**Stand: 14.06.06**

**V o r b l a t t**

# Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz)

## A. Problem und Ziel

Ziel des Gesetzentwurfs ist es, angesichts der Bedrohungen durch den internationalen Terrorismus den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern.

## B. Lösung

Es werden die gesetzlichen Grundlagen für die Errichtung einer gemeinsamen standardisierten Zentralen Antiterrordatei sowie von gemeinsamen Projektdateien von Polizeien und Nachrichtendiensten geschaffen.

## C. Alternativen

Keine.

## D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

2. Vollzugsaufwand

Die Einrichtung einer gemeinsamen standardisierten Zentralen Antiterrordatei führt zu einem einmaligen finanziellen Mehraufwand beim Bund und bei den Ländern. Die Folgekosten lassen sich derzeit noch nicht beziffern.

## E. Sonstige Kosten

Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

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

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

Das Bundeskriminalamt, 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
### Inhalt der Antiterrordatei und Speicherungspflicht

(1) Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach Absatz 2 in der Antiterrordatei zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse verfügen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die Daten sich auf

1. Personen, die

   a) einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, die einen internationalen Bezug 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 Vereinigung, 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, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen,

3. Personen, bei denen tatsächliche Anhaltspunkte die Annahme begründen, dass sie mit den in Nummer 1 Buchstabe a oder in Nummer 2 genannten Personen in Verbindung stehen und durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können, oder

4. a) Vereinigungen, 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,

beziehen 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.

(2) In der Antiterrordatei werden, soweit vorhanden, folgende Datenarten gespeichert:

1. a) zu Personen:
aa) nach Absatz 1 Satz 1 Nr. 1 bis 3 folgende Grunddaten: der Familienname, die Vornamen, frühere Namen, andere

Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, die aktuelle und frühere Staatsangehörigkeiten, die Volkszugehörigkeit, die aktuelle und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder und die Rechtsgrundlage der Speicherung (Grunddaten),

bb) nach Absatz 1 Satz 1 Nr. 1 und 2 folgende erweiterte Grunddaten:

aaa) eigene und genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte,
bbb) Adressen für elektronische Post,
ccc) Bankverbindungen,
ddd) Schließfächer
eee) auf die Person zugelassene Kraftfahrzeuge sowie sonstige genutzte Fahrzeuge,
fff) 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 Strafgesetzbuches dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,
ggg) Fahr- und Flugerlaubnisse,
hhh) besuchte Orte, an denen sich in Absatz 1 Satz 1 Nr. 1 und 2 genannte Personen treffen,
iii) Kontaktpersonen zu den jeweiligen Personen nach Absatz 1 Satz 1 Nr. 1 Buchstabe a oder Nr. 2, sofern sie die Voraussetzungen von Absatz 1 Satz 1 Nr. 3 erfüllen,
jjj) Zugehörigkeit zu einer konkreten Vereinigung nach Absatz 1 Satz 1 Nr. 1 Buchstabe a oder b, und

b) Angaben zur Identifizierung der in Absatz 1 Satz 1 Nr. 4 genannten Vereinigungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Tele-

kommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post, mit Ausnahme weiterer personenbezogener Daten,

2. die Behörde, die über die Erkenntnisse verfügt, sowie das zugehörige Aktenzeichen oder sonstige Geschäftszeichen und, soweit vorhanden, die jeweilige Einstufung als Verschlusssache.

(3) Nur die Behörde, die Daten in die Antiterrordatei eingegeben hat, darf diese Daten verändern, berichtigen, sperren oder löschen.

## § 3
## Beschränkte und verdeckte Speicherung

(1) Soweit besondere Geheimhaltungsinteressen dies erfordern, darf eine beteiligte Behörde entweder von einer Speicherung der in § 2 Abs. 2 Nr. 1 Buchstabe a Doppelbuchstabe bb genannten erweiterten Grunddaten ganz oder teilweise absehen (beschränkte Speicherung) oder alle jeweiligen Daten zu in § 2 Abs. 1 genannten Personen, Vereinigungen, 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).

(2) Sind Daten, auf die sich eine Abfrage bezieht, verdeckt gespeichert, wird die eingebende Behörde automatisiert durch Übermittlung aller Anfragedaten über die Abfrage unterrichtet und hat unverzüglich mit der abfragenden Behörde Kontakt aufzunehmen, um zu klären, ob Erkenntnisdaten nach § 5 übermittelt werden können. Die eingebende Behörde 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.

## § 4
## Verwendung der Daten

(1) Die beteiligten Behörden dürfen die in der Antiterrordatei gespeicherten Daten im automatisierten Verfahren nutzen. Im Falle eines Treffers erhält die abfragende Behörde Zugriff

1. a) bei einer Abfrage zu Personen nach § 2 Abs. 1 Satz 1 Nr. 1 und 2 auf die zu ihnen gespeicherten Grunddaten und erweiterten Grunddaten,
   b) bei einer Abfrage zu Personen nach § 2 Abs. 1 Satz 1 Nr. 3 auf die zu ihnen gespeicherten Grunddaten oder
   c) bei einer Abfrage zu Vereinigungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post nach § 2 Abs. 1 Satz 1 Nr. 4 auf die dazu gespeicherten Daten, und

2. auf die Daten nach § 2 Abs. 2 Nr. 2.

Die abfragende Behörde darf die Daten nur zur Prüfung, ob der Treffer der gesuchten Person oder der gesuchten Angabe nach § 2 Abs. 1 Satz 1 Nr. 4 zuzuordnen ist, und für ein Ersuchen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus verwenden. Eine Verwendung zu einem anderen Zweck als nach Satz 3 ist nur zulässig, soweit

1. es zur Erfüllung der jeweiligen Aufgaben zur Aufklärung und Bekämpfung des internationalen Terrorismus erforderlich ist,
2. eine Übermittlung nach anderen Rechtsvorschriften auch zu diesem Zweck zulässig wäre und
3. die eingebende Behörde der Verwendung zustimmt.

Im Falle einer Verwendung nach Satz 4 sind die Daten zu kennzeichnen; nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrecht zu erhalten.

(2) Innerhalb der beteiligten Behörden erhalten ausschließlich besonders ermächtigte Personen Zugriff auf die Antiterrordatei.

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

(4) Soweit das Bundeskriminalamt und die Landeskriminalämter auf Ersuchen oder im Auftrag des Generalbundesanwalts die Antiterrordatei nutzen, übermitteln sie die Daten nach Absatz 1 Satz 2 dem Generalbundesanwalt für die Zwecke der Strafverfolgung. Der Generalbundesanwalt darf die Daten für Ersuchen nach Absatz 1 Satz 3 verwenden. § 487 Abs. 3 der Strafprozessordnung gilt entsprechend.

## § 5
## Übermittlung von Erkenntnissen

Die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 4 Abs. 1 Satz 3 zwischen den beteiligten Behörden richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

## § 6
## 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 eingebende Behörde muss erkennbar sein. Die Verantwortung für die Zulässigkeit der Abfrage trägt die abfragende Behörde.

(2) Hat eine Behörde Anhaltspunkte dafür, dass Daten, die eine andere Behörde gespeichert hat, unrichtig sind, teilt sie dies umgehend der eingebenden Behörde mit, die diese Mitteilung unverzüglich prüft und erforderlichenfalls die Daten unverzüglich berichtigt.

## § 7
## 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 § 4 Abs. 3 zu protokollieren. Die Protokolldaten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage und, soweit erforderlich, zum Nachweis der Kenntnisnahme bei Verschlusssachen verwendet werden. Die ausschließlich für Zwecke nach Satz 1 gespeicherten Protokolldaten sind nach achtzehn Monaten zu löschen.

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

## § 8
## Datenschutzrechtliche Kontrolle, Rechte der 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 jeweiligen 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 § 6 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 eingebende Behörde geltenden Rechtsvorschriften.

## § 9
## 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 Erkenntnisdaten 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.

## § 10
## 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. der Art der zu speichernden Daten,
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 zu-

ständigen obersten Landesbehörden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass der Errichtungsanordnung anzuhören.

## Artikel 2
## Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch ..., 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 Vorbereitungshandlungen 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 eingebende Behörde die Daten auch in eigene Dateien speichern darf. Die eingebende Behörde 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 eingebende Behörde, gelten die jeweiligen, für die Behörde 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 eingebende Behörde,
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 Löschfrist und
9. die Zuständigkeit des Bundesamtes für Verfassungsschutz für Schadensersatzansprüche des Betroffenen nach § 8 Bundesdatenschutzgesetz.

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 Gesetzes über den Bundesnachrichtendienst

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch ..., 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 eingebende Behörde die Daten auch in eigenen Dateien speichern darf. Die eingebende Behörde hat die Daten 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 Projek-

tende 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 eingebende Behörde 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 eingebende Behörde,
7. die Möglichkeit der ergänzenden Eingabe weiterer Daten zu den bereits über eine Person gespeicherte 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 ..., 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 eingebende Behörde die Daten auch in eigenen Dateien speichern darf. Die eingebende Behörde hat die Daten 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 eingebende Behörde, gelten die jeweiligen, für diese Behörde anwendbaren 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**

Artikel 1 tritt am ersten Tag des ……. auf die Verkündung folgenden Kalendermonats in Kraft. Artikel 2 bis 4 dieses Gesetzes treten am Tage nach der Verkündung in Kraft.

