

**Gesetz
zur Errichtung gemeinsamer Dateien
von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder
(Gemeinsame-Dateien-Gesetz)**

Vom 22. Dezember 2006

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

**Gesetz
zur Errichtung
einer standardisierten zentralen
Antiterrordatei von Polizeibehörden und
Nachrichtendiensten von Bund und Ländern
(Antiterrordateigesetz – ATDG)**

§ 1

Antiterrordatei

(1) Das Bundeskriminalamt, die Bundespolizeidirektion, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt (beteiligte Behörden) führen beim Bundeskriminalamt zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland eine gemeinsame standardisierte zentrale Antiterrordatei (Antiterrordatei).

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

1. diesen Aufgaben zur Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland nicht nur im Einzelfall besonders zugewiesen sind,
2. ihr Zugriff auf die Antiterrordatei 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 Antiterrordatei und Speicherungspflicht

Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Abs. 1 in der Antiterrordatei zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die Daten sich beziehen auf

1. Personen, die
 - a) einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, die einen internationalen Be-

zug aufweist, oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Abs. 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland oder

- b) einer Gruppierung, die eine Vereinigung nach Buchstabe a unterstützt, angehören oder diese unterstützen,
2. Personen, die rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen,
3. Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in Nummer 1 Buchstabe a oder in Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind (Kontaktpersonen), oder
4. a) Vereinigungen, Gruppierungen, Stiftungen oder Unternehmen,
b) Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post,
bei denen tatsächliche Anhaltspunkte die Annahme begründen, dass sie im Zusammenhang mit einer Person nach Nummer 1 oder Nummer 2 stehen und durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können,

und die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland 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 Antiterrordatei werden, soweit vorhanden, folgende Datenarten gespeichert:

1. zu Personen
 - a) nach § 2 Satz 1 Nr. 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, Sprachen, Dialekte, Lichtbilder, die Bezeichnung der Fallgruppe nach § 2 und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),
- b) nach § 2 Satz 1 Nr. 1 und 2 sowie zu Kontaktpersonen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie von der Planung oder Begleitung einer in § 2 Satz 1 Nr. 1 Buchstabe a genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne von § 2 Satz 1 Nr. 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) Volkszugehörigkeit,
 - hh) Angaben zur Religionszugehörigkeit, soweit diese im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind,
 - ii) besondere Fähigkeiten, die nach den auf bestimmten Tatsachen beruhenden Erkenntnissen der beteiligten Behörden der Vorbereitung und Durchführung terroristischer Straftaten nach § 129a Abs. 1 und 2 des Strafgesetzbuchs dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,
 - jj) Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf,
 - kk) Angaben zu einer gegenwärtigen oder früheren Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Abs. 5 des Sicherheitsüberprüfungsgesetzes oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude,
 - ll) Angaben zur Gefährlichkeit, insbesondere Waffenbesitz oder zur Gewaltbereitschaft der Person,
 - mm) Fahr- und Flugerlaubnisse,
 - nn) besuchte Orte oder Gebiete, an oder in denen sich in § 2 Satz 1 Nr. 1 und 2 genannte Personen treffen,
 - oo) Kontaktpersonen nach § 2 Satz 1 Nr. 3 zu den jeweiligen Personen nach § 2 Satz 1 Nr. 1 Buchstabe a oder Nr. 2,
 - pp) die Bezeichnung der konkreten Vereinigung oder Gruppierung nach § 2 Satz 1 Nr. 1 Buchstabe a oder b,
 - qq) der Tag, an dem das letzte Ereignis eingetreten ist, das die Speicherung der Erkenntnisse begründet, und
 - rr) auf tatsächlichen Anhaltspunkten beruhende 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 internationalen Terrorismus unerlässlich ist,
2. Angaben zur Identifizierung der in § 2 Satz 1 Nr. 4 genannten Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, 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 Antiterrordatei 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 Abs. 1 Nr. 1 Buchstabe b genannten erweiterten Grunddaten ganz oder teilweise absehen (beschränkte Speicherung) oder alle jeweiligen Daten zu in § 2 genannten Personen, Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräte, 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 Anfragedaten über die Abfrage unterrichtet und hat unverzüglich mit der abfragenden Behörde Kontakt aufzunehmen, um zu klären, ob Erkenntnisse nach § 7 übermittelt werden können. Die Behörde, die die Daten eingegeben hat, sieht von einer Kontaktaufnahme nur ab, wenn Geheimhaltungsinteressen auch nach den Um-

ständen 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 Antiterrordatei gespeicherten Daten im automatisierten Verfahren nutzen, soweit dies zur Erfüllung der jeweiligen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus 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 Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post nach § 2 Satz 1 Nr. 4 auf die dazu gespeicherten Daten, und
2. auf die Daten nach § 3 Abs. 1 Nr. 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 § 11 Abs. 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 Antiterrordatei.

