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.