*[zur Erläuterung: Die Regelung zum Inkrafttreten ist des ATDG ist abhängig davon, wie schnell sich die Datei technisch realisieren lässt. Erste Realisierungsschritte sind bereits eingeleitet. Weitere Schritte sind jedoch u.a. davon abhängig, ob noch wesentliche Änderungen an dem Gesetzestext vorgenommen werden.]*

## Begründung

## Erster Teil: Allgemeines

### A. Anlass und Zielsetzung des Entwurfs

Die anhaltend hohe Bedrohung durch den internationalen Terrorismus erfordert einen bestmöglichen Einsatz der Instrumente zur Gewinnung und zum Austausch von Erkenntnissen der Sicherheitsbehörden von Bund und Ländern. Dazu gehört auch die Nutzung moderner Informationstechnologie, einschließlich gemeinsamer Dateien von Polizeien und Nachrichtendiensten.

Die Rechtsgrundlagen für die Tätigkeit der Polizeibehörden (BKAG, BGSG und der Nachrichtendienste des Bundes (BVerfSchG, MADG, BNDG, Artikel 10-Gesetz (G 10)) sowie der Länder und des Zollkriminalamtes (ZFdG) 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 der Verfassungsschutzbehörden von Bund und Ländern. Demgegenüber fehlen Normen, die gemeinsame Dateien zulassen, an denen sowohl Polizeibehörden als auch Nachrichtendienste beteiligt sind. Mit dem vorliegenden Gesetzentwurf werden die besonderen Rechtsgrundlagen für den Betrieb solcher gemeinsamer Dateien geschaffen. Die in dem Entwurf vorgesehenen gemeinsamen Dateien dienen dazu, den Informationsaustausch zwischen diesen Behörden effektiver zu gestalten und bewährte Formen der Zusammenarbeit sinnvoll zu ergänzen. Sie verringern zudem das Risiko von Übermittlungsfehlern.

### B. Wesentliche Schwerpunkte des Entwurfs

Durch den Gesetzentwurf wird zum einen die Rechtsgrundlage für die Errichtung einer gemeinsamen standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG) geschaffen.

Mit der standardisierten zentralen Antiterrordatei wird der Informationsaustausch zwischen dem Bundeskriminalamt (BKA) den Landeskriminalämtern, den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst (MAD), dem Bundesnachrichtendienst (BND) und dem Zollkriminalamt (ZKA) im Be-

reich der Bekämpfung des internationalen Terrorismus intensiviert und beschleunigt. Einzelne Erkenntnisse, über die eine beteiligte Behörde bereits verfügt und die bei einer entsprechenden Verknüpfung mit den Erkenntnissen anderer beteiligter Behörden zur Terrorismusbekämpfung beitragen können, werden durch die standardisierte Zentrale Antiterrordatei leichter zugänglich. Zu diesem Zwecke werden die beteiligten Behörden verpflichtet, in der Antiterrordatei Daten zu den relevanten Personen und Objekten zu speichern. Ein Datenabruf aus der Antiterrordatei führt zu einer deutlichen Vereinfachung des Verfahrens und damit zu einer Optimierung des Informationsaustauschs.

Das ATDG sieht vor, dass neben Grunddaten, die in erster Linie die Identifizierung einer bestimmten Person oder eines bestimmten Objekts ermöglichen und angeben, bei welcher Behörde weitere Erkenntnisse vorliegen, auch erweiterte Grunddaten zu diesen Personen oder Objekten gespeichert werden, die auch eine erste Bewertung zulassen. Von der Speicherung dieser erweiterten Grunddaten kann jedoch abgesehen werden, wenn besondere Geheimhaltungsinteressen entgegenstehen. Durch diese Regelung wird sichergestellt, dass die beteiligten Nachrichtendienste sensible Informationen zu Personen nicht ohne vorherige Prüfung des jeweiligen Falles anderen Behörden offen legen müssen. Die Geheimhaltung einer Quelle ist 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, unverzichtbar.

Zum anderen werden mit dem Gesetzentwurf die gesetzlichen Grundlagen für projektbezogene gemeinsame Dateien (Projektdateien) geschaffen, die der Unterstützung einer befristeten projektbezogenen Zusammenarbeit der Verfassungsschutzbehörden des Bundes und der Länder, des MAD, dem BND, der Polizeibehörden des Bundes und der Länder und des ZKA dienen.

In Analyseprojekten und Arbeitsgruppen zum Informationsaustausch, die zur Durchführung einzelner Projekte zu bestimmten kriminalpolizeilich und nachrichtendienstlich relevanten Bereichen eingerichtet werden, arbeiten verschiedene der genannten Behörden bereits heute eng zusammen. Diese Analyseprojekte und Arbeitsgruppen zum Informationsaustausch haben sich als wichtige Instrumente der Terrorismusbekämpfung bewährt. Sie dienen dazu, auf der Grundlage der bestehenden Übermittlungsvorschriften phänomenbezogene Erkenntnisse auszutauschen, zu analysieren und Bekämpfungsansätze zu entwickeln. In den vom BKA betreuten Arbeitsgruppen

zum Informationsaustausch (z.B. in der bereits im April 2001 im Zusammenhang mit dem „Meliani-Komplex“ eingerichteten Arbeitsgruppe „Netzwerke Arabischer Mudjahedin“) werden einzelne Gefährdungssachverhalte und strafrechtlich relevante Erkenntnisse im Hinblick auf relevante Zusammenhänge ausgewertet. Ziel ist eine bessere Nutzung der vorhandenen Informationen für konkrete strafrechtliche Ermittlungen und Maßnahmen der Gefahrenabwehr. Die beim BfV eingerichteten Analyseprojekte (z.B. „Ausbildungslager der Arabischen Mudjahedin“) dienen der Erstellung von Hintergrundanalysen zu Aktivitäten des islamistischen Terrorismus und ergänzen damit die vorrangig ermittlungsbezogene Arbeit der Arbeitsgruppen zum Informationsaustausch.

Nach geltendem Recht müssen die Projektmitarbeiterinnen und -mitarbeiter der beteiligten Behörden allerdings im Rahmen der Projektarbeit jeweils eigene Dateien ihrer Behörden anlegen, auf die die Projektmitarbeiterinnen und -mitarbeitern anderer Behörden keinen Zugriff haben. Dies bedeutet, dass Informationen, die allen Projektmitarbeiterinnen und -mitarbeitern bereits zur Verfügung stehen oder übermittelt werden dürfen, jeweils getrennt in mehrere – inhaltlich gleiche – Dateien eingegeben oder regelmäßig auf Datenträgern, wie CD-ROMs, an die übrigen teilnehmenden Behörden übermittelt werden. Dadurch werden die Arbeitsabläufe der Projektarbeit deutlich erschwert. Gemeinsame Projektdateien führen hier zu einer erheblichen Arbeitserleichterung. Durch ihren jeweiligen Zuschnitt auf die konkrete Projektarbeit können in den Projektdateien umfassende Informationen zu relevanten Personen, Objekten und Sachverhalten zu konkreten Themenkomplexen zudem gezielt verdichtet werden.

Gesetzliche Grundlagen für die Errichtung von gemeinsamen Projektdateien werden nach dem Gesetzentwurf sowohl in das BVerfSchG und in das BNDG als auch in das BKAG eingefügt. Damit wird dem Umstand Rechnung getragen, dass die Projektarbeit jeweils bei diesen Behörden angesiedelt sein kann. Die Regelungen zu den gemeinsamen Projektdateien der verschiedenen Behörden entsprechen einander.

## C. Gesetzgebungskompetenz des Bundes

Die Zuständigkeit des Bundes zum Erlass dieser Vorschriften ergibt sich aus Art. 73 Nr. 10 GG, soweit das Zollkriminalamt betroffen ist, aus Art. 73 Nr. 5 GG und, soweit der Bundesnachrichtendienst und der Militärische Abschirmdienst betroffen sind, aus Artikel 73 Nr. 1 GG.

## D. Finanzielle Auswirkung

Mit der Ausführung des Gesetzes werden Bund und Länder mit [noch nicht näher zu spezifizierenden] Mehrkosten belastet. Die Einrichtung einer gemeinsamen zentralen Antiterrordatei führt zu einem einmaligen finanziellen Mehraufwand beim Bund und bei den Ländern. *[wird noch näher ausgeführt]* Die Folgekosten lassen sich derzeit noch nicht beziffern. *[wird ebenfalls noch näher ausgeführt]* Die entstehenden Mehrkosten müssen in den betroffenen Einzelplänen gegenfinanziert werden.

## E. Sonstige Kosten

Das Antiterrordateigesetz sowie die Änderungen des BVerfSchG, des BNDG und des BKAG werden keine Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, haben.