(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, nur zur Prüfung, ob der Treffer der gesuchten Person oder der gesuchten Angabe nach § 2 Satz 1 Nr. 4 zuzuordnen ist, und für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus verwenden. Eine Verwendung zu einem anderen Zweck als zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus 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 Zugriff erhalten hat, nur verwenden, soweit dies zur Abwehr der gegenwärtigen Gefahr nach § 5 Abs. 2 Satz 1 im Zusammenhang mit der Bekämpfung des internationalen Terrorismus 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 Abs. 2.

(4) Soweit das Bundeskriminalamt und die Landeskriminalämter auf Ersuchen oder im Auftrag des Generalbundesanwalts die Antiterrordatei nutzen, übermitteln sie die Daten, auf die sie Zugriff erhalten haben, dem Generalbundesanwalt für die Zwecke der Strafverfolgung. Der Generalbundesanwalt darf die Daten für Ersuchen nach Absatz 1 Satz 1 verwenden. § 487 Abs. 3 der Strafprozessordnung gilt entsprechend.

§ 7

Übermittlung von Erkenntnissen

Die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 zwischen den beteiligten Behörden richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

§ 8

Datenschutzrechtliche Verantwortung

(1) Die datenschutzrechtliche Verantwortung für die in der Antiterrordatei 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.

(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 eingegeben hat, mit, die diese Mitteilung unverzüglich

lich prüft und erforderlichenfalls die Daten unverzüglich berichtigt.

§ 9

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 Abs. 4 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.

§ 10

Datenschutzrechtliche Kontrolle, Auskunft an den Betroffenen

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 24 Abs. 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 § 8 Abs. 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.

§ 11

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 internationalen Terrorismus 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.

§ 12

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 internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland,
2. den weiteren beteiligten Polizeivollzugsbehörden nach § 1 Abs. 2,
3. der Art der zu speichernden Daten nach § 3 Abs. 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 und
7. der Protokollierung.

Die Errichtungsanordnung bedarf der Zustimmung des Bundesministeriums des Innern, des Bundeskanzleramts, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen 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.

§ 13

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.

Artikel 2

Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Juni 2005 (BGBl. I S. 1818), wird wie folgt geändert:

Nach § 22 wird folgender § 22a eingefügt:

„§ 22a

Projektbezogene gemeinsame Dateien

(1) Das Bundesamt für Verfassungsschutz kann für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit den Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, den Polizeibehörden des Bundes und der Länder und dem Zollkriminalamt eine gemeinsame Datei errichten. Die projektbezogene Zusammenarbeit bezweckt nach Maßgabe der Aufgaben

und Befugnisse der in Satz 1 genannten Behörden den Austausch und die gemeinsame Auswertung von Erkenntnissen zu Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungsmaßnahmen gegen die in § 3 Abs. 1 Nr. 1 bis 4 genannten Schutzgüter gerichtet sind. Personenbezogene Daten zu Bestrebungen nach Satz 2 dürfen unter Einsatz der gemeinsamen Datei durch die an der projektbezogenen Zusammenarbeit beteiligten Behörden im Rahmen ihrer Befugnisse verwendet werden, soweit dies in diesem Zusammenhang zur Erfüllung ihrer Aufgaben erforderlich ist. Bei der weiteren Verwendung der personenbezogenen Daten finden für die beteiligten Behörden die jeweils für sie geltenden Vorschriften über die Verwendung von Daten Anwendung.

(2) Für die Eingabe personenbezogener Daten in die gemeinsame Datei gelten die jeweiligen Übermittlungsvorschriften zugunsten der an der Zusammenarbeit beteiligten Behörden entsprechend mit der Maßgabe, dass die Eingabe nur zulässig ist, wenn die Daten allen an der projektbezogenen Zusammenarbeit teilnehmenden Behörden übermittelt werden dürfen. Eine Eingabe ist ferner nur zulässig, wenn die Behörde, die die Daten eingegeben hat, die Daten auch in eigene Dateien speichern darf. Die Behörde, die die Daten eingegeben hat, hat die Daten zu kennzeichnen.

