für die Datei. Die Auskunft wird im Einvernehmen mit der beteiligten Behörde erteilt, die die datenschutzrechtliche Verantwortung für das betreffende Datum trägt. Die im Innenverhältnis zu beteiligende Behörde prüft das Ersuchen nach den für sie geltenden Bestimmungen. Die Regelung trägt den unterschiedlichen Auskunftsregelungen der an der Datei beteiligten Behörden Rechnung. Das bedeutet, dass die Verweigerungsgründe der spezialgesetzlichen Regelungen (zum Beispiel § 15 Absatz 2 BVerfSchG) Anwendung finden.

Die Auskunft über verdeckt gespeicherte Daten kann nur die beteiligte Behörde, die diese Daten verdeckt gespeichert hat, erteilen. Die Auskunftserteilung richtet sich insoweit nach den für sie geltenden Bestimmungen. Eine Auskunftserteilung nach dem in Satz 1 festgelegten Verfahren ist hier unmöglich, da das BKA die von anderen Behörden verdeckt gespeicherten Daten nicht erkennen kann. Wendet sich der Betroffene mit seinem Auskunftsersuchen zunächst an das BKA, hat es in seiner Auskunftserteilung darauf hinzuweisen, dass sich diese nur auf nicht verdeckt gespeicherte Daten bezieht. Zusätzlich nennt das BKA bei der Auskunftserteilung die an der Datei beteiligten Behörden, die die Betroffenen um Auskunft zu einer etwaigen verdeckten Speicherung ersuchen können. Ferner weist es darauf hin, dass sich die Betroffenen zur Auskunftserteilung im Übrigen auch an den Bundesbeauftragten für Datenschutz und die Informationsfreiheit oder die entsprechenden Landesbehörden wenden können.

Zu § 12

Zu Absatz 1

Die Regelung begründet die Pflicht zur Berichtigung unrichtiger Daten. Die Berichtigung erfolgt nach § 9 Absatz 2 ausschließlich durch die Behörde, die die Daten eingegeben hat.

Zu Absatz 2

Satz 1 regelt die Pflicht zur Löschung personenbezogener Daten in der Datei, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus nicht mehr erforderlich ist. Nach Satz 2 sind die in der Datei gespeicherten Daten spätestens zu löschen, wenn die zugehörigen Erkenntnisdaten nach den für die jeweiligen beteiligten Behörden maßgeblichen Vorschriften zu löschen sind.

Zu Absatz 3

Satz 1 sieht als Ausnahme zur Löschung nach Absatz 2 eine Sperrung der Daten vor, wenn Grund zu der Annahme besteht, dass bei einer Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden. Der Abruf und die Nutzung gesperrter Daten ist nach Satz 2 nur für den Zweck zulässig, für den die Löschung unterblieben ist, oder soweit ihr Abruf und ihre Nutzung zum Schutz besonders hochwertiger Rechtsgüter unerlässlich ist und die Aufklärung des Sachverhalts ansonsten aussichtslos oder wesentlich erschwert wäre oder der Betroffene einwilligt.

Zu Absatz 4

Absatz 4 verpflichtet die Behörde, die die Daten eingegeben hat, bei der Einzelfallbearbeitung und nach den für die zugehörigen Erkenntnisdaten geltenden Fristen zu prüfen, ob personenbezogene Daten zu berichtigen oder zu löschen sind.

Zu § 13

Die Vorschrift enthält Vorgaben für den Inhalt sowie den Erlass der Errichtungsanordnung für die gemeinsame Datei gewaltbezogener Rechtsextremismus.

Mit der nach Nummer 1 vorzunehmenden Festlegung der Einzelheiten zu den Bereichen des erfassten gewaltbezogenen Rechtsextremismus wird der Anwendungsbereich der Datei konkretisiert. Festzulegen sind die weiteren beteiligten Polizeivollzugsbehörden nach § 1 Absatz 2 (Nummer 2), Einzelheiten zu der Art der zu speichernden Daten (Nummer 3), der Eingabe der zu speichernden Daten (Nummer 4) sowie den zugriffsberechtigten Organisationseinheiten der beteiligten Behörden (Nummer 5), den Einteilungen bzw. Kategorien der Zwecke und der Dringlichkeit einer Abfrage nach § 5 Absatz 3 (Nummer 6), Umfang und Verfahren der erweiterten Datennutzung (Nummer 7) und der Protokollierung nach § 9 Absatz 1 (Nummer 8).

Des Weiteren regelt § 13 das Verfahren zum Erlass der Errichtungsanordnung. Hierzu bedarf es zum einen des Einvernehmens der beteiligten Behörden und der zuständigen Ministerien. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass der Errichtungsanordnung anzuhören.

Zu § 14
Durch die Vorschrift wird das Zitiergebot nach Artikel 19 Absatz 1 des Grundgesetzes erfüllt.

Zu § 15
Die Vorschriften zur erweiterten Datennutzung nach § 7 treten mit Ablauf des 31. Januar 2016 außer Kraft.

Zu Artikel 2 (Bundesverfassungsschutzgesetz – BVerfSchG)

Durch Artikel 2 soll die in § 6 Satz 8 BVerfSchG bereits bestehende Möglichkeit zur Führung einer Volldatei im Verfassungsschutzverbund auf den gesamten Bereich rechtsextremistischer Bestrebungen erweitert werden.