## F. 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 jedoch gleichstellungspolitisch weder positive noch negative Auswirkungen. Die Regelungen sind entsprechend § 1 Abs. 2 Satz 1 BGleiG geschlechtergerecht formuliert.

**Zweiter Teil: Zu den einzelnen Vorschriften**

**Zu Art. 1** (Antiterrordateigesetz – ATDG)

Zu § 1

Die Vorschrift schafft die Rechtsgrundlage für die Einrichtung der gemeinsamen standardisierten zentralen Antiterrordatei. 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 Antiterrordatei. 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 Antiterrordatei dient dazu, die beteiligten Behörden bei der Erfüllung der ihnen in den jeweiligen gesetzlichen Vorschriften zugewiesenen Aufgaben im Bereich des internationalen Terrorismus zu unterstützen, wobei mit den Begriffen der „Aufklärung“ die nachrichtendienstlichen Aufgaben und mit dem Begriff der „Bekämpfung“ die polizeilichen Aufgaben erfasst werden. Das ZKA nimmt insoweit mit der Aufgabe, den Missbrauch des grenzüberschreitenden Waren- und Kapitalverkehrs für terroristische Zwecke zu verhindern, an der Bekämpfung des internationalen Terrorismus teil. Im Bereich des grenzüberschreitenden Warenverkehrs handelt es sich insbesondere um die Mitwirkung bei der außenwirtschaftsrechtlichen Überwachung (Exportkontrolle) im Hinblick auf die Verhinderung des unzulässigen Exports bestimmter Waren, z. B. von Sprengstoffen, Waffen oder von Massenvernichtungsmitteln, welche für terroristische Zwecke verwendet werden könnten. Im Rahmen der Maßnahmen zur Bekämpfung der Finanzierung des internationalen Terrorismus betrifft dies beispielsweise die Umsetzung der Verordnungen (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001 (ABl. EG Nr. L 344 S. 70) und (EG) Nr. 881/2002 vom 27. Mai 2002 (ABl. EG Nr. L 139 S. 9) in ihrer jeweils geltenden Fassung.

Die Antiterrordatei unterstützt die beteiligten Behörden bei ihrer Aufgabenerfüllung, indem sie den Austausch von Erkenntnissen zu terrorismusrelevanten Sachverhalten erleichtert und damit den Informationsaustausch insgesamt beschleunigt. Neue Aufgaben werden mit dem ATDG für die beteiligten Behörden nicht geschaffen. Die Begrenzung auf den internationalen Terrorismus mit Bezügen zur Bundesrepublik

Deutschland begrenzt den Umfang der in der Antiterrordatei zu speichernden Informationen. Insbesondere beim BND vorliegende Erkenntnisse über das Ausland, die zwar für die Lagebeurteilung von großem Wert sein können, aus denen sich jedoch keine Anhaltspunkte für eine Gefährdung der Bundesrepublik Deutschland ergeben, erscheinen für die Terrorismusbekämpfung innerhalb Deutschlands von vornherein nicht relevant.

Zu § 2

Die Vorschrift regelt den Inhalt der Antiterrordatei.

Absatz 1

Satz 1 verpflichtet die beteiligten Behörden sowohl zur Speicherung von Daten zu Personen als auch von Daten zu Vereinigungen, Stiftungen, Unternehmen oder Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post sowie die dazugehörigen Fundstellen in der Antiterrordatei. Es handelt sich hierbei um bestimmte Personen (Satz 1 Nr. 1 bis 3) und Organisationen oder Sachen etc. (Satz 1 Nr. 4), zu denen bei den beteiligten Behörden weitergehende polizeiliche oder nachrichtendienstliche Erkenntnisse vorliegen, deren Kenntnis für die beteiligten Behörden bei der Aufklärung und Bekämpfung des internationalen Terrorismus erforderlich ist. Der Begriff der polizeilichen oder nachrichtendienstlichen Erkenntnisse umfasst so genannte Vorfelderkenntnisse. 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 Antiterrordatei vorliegen. Durch die unverzügliche Speicherung dieser Daten ist die Aktualität der Antiterrordatei sicherzustellen.

Das ATDG schafft keine zusätzliche Rechtsgrundlage für die Datenerhebung durch die beteiligten Behörden. In der Antiterrordatei 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 Kontakt- und Begleitpersonen (Satz 1 Nr. 3). Damit sind die bereichsspezifischen Regelungen zur Erhebung und Speicherung von Daten zu Kontakt- und Begleitpersonen in den jeweils für die beteiligten Behörden geltenden speziellen Vorschriften zu beachten.

Voraussetzung für die Speicherung von Daten in der Antiterrordatei ist, dass sich aus den bei den Behörden vorhandenen Erkenntnissen tatsächliche Anhaltspunkte dafür ergeben, dass sich diese auf die nachfolgend beschriebenen Personen oder Organisationen oder Sachen etc. (Satz 1 Nr. 4) beziehen. Das Tatbestandsmerkmal der tatsächlichen Anhaltspunkte ist erfüllt, wenn die im Einzelfall vorliegenden Anhaltspunkte nach nachrichtendienstlichen und polizeilichen Erfahrungswerten die Einschätzung rechtfertigen, dass die Erkenntnisse zu den betreffenden Personen und Organisationen oder Sachen etc. (Satz 1 Nr. 4) zur Aufklärung und Bekämpfung des internationalen Terrorismus beitragen. Dabei ist zu berücksichtigen, dass die Antiterrordatei auch das Ziel hat, bereits vorhandene Informationen der beteiligten Behörden zusammenzuführen, um terroristischen Gefahren bereits im Vorfeld zu begegnen. Der letzte Halbsatz regelt, dass die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland erforderlich sein muss. Diese Erforderlichkeit ist hinsichtlich der Personen nach Nummer 1 bereits aufgrund der dortigen Tatbestandsmerkmale gegeben.

Zu Nummer 1

Nach Nummer 1 Buchstabe a sind Daten zu Personen zu speichern, die einer inländischen terroristischen Vereinigung nach § 129a StGB, welche einen internationalen Bezug aufweist, oder einer ausländischen terroristischen Vereinigung nach §§ 129a, 129b Abs. 1 Satz 1 StGB mit einem Bezug zu Deutschland angehören oder diese unterstützen. Durch die Begrenzung auf inländische terroristische Vereinigungen nach § 129a StGB mit einem internationalen Bezug einerseits und ausländische terroristische Vereinigungen nach §§ 129a, 129b Abs. 1 Satz 1 StGB mit einem Deutschlandbezug andererseits werden rein innerstaatliche Kriminalitätsbereiche, wie etwa ein auf Deutschland fixierter links- oder rechtsextremistisch motivierter Terrorismus, ebenso wenig erfasst wie im Ausland lediglich regional auftretende terroristische Vereinigungen, von denen nach den vorliegenden Erkenntnissen aller Voraussicht nach keine terroristischen Gefahren für Deutschland ausgehen. Ein internationaler Bezug einer terroristischen Vereinigung mit Organisation in Deutschland liegt jedoch insbesondere dann vor, wenn sie international propagierten ideologischen Strömungen, die auch in anderen Staaten militant verfolgt werden, zuzurechnen ist. Ein Bezug zu Deutschland muss angenommen werden, wenn die terroristische Vereinigung einer ideologischen Strömung angehört, die sich auch gegen Deutschland oder deutsche Ziele und Interessen richtet oder von ihr aufgrund sonstiger Erwägungen eine potenzielle Gefahr auch für Deutschland ausgeht. Damit wird der gesamte Bereich des islamistischen Terrorismus erfasst.

Erfasst werden Personen, bei denen tatsächliche Anhaltspunkte dafür sprechen, dass sie einer solchen terroristischen Vereinigung selbst angehören oder sie unterstützen. Das Vorliegen der Voraussetzungen des Abs. 1 Nr. 1 kann in Betracht kommen, wenn es sich um eine Person handelt, deren Name in die im Zusammenhang mit der Bekämpfung des Terrorismus angenommene Liste zum Gemeinsamen Standpunkt des Rates 2001/931/GASP vom 27. Dezember 2001 (ABl. EG Nr. L 344 S. 93) in der jeweils geltenden Fassung aufgenommen wurde oder in Anhang I der Verordnung (EG) Nr. 881/2002 des Rates vom 27. Mai 2002 (ABl. EG Nr. L 139 vom 29. Mai 2002 S. 9) in der jeweils geltenden Fassung gelistet ist. Der Begriff des Unterstützens ist im Sinne des § 129a Abs. 5 Satz 1 StGB zu verstehen.

Über Nummer 1 Buchstabe b werden auch Daten zu Personen erfasst, die einer Vereinigung angehören oder sie unterstützen, die zwar selbst keine terroristischen Anschläge plant und begeht, aber terroristische Organisationen unterstützt. Buchstabe b ergänzt die Regelung der Nummer 1 Buchstabe a zu terroristischen Vereinigungen im strafrechtlichen Sinne somit um das terroristische Umfeld.