(3) Für die Führung einer projektbezogenen gemeinsamen Datei gelten § 6 Satz 5 bis 7 und § 14 Abs. 2 entsprechend. § 15 ist mit der Maßgabe anzuwenden, dass das Bundesamt für Verfassungsschutz die Auskunft im Einvernehmen mit der Behörde erteilt, die die datenschutzrechtliche Verantwortung nach Satz 1 trägt und die beteiligte Behörde die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Bestimmungen prüft.

(4) Die gemeinsame Datei nach Absatz 1 ist auf höchstens zwei Jahre zu befristen. Die Frist kann zweimalig um jeweils bis zu einem Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.

(5) Für die Berichtigung, Sperrung und Löschung der Daten zu einer Person durch die Behörde, die die Daten eingegeben hat, gelten die jeweiligen, für sie anwendbaren Vorschriften über die Berichtigung, Sperrung und Löschung der Daten entsprechend.

(6) Das Bundesamt für Verfassungsschutz hat für die gemeinsame Datei in einer Dateianordnung die Angaben nach § 14 Abs. 1 Satz 1 Nr. 1 bis 7 sowie weiter festzulegen:

1. die Rechtsgrundlage der Datei,
2. die Art der zu speichernden personenbezogenen Daten,
3. die Arten der personenbezogenen Daten, die der Erschließung der Datei dienen,
4. Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchen Verfahren übermittelt werden,
5. im Einvernehmen mit den an der projektbezogenen Zusammenarbeit teilnehmenden Behörden deren jeweilige Organisationseinheiten, die zur Eingabe und zum Abruf befugt sind,

6. die umgehende Unterrichtung der eingebenden Behörde über Anhaltspunkte für die Unrichtigkeit eingegebener Daten durch die an der gemeinsamen Datei beteiligten Behörden sowie die Prüfung und erforderlichenfalls die unverzügliche Änderung, Berichtigung oder Löschung dieser Daten durch die Behörde, die die Daten eingegeben hat,
7. die Möglichkeit der ergänzenden Eingabe weiterer Daten zu den bereits über eine Person gespeicherten Daten durch die an der gemeinsamen Datei beteiligten Behörden,
8. die Protokollierung des Zeitpunkts, der Angaben zur Feststellung des aufgerufenen Datensatzes sowie der für den Abruf verantwortlichen Behörde bei jedem Abruf aus der gemeinsamen Datei durch das Bundesamt für Verfassungsschutz für Zwecke der Datenschutzkontrolle einschließlich der Zweckbestimmung der Protokolldaten sowie deren Löschrfrist und
9. die Zuständigkeit des Bundesamtes für Verfassungsschutz für Schadensersatzansprüche des Betroffenen nach § 8 des Bundesdatenschutzgesetzes.

Die Dateianordnung bedarf der Zustimmung des Bundesministeriums des Innern sowie der für die Fachaufsicht über die beteiligten Behörden zuständigen obersten Bundes- oder Landesbehörden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass einer Dateianordnung anzuhören. § 14 Abs. 3 Halbsatz 1 gilt entsprechend.“

Artikel 3

Änderung des BND-Gesetzes

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch Artikel 3 des Gesetzes vom 21. Juni 2005 (BGBl. I S. 1818), wird wie folgt geändert:

Nach § 9 wird folgender § 9a eingefügt:

„§ 9a

Projektbezogene gemeinsame Dateien

(1) Der Bundesnachrichtendienst kann für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, den Polizeibehörden des Bundes und der Länder und dem Zollkriminalamt eine gemeinsame Datei errichten. Die projektbezogene Zusammenarbeit bezweckt nach Maßgabe der Aufgaben und Befugnisse der in Satz 1 genannten Behörden den Austausch und die gemeinsame Auswertung von Erkenntnissen im Hinblick auf

1. die in § 5 Abs. 1 Satz 3 Nr. 1 bis 3 des Artikel 10-Gesetzes genannten Gefahrenbereiche oder
2. die in § 5 Abs. 1 Satz 3 Nr. 4 bis 6 des Artikel 10-Gesetzes genannten Gefahrenbereiche, soweit deren Aufklärung Bezüge zum internationalen Terrorismus aufweist.

Personenbezogene Daten zu den Gefahrenbereichen nach Satz 2 dürfen unter Einsatz der gemeinsamen Datei durch die an der projektbezogenen Zusammenarbeit beteiligten Behörden im Rahmen ihrer Befugnisse verwendet werden, soweit dies in diesem Zusammenhang zur Erfüllung ihrer Aufgaben erforderlich ist. Bei der

weiteren Verwendung der personenbezogenen Daten finden für die beteiligten Behörden die jeweils für sie geltenden Vorschriften über die Verwendung von Daten Anwendung.