Bisher wird das Verbundsystem NADIS in weiten Teilen als reines Aktenhinweissystem geführt. Nur in den in § 6 Satz 8 BVerfSchG genannten Fällen dürfen weitergehende Dateien geführt werden. Dazu zählen bereits jetzt Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten. Hierdurch ist schon nach geltender Rechtslage ein weiter Teil rechtsextremistischer Bestrebungen erfasst. Durch die jetzt beabsichtigte Erweiterung soll der gesamte Bereich rechtsextremistischer Bestrebungen, unabhängig von einem Gewaltelement, erfasst werden.

Beim Informationsaustausch innerhalb des Verfassungsschutzverbundes bei der Bekämpfung des Rechtsextremismus kommt es weniger auf den konkreten Gewaltbezug an, als vielmehr um die Vermittlung eines der Bedrohungsrealität in allen Facetten entsprechenden Abbildes der verfassungsfeindlichen und sicherheitsgefährdenden Bestrebungen. Eine sich in der Realität nicht widerspiegelnde trennscharfe Unterscheidung zwischen gewaltfreien und gewaltbezogenen Bestrebungen steht daher dem effektiven und unverzüglichen Informationsaustausch entgegen. Die zeitnahe Verfügbarkeit von Erkenntnissen dient insoweit der Verbesserung der Zusammenarbeit im Verfassungsschutzverbund.

Die Erforderlichkeit der Erweiterung des Anwendungsbereichs von § 6 Satz 8 BVerfSchG zeigt beispielsweise die im Herbst 2011 bekannt gewordene erhebliche Bedrohung durch den Rechtsextremismus in Deutschland. Hier hat sich ein enges Zusammenwirken zwischen verschiedenen rechtsextremistischen Personenkreisen offenbart. Dazu gehören Rechtsextremisten, die ihre jeweiligen extremistischen Bestrebungen in Personenzusammenschlüssen ohne jeden erkennbaren Gewaltbezug verfolgen. Ohne Gewaltbezug ist bisher jedoch ein Führen von Volldateien zu diesen

Personen nicht möglich. Weil aber ein Wechsel von und zwischen Personen und Personenzusammenschlüssen mit und ohne Gewaltbezug gerade für das rechtsextremistische Spektrum typisch ist, eine trennscharfe Unterscheidung zwischen dem gewaltfreien Rechtsextremismus und dem gewalttätigen bis hin zum terroristischen Rechtsextremismus aufgrund der fließenden Grenze im Bereich des Rechtsextremismus nicht möglich erscheint, sollen nun die gesamten rechtsextremistischen Bestrebungen unter § 6 Satz 8 BVerfSchG fallen und dem Verfassungsschutz ein dem Phänomen angemessenes umfassendes Dateisystem ermöglichen.

Zu Artikel 3 (Inkrafttreten, Evaluierung)

Das Gesetz tritt am Tage nach der Verkündung in Kraft. Absatz 2 sieht die Evaluierung der Vorschriften des Artikel 1 vor. Es besteht die Vorstellung, maximal zwei oder drei Sachverständige zu bestellen. Die Evaluierung hat sich an den Kriterien von Artikel 3 Absatz 2 Satz 2 zu orientieren.

Drucksache 31/12

Anlage

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKR-Gesetz

NKR-Nr. 1971: Gesetz zur Verbesserung der Bekämpfung des Rechtsextremismus

Der Nationale Normenkontrollrat hat den oben genannten Entwurf geprüft.

Mit dem Gesetz sollen die gesetzlichen Grundlagen für die Errichtung einer gemeinsamen Datei von Polizeien und Nachrichtendiensten zur Bekämpfung des gewaltbereiten Rechtsextremismus geschaffen werden.

Für Bürgerinnen und Bürger sowie die Wirtschaft ist mit dem Regelungsentwurf kein Erfüllungsaufwand verbunden. Für die Verwaltung führt die Einrichtung einer gemeinsamen standardisierten zentralen Datei zu zusätzlichem Erfüllungsaufwand. Beim Bund entsteht einmaliger Umstellungsaufwand von ca. 6,3 Mio. Euro sowie jährlicher Sachaufwand von ca. 0,9 Mio. Euro. Hinzu kommen Kosten für befristeten Personalbedarf in den Jahren 2012 - 2014 in Höhe von 2,829 Mio. Euro (0,943 Mio. Euro jährlich). Für die Länder verursacht der Entwurf insgesamt einmalige Kosten von 1,07 Mio. Euro sowie jährliche Kosten in Höhe von 1,7 Mio. Euro. Zudem wird der zusätzliche Personalaufwand bei den Ländern auf 22 Stellen geschätzt.

Das Bundesministerium des Innern hat den bei den Verwaltungen bei Bund und Ländern entstehenden Erfüllungsaufwand nach Abfrage bei den betroffenen Bundesbehörden und Ländern ermittelt. Der ausgewiesene Aufwand scheint plausibel.

Der Nationale Normenkontrollrat hat im Rahmen seines gesetzlichen Prüfauftrages keine Bedenken gegen das Regelungsvorhaben.

Dr. Ludewig
Vorsitzender

Prof. Dr. Kuhlmann
Berichterstatterin