Zu Nummer 2

Die Regelung stellt auf Personen ab, die rechtswidrig Gewalt als Mittel zur Durchsetzung ihrer international ausgerichteten politischen oder religiösen Belange anwenden, eine solche Gewaltanwendung unterstützen, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen. Erfasst werden insbesondere auch gewalttätige und gewaltbereite Einzeltäter oder Einzeltäterinnen. Dabei wird eine positive Stellungnahme des Betroffenen zur Gewaltanwendung vorausgesetzt. Dementsprechend betreffen die Tatbestandsmerkmale des Unterstützens und vorsätzlichen Hervorrufens die Förderung von Gewaltanwendung, wobei diese nicht bereits durch bestimmte Handlungen konkretisiert sein muss. Der Begriff des Unterstützens ist auch hier im Sinne des § 129a Abs. 5 Satz 1 StGB, d.h. als Handlung, die für den Einsatz von Gewalt irgendwie vorteilhaft ist, zu verstehen. Das Tatbestandsmerkmal des Befürwortens setzt voraus, dass die betreffende Person die entsprechende Gewaltanwendung gutheißt. Dies könnte insbesondere bei so genannten Hasspredigern der Fall sein. Die Einbeziehung des Vorfeldes ist angesichts der zu schützenden hochrangigen Rechtsgüter notwendig, um terroristische Gefahren umfassend aufzuklären und ihnen möglichst frühzeitig begegnen zu können.

Zu Nummer 3

Nach Nummer 3 sind auch Daten zu Kontakt- und Begleitpersonen von potenziellen terroristischen Straftätern oder Straftäterinnen und extremistischen Gewalttätern oder Gewalttäterinnen im Sinne von Nummer 1 Buchstabe 1 a und Nummer 2 zu spei-

chern. Kontakt- und Begleitpersonen sind Personen, bei denen tatsächliche Anhaltspunkte die Annahme begründen, dass sie mit den in Nummer 1 Buchstabe a und Nummer 2 genannten Personen in Verbindung stehen und durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können. Die konkreten tatsächlichen Umstände sind hierzu unter Berücksichtigung nachrichtendienstlicher bzw. polizeilicher Erfahrung zu würdigen. Kriterien für eine derartige Verbindung können beispielsweise die nähere persönliche oder geschäftliche Beziehung, die Dauer der Verbindung oder die konspirativen Umständen sein, unter denen die Personen die Verbindung hergestellt haben oder pflegen. In der Antiterrordatei dürfen jedoch nur die Kontakt- und Begleitpersonen 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 Kontakt- und Begleitpersonen aufgrund spezialgesetzlicher Ausprägungen des Verhältnismäßigkeitsgrundsatzes besondere Anforderungen gelten, sind diese auch im Falle der Speicherung in der Antiterrordatei zu beachten.

Zu Nummer 4

Die Vorschrift regelt die Speicherung von Daten zu Vereinigungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post. Die Aufzählung ist abschließend. Die Regelung betrifft nur Organisationen oder Sachen etc., die mit Personen nach Nummer 1 oder Nummer 2 in Zusammenhang stehen. Dabei kommt es nicht darauf an, dass die Identität einer solchen Person bereits bekannt ist oder das Objekt einer bestimmten Person zugeordnet werden kann. Eine Verknüpfung zu einer nach Nummer 1 oder 2 gespeicherten Person in der Datei ist nicht vorgesehen. Daten zu Personen und zu Organisationen oder Sachen etc. sind getrennt zu recherchieren (vgl. § 4 Abs. 1).

Satz 2 enthält eine Einschränkung der in Satz 1 geregelten Speicherungspflicht. In der Antiterrordatei sind von den beteiligten Behörden nur die Daten zu speichern, die sie automatisiert verarbeiten dürfen. So darf das BfV beispielsweise Daten von Minderjährigen, die das 16. Lebensjahr noch nicht vollendet haben, nicht in Dateien speichern (§ 11 Abs. 1 Satz 2 BVerfSchG). Satz 2 stellt sicher, dass derartige Einschränkungen auch für die Speicherung von Daten in der Antiterrordatei gelten.

Zu Absatz 2

Absatz 2 regelt, welche Datenkategorien zu den in Absatz 1 genannten Personen und Objekten gespeichert werden.

Nummer 1 Buchstabe a) bezieht sich auf die zu speichernden Personendaten. Zu speichern sind Grunddaten nach Buchstabe aa) sowie erweiterte Grunddaten nach Buchstabe bb). Zu den Grunddaten zählen neben den üblichen Personendaten (vgl. § 5 Abs. 1 Nr. 1 Bundeszentralregistergesetz) andere Namen, Aliaspersonalien und abweichende Namensschreibweisen (vgl. § 3 Nr. 5 Ausländerzentralregistergesetz) die Volkszugehörigkeit, aktuelle und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte und Lichtbilder. Diese Daten dienen der Identifizierung der abgefragten Personen. Den beteiligten Behörden liegen insbesondere im Bereich des islamistischen Terrorismus häufig nur bruchstückhafte Informationen zu relevanten Personen vor. Unter diesen Informationen sind nach den polizeilichen und nachrichtendienstlichen Erfahrungen häufig neben dem Namen, dem in zahlreichen Kulturkreisen nur eine untergeordnete und unverbindliche Bedeutung zukommt und der daher zur Identifizierung einer Person nur sehr bedingt geeignet ist, Angaben zur Volkszugehörigkeit, zu Anschriften, besonderen körperlichen Merkmalen, wie etwa Tätowierungen oder Narben, Sprachen oder Dialekten zu finden. Die Speicherung dieser Daten ist daher für einen zielgenauen und schnellen Trefferabgleich, dem zur Vereitelung eines terroristischen Anschlags entscheidende Bedeutung zukommen kann, unverzichtbar (vgl. Erläuterung zu § 4 Abs. 1). Weiteres Grunddatum ist die Angabe, auf welcher Rechtsgrundlage die Speicherung erfolgt ist. Mit den Rechtsgrundlagen sind die jeweiligen Tatbestände des Abs. 1 sowie die dort genannten Tatbestandsalternativen gemeint. Die Angabe der Rechtsgrundlage dient zum einen der Kontrolle der Verwaltung. Zum anderen ermöglicht sie der abfragenden Behörde eine erste Einschätzung, mit welcher Priorität und Dringlichkeit ein Ersuchen zu stellen ist. Bei einer der abfragenden Behörde bislang unbekannten Person, die nach Absatz 1 Nr. 1 als Rädelsführer oder Hintermann einer terroristischen Vereinigung (§ 129a Abs. 4 StGB) verdächtig bei der Polizei gespeichert ist, kann die Kontaktaufnahme zu der eingebenden Behörde beispielsweise auch nachts angezeigt sein, während dies bei einer bloßen Kontakt- und Begleitperson nicht ohne weiteres der Fall wäre.

Während die Grunddaten nach Doppelbuchstabe aa zu allen in Absatz 1 genannten Personen gespeichert werden, ist die Speicherung der erweiterten Grunddaten nach Doppelbuchstabe bb nur hinsichtlich der Personen nach Absatz 1 Nr. 1 und 2 vorgesehen. Zu den nach Absatz 1 Nr. 3 zu speichernden Kontakt- und Begleitpersonen werden aus Gründen der Verhältnismäßigkeit keine erweiterten Grunddaten erfasst. Die erweiterten Grunddaten dienen ebenfalls der Identifizierung einer gesuchten Person. Zu diesen Objektdaten zählen die eigenen und genutzten Telekommunikationsanschlüsse und Telekommunikationsendgeräte, Adressen für elektronische Post,

Bankverbindungen, Schließfächer, besondere Fähigkeiten, Fahr- und Flugerlaubnisse, besuchte Orte und auf die Person zugelassene sowie sonstige genutzte Fahrzeuge. Die einzelnen Datenkategorien, die nach Absatz 1 Nr. 4 z.T. 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 internationalen Terrorismus. Ihnen kommt nach den Erfahrungen der beteiligten Behörden bei der Terrorismusbekämpfung ebenso wie den Grunddaten nach Doppelbuchstabe aa eine herausragende Bedeutung zu. Dies gilt insbesondere für Bankverbindungen, Telekommunikationsanschlüsse und Fahrzeuge.

Die Angabe von Bankverbindungen der in Absatz 1 Nr. 1 und 2 genannten Personen ist erforderlich, weil der Vorbereitung und Durchführung terroristischer Anschläge in aller Regel finanzielle Transaktionen vorausgehen, zu denen den beteiligten Behörden häufig Hinweise vorliegen. Gelder, die für terroristische Zwecke benötigt werden, werden überwiegend durch Spenden sowie durch legale oder illegale wirtschaftliche Tätigkeiten beschafft. Hierzu werden neben den inoffiziellen Überweisungssystemen nachweislich auch die offiziellen Zahlungs- und Geldtransfersysteme der Banken genutzt.