(2) Für die Eingabe personenbezogener Daten in die gemeinsame Datei gelten die jeweiligen Übermittlungsvorschriften zugunsten der an der Zusammenarbeit beteiligten Behörden entsprechend mit der Maßgabe, dass die Eingabe nur zulässig ist, wenn die Daten allen an der projektbezogenen Zusammenarbeit teilnehmenden Behörden übermittelt werden dürfen. Eine Eingabe ist ferner nur zulässig, wenn die Behörde, die die Daten eingegeben hat, die Daten auch in eigenen Dateien speichern darf. Die Daten sind zu kennzeichnen.

(3) Für die Führung einer projektbezogenen gemeinsamen Datei gelten die §§ 4 und 5 in Verbindung mit § 6 Satz 5 bis 7 und § 14 Abs. 2 des Bundesverfassungsschutzgesetzes entsprechend. § 7 dieses Gesetzes ist mit der Maßgabe anzuwenden, dass der Bundesnachrichtendienst die Auskunft im Einvernehmen mit der Behörde erteilt, die die datenschutzrechtliche Verantwortung nach Satz 1 trägt und die beteiligte Behörde die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Bestimmungen prüft.

(4) Eine gemeinsame Datei nach Absatz 1 ist auf höchstens zwei Jahre zu befristen. Die Frist kann zweimalig um bis zu jeweils einem Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.

(5) Für die Berichtigung, Sperrung und Löschung der Daten zu einer Person durch die Behörde, die die Daten eingegeben hat, gelten die jeweiligen, für die Behörde anwendbaren Vorschriften über die Berichtigung, Sperrung und Löschung von Daten entsprechend.

(6) Der Bundesnachrichtendienst hat für die gemeinsame Datei in einer Dateianordnung die Angaben nach § 6 in Verbindung mit § 14 Abs. 1 Satz 1 Nr. 1 bis 7 des Bundesverfassungsschutzgesetzes sowie weiter festzulegen:

1. die Rechtsgrundlage der Datei,
2. die Art der zu speichernden personenbezogenen Daten,
3. die Arten der personenbezogenen Daten, die der Erschließung der Datei dienen,
4. Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden,
5. im Einvernehmen mit den an der projektbezogenen Zusammenarbeit teilnehmenden Behörden deren jeweilige Organisationseinheiten, die zur Eingabe und zum Abruf befugt sind,
6. die umgehende Unterrichtung der eingebenden Behörde über Anhaltspunkte für die Unrichtigkeit eingegebener Daten durch die an der gemeinsamen Datei beteiligten Behörden sowie die Prüfung und erforderlichenfalls die unverzügliche Änderung, Berichtigung oder Löschung dieser Daten durch die Behörde, die die Daten eingegeben hat,
7. die Möglichkeit der ergänzenden Eingabe weiterer Daten zu den bereits über eine Person gespeicher-

ten Daten durch die an der gemeinsamen Datei beteiligten Behörden,

8. die Protokollierung des Zeitpunktes, der Angaben zur Feststellung des aufgerufenen Datensatzes sowie der für den Abruf verantwortlichen Behörde bei jedem Abruf aus der gemeinsamen Datei durch den Bundesnachrichtendienst für Zwecke der Datenschutzkontrolle einschließlich der Zweckbestimmung der Protokolldaten sowie deren Löschfrist und
9. die Zuständigkeit des Bundesnachrichtendienstes für Schadensersatzansprüche des Betroffenen nach § 8 des Bundesdatenschutzgesetzes.

Die Dateianordnung bedarf der Zustimmung des Bundeskanzleramtes sowie der für die Fachaufsicht der zusammenarbeitenden Behörden zuständigen obersten Bundes- oder Landesbehörden. Der Bundesbeauftragte für Datenschutz und die Informationsfreiheit ist vor Erlass einer Dateianordnung anzuhören. § 14 Abs. 3 erster Halbsatz des Bundesverfassungsschutzgesetzes gilt entsprechend.“

Artikel 4

Änderung

des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Artikel 22 des Gesetzes vom 21. Juni 2005 (BGBl. I S. 1818), wird wie folgt geändert:

Nach § 9 wird folgender § 9a eingefügt:

„§ 9a

Projektbezogene gemeinsame Dateien

(1) Das Bundeskriminalamt kann für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, Polizeibehörden des Bundes und der Länder und dem Zollkriminalamt eine gemeinsame Datei errichten. Die projektbezogene Zusammenarbeit bezweckt nach Maßgabe der Aufgaben und Befugnisse der in Satz 1 genannten Behörden den Austausch und die gemeinsame Auswertung von polizeilichen oder nachrichtendienstlichen Erkenntnissen zu

1. Straftaten nach § 99 des Strafgesetzbuchs,
2. Straftaten nach § 129a, auch in Verbindung mit § 129b Abs. 1, des Strafgesetzbuchs,
3. Straftaten nach § 34 Abs. 1 bis 6 des Außenwirtschaftsgesetzes, soweit es sich um einen Fall von besonderer Bedeutung handelt, oder
4. Straftaten, die mit Straftaten nach den Nummern 1 bis 3 in einem unmittelbaren Zusammenhang stehen.

Personenbezogene Daten zu Straftaten nach Satz 2 dürfen unter Einsatz der gemeinsamen Datei durch die an der projektbezogenen Zusammenarbeit beteiligten Behörden im Rahmen ihrer Befugnisse verwendet werden, soweit dies in diesem Zusammenhang zur Erfüllung ihrer Aufgaben erforderlich ist. Bei der weiteren Verwendung der personenbezogenen Daten finden für die beteiligten Behörden die jeweils für sie geltenden Vorschriften über die Verwendung von Daten Anwendung.

(2) Für die Eingabe personenbezogener Daten in die gemeinsame Datei gelten die jeweiligen Übermittlungsvorschriften zugunsten der an der Zusammenarbeit beteiligten Behörden entsprechend mit der Maßgabe, dass die Eingabe nur zulässig ist, wenn die Daten allen an der projektbezogenen Zusammenarbeit teilnehmenden Behörden übermittelt werden dürfen. Eine Eingabe ist ferner nur zulässig, wenn die Behörde, die die Daten eingegeben hat, die Daten auch in eigenen Dateien speichern darf. Die Daten sind zu kennzeichnen.

(3) Für die Führung einer projektbezogenen gemeinsamen Datei gelten § 11 Abs. 3 und § 12 Abs. 1 bis 4 entsprechend. § 11 Abs. 6 findet mit der Maßgabe Anwendung, dass die Protokollierung bei jedem Datenabruf erfolgt. § 12 Abs. 5 ist mit der Maßgabe anzuwenden, dass das Bundeskriminalamt die Auskunft im Einvernehmen mit der nach § 12 Abs. 5 Satz 2 zu beteiligenden Behörde erteilt und diese die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Bestimmungen prüft.

(4) Eine gemeinsame Datei nach Absatz 1 ist auf höchstens zwei Jahre zu befristen. Die Frist kann zweimalig um bis zu jeweils einem Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.

(5) Für die Berichtigung, Sperrung und Löschung personenbezogener Daten durch die Behörde, die die Daten eingegeben hat, gelten die jeweiligen, für sie an-

wendbaren Vorschriften über die Berichtigung, Sperrung und Löschung von Daten entsprechend. Für Daten, die das Bundeskriminalamt eingegeben hat, findet § 32 mit Ausnahme von § 32 Abs. 2 Nr. 2, Abs. 4 Satz 5 und Abs. 5 Anwendung.

(6) Das Bundeskriminalamt hat für die gemeinsame Datei in einer Errichtungsanordnung die Angaben nach § 34 Abs. 1 Satz 1 Nr. 1 bis 9 festzulegen sowie im Einvernehmen mit den an der projektbezogenen Zusammenarbeit teilnehmenden Behörden deren jeweilige Organisationseinheiten zu bestimmen, die zur Eingabe und zum Abruf befugt sind. Die Errichtungsanordnung bedarf der Zustimmung des Bundesministeriums des Innern sowie der für die Fachaufsicht der zusammenarbeitenden Behörden zuständigen obersten Bundes- und Landesbehörden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass einer Errichtungsanordnung anzuhören. § 34 Abs. 3 gilt entsprechend.“

Artikel 5

Inkrafttreten

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

(2) Artikel 1 tritt mit Ablauf des 30. Dezember 2017 außer Kraft und ist fünf Jahre nach dem Inkrafttreten unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren.

Die verfassungsmäßigen Rechte des Bundesrates sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt. Es ist im Bundesgesetzblatt zu verkünden.

Berlin, den 22. Dezember 2006

Der Bundespräsident
Horst Köhler

Die Bundeskanzlerin
Dr. Angela Merkel

Der Bundesminister des Innern
Schäuble