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 nach den Anschlägen der jüngeren Vergangenheit ist, dass die Täter in aller Regel nicht ihre eigenen Mobilfunkgeräte oder Fahrzeuge genutzt haben, sondern sich unter Verwendung von Aliaspersonalien bzw. der unerlaubten Nutzung echter Personalien Zugang zu Telekommunikationsgeräten bzw. –anschlüssen verschaffen. Mobiltelefone 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 Abs.1 Satz 1 Nr. 1 oder 2 fallen und nicht wissen, dass ihr Telefon von entsprechenden Personen genutzt wird. Angesichts der durch den internationalen Terrorismus bedrohten Rechtsgüter ist die Speicherung dieser Daten verhältnismäßig. Unter den Voraussetzungen des § 100a Abs. 1 Satz 2

StPO wäre auch eine Telekommunikationsüberwachung der Anschlüsse Unbeteiligter zulässig.

Gleiches gilt für genutzte Kraftfahrzeuge, da bei der Tatvorbereitung z.B. Fahrten zu bestimmten Treffpunkten in der Regel nicht ihre eigenen Fahrzeuge nutzen.

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

Die Angabe von besuchten Orten, an denen sich die in Absatz 1 Satz 1 Nr. 1 und 2 genannte Personen treffen, ist erforderlich, weil gerade die Information, dass sich eine Person an einschlägigen Orten verkehrt, häufig Bestandteil eines ansonsten bruchstückhaften, aber höchst terrorismusrelevanten, Hinweises ist. Zu diesen Orten zählen im Bereich des islamistischen Terrorismus unter anderem bekannte Trefforte wie z.B. Kulturzentren, einschlägig bekannte Moscheen aber auch Reisen und Auslandsaufenthalte z.B. in Trainingslagern oder Kampfgebieten entsprechender Staaten.

Zudem lässt sich in der Regel erst anhand der erweiterten Grunddaten beurteilen, in welcher Reihenfolge und mit welcher Dringlichkeit die entsprechenden Behörden um weitergehende Erkenntnisse ersucht werden müssen. Die anhand der erweiterten Grunddaten mögliche Beurteilung der Person kann unter Umständen im Zusammenhang mit den zusätzlichen Informationen dazu führen, dass diese sogleich weitere Maßnahmen ergreifen muss, um den aktuellen Sachverhalt weiter aufzuklären und möglicherweise einen terroristischen Anschlag zu vereiteln. Für diese Fälle sieht § 4 Abs. 1 Satz 4 unter bestimmten Voraussetzungen eine weitere Verwendung der Daten ohne ein vorheriges Ersuchen vor.

Soweit dies nicht aufgrund der zwingenden Individualität der Daten, wie z.B. bei der Bankverbindung, unmöglich ist, werden die erweiterten Grunddaten standardisiert eingegeben. Standardisierung der Angaben bedeutet, dass diese 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 Vereinheitlichung der Verwaltungspraxis sowie dem Schutz der Betroffenen gleichermaßen. Durch die Standardisierung sind die beteiligten Behörden gezwungen, sich insbesondere auf einen begrenzten Katalog von terrorismusrelevanten Fähigkeiten oder Orten zu verständigen. Dies können beispielsweise berufliche Fähigkeiten sein, die der Vorbereitung oder Durchführung eines terroristi-

schen Anschlags nach den Erkenntnissen der beteiligten Behörden besonders dienlich sein können (z.B. Chemiker oder Kampfsportler), Der einheitliche Sprachgebrauch erleichtert zudem die Kommunikation und den Datenaustausch zwischen den Behörden. Dem Schutz des Betroffenen dient die Standardisierung insofern, als keine weitergehenden individualisierten Angaben gemacht werden können.

Nach Buchstabe b sind Angaben zur Identifizierung der Organisationen oder Sachen etc. zu speichern. Zu den Angaben nach Abs. 1 Satz 2 Nr. 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 Organisationen oder Sachen etc. gespeichert werden.

Zu den Personendaten und den Angaben nach Absatz 1 Satz 2 Nr. 4 sind nach Nummer 2 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 Abs. 2 SÜG.

Zu Absatz 3

Nach Absatz 3 trägt die eingebende Behörde die datenschutzrechtliche Verantwortung. Nur sie ist berechtigt, die von ihr eingegebenen Daten zu verändern, zu berichtigen, zu sperren oder zu löschen.

Zu § 3

Die Vorschrift regelt die Möglichkeit der beschränkten und verdeckten Speicherung. Dieses Korrektiv stellt sicher, dass im Einzelfall überwiegenden Sicherheitsinteressen Rechnung getragen werden kann.

Zu Absatz 1

Die Vorschrift regelt den Begriff und die Voraussetzung der beschränkten und verdeckten Speicherung. Die jeweilige Behörde kann entweder im Falle einer beschränkten Speicherung ganz oder teilweise von einer Speicherung der in § 2 Abs. 2 Nr. 1 a) bb) genannten erweiterten Grunddaten absehen oder im Falle einer verdeck-

ten Speicherung diese 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 Organisationen oder Sachen etc. Daten verdeckt gespeichert sind. Eine beschränkte und verdeckte Speicherung ist nur zulässig, wenn sie aufgrund besonderer Geheimhaltungsinteressen erforderlich ist. Die Ausnahmevorschrift ist 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 nicht offen gespeichert werden können.

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 eingebende Behörde 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 verdeckt speichernden Behörde ermöglicht, den Trefferfall zu verifizieren. Nur in engen Ausnahmefällen, bei überwiegenden Geheimhaltungsinteressen nach den Umständen des Einzelfalls, darf die verdeckt speichernde Behörde 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 ggf. 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 verdeckt speichernde Behörde Informationen über die Dringlichkeit bzw. Wichtigkeit der Abfrage. Während etwa bei einer Abfrage, die der Abwehr einer erheblichen und gegenwärtigen Gefahr im Sinne eines drohenden terroristischen Anschlags dient, davon ausgegangen werden muss, dass das Ermessen der verdeckt speichernden Behörden, von einer Kontaktaufnahme abzusehen, gegen Null schrumpft und gegebenenfalls auch eine Notbereitschaft in Anspruch genommen werden muss, kann dem Aspekt des Quellenschutzes bei einer Abfrage im Rahmen eines laufenden Ermittlungsverfahrens ein anderes Gewicht zukommen oder im Hinblick auf die Eilbedürftigkeit durch die abfragende Behörde deutlich gemacht werden, dass im Falle einer verdeckten Speicherung eine unverzügliche Kon-

taktaufnahme im Rahmen des regulären Dienstbetriebes ausreicht. Die Informationen über die Dringlichkeit bzw. Wichtigkeit der Abfrage werden der verdeckt speichernden Behörde mit der Abfrage automatisiert und für die abfragende Behörde nicht erkennbar übermittelt (vgl. § 4 Abs. 3). Nach Satz 3 sind die wesentlichen Gründe für die nach Satz 2 zu treffende Entscheidung über eine Kontaktaufnahme zu dokumentieren. Die Dokumentationspflicht dient 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 § 9 Abs. 2; sie erfolgt mit der Löschung der dazugehörigen Erkenntnisdaten.

Zu § 4

Zu Absatz 1

Die Vorschrift regelt, dass die beteiligten Behörden die Antiterrordatei im automatisierten Verfahren nutzen dürfen. Satz 2 legt fest, auf welche der gespeicherten Daten die abfragende Behörde im Trefferfall Zugriff erhält. Im Falle einer Abfrage auf Personendaten nach § 2 Abs. 1 Satz 1 Nr. 1 bis 2 sind dies neben der Fundstelle und der etwaigen Einstufung als Verschlusssache (§ 2 Abs. 2 Nr. 2) die von den beteiligten Behörden gespeicherten Grunddaten und erweiterten Grunddaten. Da zu den Kontakt- und Begleitpersonen nach § 2 Abs. 1 Nr. 3 keine erweiterten Grunddaten gespeichert werden, erhält die Behörde nach Satz 2 Nr. 1 Buchstabe b nur Zugriff auf die gespeicherten Grunddaten. Aus der Verbindung des Satzes 2 Nr. 1 Buchstabe a und b mit Satz 2 Nr. 1 Buchstabe c durch das Wort „oder“ ergibt sich, dass eine kombinierte Abfrage von Daten nach Nummer 1 Buchstaben a, b und c nicht zulässig ist.

Die abgerufenen Daten der Antiterrordatei dürfen nach Satz 3 nur für Ersuchen zur Übermittlung von Erkenntnissen im Rahmen der Wahrnehmung der jeweiligen Aufgaben der beteiligten Behörden zur Aufklärung oder Bekämpfung des internationalen Terrorismus genutzt werden, wobei das eigentliche Ersuchen in der üblichen Art und Weise gestellt und weiter bearbeitet wird. Die Verwendungsbeschränkung gilt unbeschadet des Absatzes 4, der unter bestimmten Voraussetzungen die Übermittlung der Trefferdaten nach Satz 2 an den Generalbundesanwalt beim Bundesgerichtshof zulässt.

Eine Verwendung der Daten ist nach Satz 3 zunächst nur zum Zwecke des Trefferabgleich und des Stellens eines Ersuchens zulässig. Eine Prüfung, ob ein Treffer der gesuchten Person, Organisation 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, Organisation 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.

Eine Verwendung der Daten zu anderen Zwecken als nach Satz 3 ist nach Satz 4 nur im Rahmen der jeweiligen Aufgaben zur Aufklärung und Bekämpfung des internationalen Terrorismus zulässig. Sie setzt des Weiteren voraus, dass eine Übermittlung nach anderen Gesetzen auch zu diesem Zwecke zulässig wäre und die eingebende Behörde dieser anderen Verwendung zustimmt. Im Rahmen der Zustimmung prüft die eingebende Behörde ebenso wie bei der sonstigen Einzelfallbearbeitung die Richtigkeit und Aktualität sowie die Verlässlichkeit der Daten. Die Begrenzung sowie die weiteren Voraussetzungen der über die Ersuchensstellung hinausgehenden Verwendung der Daten trägt dem besonderen Zweck der Antiterrordatei sowie dem Umstand Rechnung, dass die beteiligten Behörden im Übrigen teilweise sehr unterschiedliche Aufgaben wahrnehmen. Die Verwendungsbeschränkung auf die jeweiligen Aufgaben zur Aufklärung und Bekämpfung des internationalen Terrorismus nach Satz 4 gilt nicht, für die Daten, die aufgrund eines Ersuchens übermittelt worden sind. Die zusätzlichen Anforderungen nach Satz 4 machen deutlich, dass die konventionelle Übermittlung der Daten aufgrund eines Ersuchens die Regel und die weitere Verwendung aufgrund einer schlichten Zustimmung nach Satz 4 die Ausnahme sein soll.

Aufgrund der Zweckbindung der nach Satz 4 weiter verwendeten Daten sind diese nach Satz 5 zu kennzeichnen.

Zu Absatz 2

Nach Absatz 2 erhalten nur Personen Zugriff auf die Antiterrordatei, die hierzu besonders ermächtigt sind. Die Ermächtigung nach Absatz 2 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 § 10 Satz 1 Nr. 4 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 internationalen Terrorismus oder diesen unterstützende Bestrebungen zuständig sind, sollen Zugriff auf die Antiterrordatei 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 3

Die Vorschrift verpflichtet die abfragende Stelle, bei jeder Abfrage den Zweck und die Dringlichkeit der Abfrage zu dokumentieren. Mit dieser Angabe soll die verdeckt speichernde Stelle im Trefferfall nach § 3 Abs. 2 Satz 2 die erforderliche Abwägung vornehmen können. Die Dokumentation des Zwecks und der Dringlichkeit kann standardisiert erfolgen und wird der verdeckt speichernden Behörde elektronisch durch das System übermittelt. Die Einteilungen der Zwecke und der Dringlichkeit einer Abfrage sind nach § 10 Satz 1 Nr. 5 in der Errichtungsanordnung festzulegen.

Zu Absatz 4

Absatz 4 Satz 1 regelt die Übermittlung der Daten nach Absatz 1 Satz 2 an den Generalbundesanwalt beim Bundesgerichtshof (GBA) im Rahmen seiner Aufgaben zur Strafverfolgung. Die Trefferdaten nach Absatz 1 Satz 2, die das BKA oder ein LKA mittels der Abfrage der Antiterrordatei erhält, sollen an den GBA übermittelt werden, wenn das BKA oder ein LKA auf Ersuchen oder im Auftrag des GBA handelt. In Ermittlungsverfahren nach § 129a StGB, auch in Verbindung mit § 129b StGB, hat der GBA die Sachleitungsbefugnis. Im Hinblick auf Struktur, Koordination und Taktik in der Führung derartiger Verfahren ist der GBA auf die Daten nach Absatz 1 Satz 2 angewiesen. Er kann daher nicht über weniger Informationen verfügen als seine Ermittlungspersonen. Der GBA kann die übermittelten Daten für Ersuchen an die zuständigen Behörden nutzen, dies stellt der Verweis auf Absatz 1 Satz 3 klar. Der

Verweis auf § 487 Abs. 3 StPO betrifft die Verantwortung für die Zulässigkeit der Übermittlung.

Zu § 5

Die Vorschrift regelt, dass die Übermittlung von weiteren Erkenntnisdaten nur nach den jeweils geltenden allgemeinen Übermittlungsvorschriften erfolgt, etwa nach § 10 Abs. 1 und 2 BKAG, § 33 ZFdG, § 5 Abs. 1 und 3, §§ 18 bis 22 BVerfSchG, § 3 Abs. 3, § 10 Abs. 1, § 11 MADG, §§ 8, 9 BNDG, § 4 Abs. 4 Nr. 1 und 2, § 7 Abs. 2 und 4 G 10 sowie nach den entsprechenden landesgesetzlichen Regelungen. Hinsichtlich der Erkenntnisdaten wird, im Gegensatz zu den Daten in der Antiterrordatei, auf die die beteiligten Behörden nach § 4 Abs. 1 Satz 2 zugreifen, mit dem Antiterrordateigesetz keine neue Übermittlungsbefugnis geschaffen.

Zu § 6

Zu Absatz 1

Die datenschutzrechtliche Verantwortung für die in der Antiterrordatei 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.

Zu Absatz 2

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 eingebende Behörde. Zudem wird die eingebende Behörde verpflichtet, die Mitteilung unverzüglich zu prüfen und erforderlichenfalls die Daten zu berichtigen (vgl. § 9 Abs. 1).

Zu § 7

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 (§ 4 Abs. 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. Einzelheiten sind nach § 10 Satz 1 Nr. 6 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. Satz 4 stellt sicher, dass im Hinblick auf den Abruf eingestufter Datensätze besondere Fristen für Verschlusssachen eingehalten werden, wobei auch in diesem Falle diejenigen Daten aus den jeweiligen Protokolldatensätzen regulär nach 18 Monaten zu löschen sind, die nicht zwingend für die Einhaltung der einschlägigen Rechts- oder Verwaltungsvorschriften zum materiellen und organisatorischen Schutz von Verschlusssachen erforderlich sind.

Zu Absatz 2

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

Zu § 8

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 Abs. 1 BDSG. Daneben können die Rechtsaufsichtsbehörden und die Gerichte zur Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften die Protokolldaten nach § 7 Abs. 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 Antiterrordatei gespeicherten Daten auf § 19 BDSG. Gemäß Satz 2 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 Antiterrordatei beteiligten Behörden Rechnung. Das bedeutet, dass die Verweigerungsgründe der spezialgesetzlichen Regelungen (zum Beispiel § 15 Abs. 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 Antiterrordatei 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 § 9

Zu Absatz 1

Die Regelung begründet die Pflicht zur Berichtigung unrichtiger Daten. Die Berichtigung erfolgt nach § 6 Abs. 1 Satz 1 ausschließlich durch die Behörde, die die Daten eingegeben hat.

Zu Absatz 2

Satz 1 regelt die Pflicht zur Löschung personenbezogener Daten in der Antiterrordatei, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des internationalen Terrorismus nicht mehr erforderlich ist. Nach Satz 2 sind die in der Antiterrordatei 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 eingebende Behörde, bei der Einzelfallbearbeitung und nach den für die zugehörigen Erkenntnisdaten geltenden Fristen zu prüfen, ob personenbezogene Daten zu berichtigen oder zu löschen sind.

Zu § 10

Die Vorschrift enthält Vorgaben für den Inhalt sowie den Erlass der Errichtungsanordnung für die gemeinsame Antiterrordatei. Mit der nach Nummer 1 vorzunehmenden Festlegung der Einzelheiten zu den Bereichen des erfassten internationalen Terrorismus wird der Anwendungsbereich der Antiterrordatei konkretisiert. Festzulegen sind Einzelheiten zu der Art der zu speichernden Daten (Nummer 2), der Eingabe der zu speichernden Daten (Nummer 3) sowie den zugriffsberechtigten Organisationseinheiten der beteiligten Behörden (Nummer 4), den Einteilungen bzw. Kategorien der Zwecke und der Dringlichkeit einer Abfrage nach § 4 Abs. 3 (Nummer 5) und der Protokollierung nach § 7 Abs. 1 (Nummer 6).

Des Weiteren regelt § 10 das Verfahren zum Erlass der Errichtungsanordnung. Hierzu bedarf es zum einen des Einvernehmens der beteiligten Behörden und zum anderen der Zustimmung des Bundeskanzleramts sowie der zuständigen Ministerien. Der

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass der Errichtungsanordnung anzuhören.

**Zu Art. 2** (§ 22a BVerfSchG)

Zu Absatz 1

Die Vorschrift schafft eine Rechtsgrundlage dafür, dass das BfV für die Dauer und zur Unterstützung einer befristeten projektbezogenen Zusammenarbeit mit anderen Sicherheitsbehörden eine gemeinsame Datei (Projektdatei) einrichten kann. Die anderen Sicherheitsbehörden sind die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden der Länder, der MAD, der BND und das ZKA. Die konkrete Ausgestaltung der Projektdatei hängt davon ab, welche der genannten Sicherheitsbehörden an der jeweiligen projektbezogenen Zusammenarbeit teilnehmen. Dies können, müssen aber nicht alle in Satz 1 genannten Behörden sein.

Satz 2 enthält eine detaillierte Regelung des Dateizwecks. Voraussetzung der Errichtung einer gemeinsamen Projektdatei ist, dass sie der Unterstützung einer „projektbezogenen Zusammenarbeit“ zwischen dem BfV und den anderen beteiligten Behörden dient, in deren Rahmen Erkenntnisse im Hinblick auf die abschließend genannten Aufgabenbereiche nach § 3 Abs. 1 Nr. 1 bis 4 BVerfSchG ausgetauscht werden. Die Möglichkeiten zur Errichtung einer Projektdatei werden durch den Projektbezug begrenzt. Eine gemeinsame Projektdatei kommt nur bei einem klar definierten Projektauftrag in Betracht. Projektauftrag, Projektziele sowie die Verfahrensweisen der beteiligten Sicherheitsbehörden müssen zu Beginn des Projekts zwischen den beteiligten Behörden konkret vereinbart werden. Die Zusammenarbeit muss dem Austausch von Erkenntnissen im Hinblick auf die im Einzelnen genannten Bestrebungen und Tätigkeiten nach § 3 Abs. 1 Nr. 1 bis 4 BVerfSchG dienen. Diese müssen durch die Anwendung von Gewalt oder darauf gerichteten Vorbereitungshandlungen gekennzeichnet sein. Diese in Anlehnung an § 18 Abs. 1 BVerfSchG gewählte Formulierung stellt den inhaltlichen Bezug zum Terrorismus her.

Nach Satz 2 sind die beteiligten Behörden beim Austausch und der gemeinsamen Auswertung von Erkenntnissen an ihre jeweiligen gesetzlichen Aufgaben und Befugnisse gebunden. Mit dem Begriff der Erkenntnisse sind alle polizeilichen und nachrichtendienstlichen Erkenntnisse, einschließlich so genannter Vorfelderkenntnisse, gemeint, die im Rahmen geltender Übermittlungsvorschriften zwischen den beteiligten Behörden ausgetauscht werden können.

Die in einer Projektdatei gespeicherten personenbezogenen Daten dürfen nur durch die an der Projektarbeit beteiligten Behörden und nur im Rahmen ihrer jeweiligen Befugnisse verwendet werden (Satz 3). Die Daten aus der gemeinsamen Datei dürfen nur verwendet werden, soweit sie im Zusammenhang mit der projektbezogenen Zusammenarbeit für die Erfüllung der jeweiligen Aufgaben der Behörden erforderlich sind. Satz 4 regelt darüber hinaus, dass die für die beteiligten Behörden jeweils geltenden Vorschriften auch für die weitere Verwendung der Daten gelten. Dies gilt insbesondere für Kennzeichnungen nach § 4 Abs. 2 Artikel 10-Gesetz, die auch nach einer Übermittlung der Daten aufrechterhalten werden müssen.

Zu Absatz 2

Absatz 2 regelt die Eingabe von Daten in die Projektdatei. Danach dürfen die an der Projektarbeit beteiligten Behörden die Daten nur dann in die gemeinsame Datei eingeben, wenn sie diese Daten allen an dem Projekt beteiligten Behörden nach den geltenden Übermittlungsvorschriften übermitteln dürfen. § 22a enthält daher keine neuen Übermittlungsvorschriften zum Austausch von Daten zwischen den am Projekt beteiligten Behörden. Sollte ein Datum auch nur einer der beteiligten Behörden aus rechtlichen Gründen nicht übermittelt werden können, darf es nicht eingestellt werden. Eine Eingabe ist darüber hinaus nur zulässig, wenn die eingebende Behörde die Daten auch in eigenen Dateien speichern darf. Hiermit wird klargestellt, dass durch die Projektdatei nicht die für die jeweiligen Behörden geltenden Speicherbefugnisse ausgedehnt werden. Die eingebende Behörde hat die Daten nach Satz 3 zu kennzeichnen, so dass die eingebende Behörde – auch im Hinblick auf die datenschutzrechtliche Verantwortung – erkennbar bleibt. Bei der Kennzeichnung sind zudem die für die beteiligten Behörden geltenden Regelungen zu beachten. Dies gilt insbesondere in Bezug auf die Kennzeichnungspflicht nach § 4 Artikel 10-Gesetz.

Zu Absatz 3

Satz 1 erklärt die §§ 6 Satz 5 bis 7 und 14 Abs. 2 BVerfSchG für entsprechend anwendbar. Diese Vorschriften enthalten Regelungen über die Verantwortung des BfV für die gemeinsame Datei, zur datenschutzrechtlichen Verantwortung der eingebenden Behörde und zur Datenschutzkontrolle. Satz 2 regelt die Auskunft an Betroffene, deren personenbezogene Daten in die gemeinsame Datei eingestellt sind. Die Auskunftsregelung des § 15 BVerfSchG wird mit der Maßgabe für anwendbar erklärt, dass das BfV im Außenverhältnis gegenüber dem Auskunftssuchenden als zentrale Auskunftsstelle für die Datei auftritt, die Auskunft aber nur im Einvernehmen mit der

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 Projektdatei beteiligten Behörden Rechnung und bietet den Auskunftssuchenden gleichwohl einen zentralen Ansprechpartner.

Zu Absatz 4

Nach Satz 1 ist eine Projektdatei beim BfV ebenso wie die Projektdateien nach dem BKAG und BNDG auf höchstens zwei Jahre zu befristen. Da es sich um Dateien handelt, die der Unterstützung konkreter Projekte dienen, orientiert sich ihre Befristung an der voraussichtlichen Projektdauer und damit an der Erreichung des mit dem Projekt verfolgten Ziels. Auch hier besteht die Möglichkeit einer zweimaligen Verlängerung um jeweils bis zu einem Jahr, wenn dies weiterhin für die Erreichung des Ziels erforderlich ist. Die Gründe für die Verlängerung sind vom BfV entsprechend zu dokumentieren.

Zu Absatz 5

Absatz 5 regelt die datenschutzrechtliche Verantwortung nach dem so genannten Besitzerprinzip und legt fest, dass sich die Berichtigung, Sperrung und Löschung personenbezogener Daten nach den jeweils für die eingebende Behörde geltenden Vorschriften richtet.

Zu Absatz 6

Die Vorschrift enthält in Satz 1 die Vorgaben für die Dateianordnung der gemeinsamen Datei. Deren Festlegungen werden über die Verweisung auf die einschlägigen Bestimmungen des § 14 Abs. 1 BVerfSchG sowie über einen Katalog bestimmt. Bei den in dem Katalog aufgenommenen Regelungen handelt es sich zum Teil um Ergänzungen der in § 14 Abs. 1 Satz 1 Nr. 1 bis 7 BVerfSchG aufgenommenen Festlegungen, zum Teil aber auch um Präzisierungen bzw. Klarstellungen der dortigen Bestimmungen. Die unter Nummer 9 aufgenommene Zuständigkeit des BfV für Schadensersatzansprüche stellt klar, dass der Betroffene einen zentralen Ansprechpartner für die Geltendmachung der Ansprüche hat. Die materiellrechtliche Ausgleichspflicht richtet sich nach der datenschutzrechtlichen Verantwortung. Satz 2 regelt das Verfahren zum Erlass der Dateianordnung. Neben der notwendigen Beteiligung der Fachaufsichtsbehörden wird die Anhörung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Satz 3 festgelegt. Durch die in Satz 4 geregelte

entsprechende Anwendung von § 14 Abs. 3 Halbsatz 1 BVerfSchG wird gewährleistet, dass nur solche Personen Zugriff auf die gemeinsame Datei erhalten, die unmittelbar mit Arbeiten in dem Gebiet betraut sind, dem die gemeinsame Datei zugeordnet ist.

**Zu Art. 3** (§ 9a BNDG)

Zu Absatz 1

Die Vorschrift schafft auch für den BND eine Rechtsgrundlage dafür, dass dieser unter seiner Federführung für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit den Polizei- und Verfassungsschutzbehörden des Bundes und der Länder, dem MAD und dem ZKA eine gemeinsame Projektdatei einrichten kann. Die konkrete Ausgestaltung der Projektdatei hängt auch beim BND davon ab, welche Behörden beteiligt werden.

Satz 2 enthält ebenso wie § 22a Abs. 1 Satz 2 BVerfSchG-E und § 9a Abs. 1 Satz 2 BKAG eine detaillierte Regelung zur Begrenzung des Dateizwecks, d.h. die Errichtung einer Projektdatei ist nur zulässig, wenn sie einer konkreten „projektbezogenen Zusammenarbeit“ dient. Voraussetzung der Projektdatei beim BND ist neben der konkreten Vereinbarung von Projektauftrag, Projektzielen sowie der Verfahrensweisen zwischen den beteiligten Behörden, dass die Projektdatei dem Austausch und der gemeinsamen Auswertung von Erkenntnissen im Hinblick auf die in § 5 Abs. 1 Satz 3 Artikel 10-Gesetz genannten Gefahrenbereichen dient. Nach Satz 2 Nr. 2 sind Projektdateien zu den Gefahrenbereichen internationaler Rauschgifthandel, Geldwäsche und Geldfälschung nur zulässig, wenn deren Aufklärung Bezüge zum internationalen Terrorismus aufweist. Dadurch ist gewährleistet, dass Projektdateien in der Federführung des BND nicht zur Aufklärung der allgemeinen (organisierten) Kriminalität eingerichtet werden dürfen.

Nach Satz 3 darf die gemeinsame Datei nur im Rahmen der bestehenden gesetzlichen Befugnisse genutzt werden. Die Daten aus der gemeinsamen Datei dürfen nur verwendet werden, soweit sie im Zusammenhang mit der projektbezogenen Zusammenarbeit für die Erfüllung der jeweiligen Aufgaben der Behörden erforderlich sind. Satz 4 entspricht § 22a Abs. 1 Satz 4 BVerfSchG-E und § 9a Abs. 1 Satz 4 BKAG-E.

Zu Absatz 2

Absatz 2 entspricht § 22a Abs. 2 BVerfSchG-E und § 9a Abs. 2 BKAG-E.

Zu Absatz 3

Satz 1 bestimmt die entsprechende Anwendung von §§ 4 und 5 BNDG in Verbindung mit § 6 Satz 5 bis 7 und § 14 Abs. 2 BVerfSchG. Diese Vorschriften enthalten Regelungen über die Verantwortung des BND für die Datei, zur datenschutzrechtlichen Verantwortung der eingebenden Behörde und zur Datenschutzkontrolle. Satz 2 regelt unter Verweis auf § 7 BNDG die Auskunft an Betroffene, deren personenbezogene Daten in die gemeinsame Datei eingestellt sind. Die Regelung zur Auskunftserteilung entspricht § 22a Abs. 3 Satz 2 BVerfSchG-E und § 9a Abs. 3 Satz 2 BKAG-E.

Zu Absatz 4

Die Regelungen zur Befristung und Verlängerung entsprechen den Regelungen für Projektdateien, die beim BfV oder beim BKA geführt werden.

Zu Absatz 5

Die Regelung ist mit § 22a BVerfSchG-E und § 9a Abs. 5 BKAG-E identisch.

Zu Absatz 6

Satz 1 legt die erforderlichen Angaben für die notwendige Dateianordnung fest. Neben den Angaben nach § 6 BNDG in Verbindung mit § 14 Abs. 1 Satz 1 Nr. 1 bis 7 BVerfSchG werden in den Nummern 1 bis 9 weitere Angaben gefordert, die teils über die dortigen Angaben hinausgehen, teils die dortigen Angaben präzisieren und klarstellen. Die unter Nummer 9 aufgenommene Zuständigkeit des Bundesnachrichtendienstes für Schadensersatzansprüche stellt klar, dass Betroffene einen zentralen Ansprechpartner für die Geltendmachung ihrer potenziellen Ansprüche haben. Die materielle Ausgleichspflicht im Innenverhältnis der beteiligten Behörden richtet sich nach deren datenschutzrechtlicher Verantwortung. Die für die Dateianordnung erforderliche Zustimmung der Fachaufsichtsbehörden ist in Satz 2, die erforderliche Anhörung des Bundesbeauftragten für Datenschutz und die Informationsfreiheit in Satz 3 geregelt. Durch die in Satz 4 geregelte entsprechende Anwendung von § 14 Abs. 3 Halbsatz 1 BVerfSchG wird gewährleistet, dass nur solche Personen Zugriff auf die gemeinsame Datei erhalten, die unmittelbar mit Arbeiten in dem Gebiet betraut sind, dem die gemeinsame Datei zugeordnet ist.

**Zu Artikel 4** (§ 9a BKAG)

Zu Absatz 1

Die Vorschrift schafft die Rechtsgrundlage für die Errichtung einer gemeinsamen Projektdatei beim BKA. Der mögliche Teilnehmerkreis nach Satz 1 entspricht denen nach § 22a Abs. 1 Satz 1 BVerfSchG-E und § 9a Abs. 1 Satz 1 BNDG-E. Nach Satz 2 ist auch eine Projektdatei in der Federführung des BKA nur zulässig, wenn sie einer „projektbezogenen Zusammenarbeit“ dient und Projektauftrag, Projektziele sowie die Verfahrensweisen der beteiligten Sicherheitsbehörden zu Beginn des Projekts zwischen den beteiligten Behörden konkret vereinbart werden. Die Errichtung einer Projektdatei beim BKA setzt des Weiteren voraus, dass das Projekt auf den Austausch und die gemeinsame Auswertung von polizeilichen oder nachrichtendienstlichen Erkenntnissen zu bestimmten Straftaten gerichtet ist. Hierbei handelt es sich um die Straftaten der geheimdienstlichen Agententätigkeit (§ 99 StGB), der Bildung – auch ausländischer – terroristischer Vereinigungen (§§ 129a, 129b StGB), der Proliferation (§ 34 Abs. 1 bis 6 AWG) sowie der mit diesen Straftaten in einem unmittelbaren Zusammenhang stehenden Straftaten. Der Straftatenkatalog ist vor dem Hintergrund einer effektiven Aufklärung und Bekämpfung des internationalen Terrorismus zu sehen. Die Berücksichtigung der geheimdienstlichen Agententätigkeiten und der Proliferation ermöglicht die Auswertung wichtiger Bezüge zu Netzwerken des internationalen Terrorismus. Mit dem Begriff der polizeilichen und nachrichtendienstlichen Erkenntnisse sind alle Erkenntnisse gemeint, die im Rahmen geltender Übermittlungsvorschriften zwischen den beteiligten Behörden ausgetauscht werden können. Der Begriff umfasst insoweit auch sogenannte Vorfelderkenntnisse. Die Sätze 3 und 4 entsprechen § 22a Abs. 1 Satz 3 und 4 BVerfSchG-E sowie § 9a Abs. 1 Satz 3 und 4 BNDG-E.

Zu Absatz 2

Absatz 2 ist identisch mit § 22a Abs. 2 BVerfSchG-E und § 9a Abs. 2 BNDG-E

Zu Absatz 3

Für die Projektdatei beim BKA wird eine Reihe von Vorschriften, die bereits im BKAG enthalten sind, für anwendbar erklärt. Die in Bezug genommenen § 11 Abs. 3 und § 12 Abs. 1 bis 4 BKAG regeln die datenschutzrechtliche Verantwortung bei einer Verbunddatei. § 11 Abs. 6 BKAG betrifft die Protokollierung und ist mit der Maßgabe

anwendbar, dass diese bei jedem Datenabruf erfolgt. Die näheren Einzelheiten der Protokollierung, insbesondere die Festlegung einer systemseitigen Vollprotokollierung, d.h. einer automatisierten, beweissicheren und lückenlosen Protokollierung aller Datenbanktransaktionen auf der Grundlage von Auswerteprogrammen, bleiben der Errichtungsanordnung vorbehalten (vgl. § 9a Abs. 6 i.V.m. § 34 Abs. 1 Nr. 9 BKAG). Die Auskunftsregelung des § 12 Abs. 5 BKAG wird entsprechend §22a Abs. 3 Satz 2 BVerfSchG-E und §9a Abs. 3 Satz 2 BNDG-E mit der Maßgabe für anwendbar erklärt, dass das BKA im Außenverhältnis gegenüber dem Auskunftssuchenden als zentrale Auskunftsstelle für die Datei auftritt, die Auskunft aber nur im Einvernehmen mit der Behörde erteilt, die die datenschutzrechtliche Verantwortung für das betreffende Datum trägt.

Zu Absatz 4 und 5

Die Regelungen entsprechen § 22a Abs. 4 und 5 BVerfSchG-E sowie § 9a Abs. 4 und 5 BNDG-E.

Zu Absatz 6

Die Vorschrift enthält wesentliche Vorgaben für die Errichtungsanordnung. Neben den entsprechend § 34 Abs. 1 Satz 1 Nr. 1 bis 9 BKAG zu treffenden inhaltlichen Festlegungen sind in der Errichtungsanordnung die an der Projektarbeit teilnehmenden Organisationseinheiten der jeweiligen Behörden zu bestimmen. Des Weiteren regelt Absatz 6 das Verfahren zum Erlass der Errichtungsanordnung.

**Zu Art. 5** (Inkrafttreten)

*[Das Antiterrordateigesetz (Artikel 1) tritt an dem genannten Inkrafttretenstermin in Kraft. Der spätere Zeitpunkt des Inkrafttretens trägt dem Umstand Rechnung, dass die Errichtung der Antiterrordatei einerseits von keiner (behördlichen) Entscheidung abhängig ist, das Antiterrordateigesetz jedoch andererseits in § 2 Abs. 1 eine Pflicht der beteiligten Behörden zur Speicherung von Daten in der Antiterrordatei enthält. Dieser Pflicht kann erst entsprochen werden, wenn die notwendigen technischen und organisatorischen Voraussetzungen für die Errichtung der Datei geschaffen worden sind. Die Änderungen des BVerfSchG, des BNDG und des BKAG treten am Tage nach der Verkündung in Kraft.]*