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

ATDG

Ausfertigungsdatum: 22.12.2006

Vollzitat:

"Antiterrordateigesetz vom 22. Dezember 2006 (BGBl. I S. 3409), das zuletzt durch Artikel 22 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist"

**Stand:** Zuletzt geändert Art. 22 V v. 19.6.2020 I 1328

Das G tritt gem. Art. 5 Abs. 2 G v. 22.12.2006 I 3409 mit Ablauf des 30.12.2017 außer Kraft, Art. 5 Abs. 2 aufgeh. durch Art. 4 Satz 3 G v. 18.12.2014 I 2318 mWv 1.1.2015; dadurch ist die Geltung des G über den 30.12.2017 hinaus verlängert worden

**Fußnote**

(+++ Textnachweis ab: 31.12.2006 +++)

Das G wurde als Artikel 1 des G v. 22.12.2006 I 3409 vom Bundestag erlassen. Es tritt gem. Art. 5 Abs. 2 dieses G mit Ablauf des 30. Dezember 2017 außer Kraft und ist fünf Jahre nach dem Inkrafttreten unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren. Art. 5 Abs. 2 G v. 22.12.2006 I 3409 aufgeh. durch Art. 4 Satz 3 G v. 18.12.2014 I 2318 mWv 1.1.2015, dadurch ist die Geltung des G über den 30.12.2017 hinaus verlängert worden.

## § 1 Antiterrordatei

(1) Das Bundeskriminalamt, die in der Rechtsverordnung nach § 58 Abs. 1 des Bundespolizeigesetzes bestimmte Bundespolizeibehörde, 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) Der Bundesminister des Innern, für Bau und Heimat kann, bei Landesbehörden auf Ersuchen des jeweils zuständigen Landes, durch Rechtsverordnung weitere Polizeivollzugsbehörden als beteiligte Behörden zur Teilnahme an der Antiterrordatei berechtigen, soweit

1. diesen Aufgaben zur Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland nicht nur im Einzelfall besonders zugewiesen sind und
2. ihr Zugriff auf die Antiterrordatei für die Wahrnehmung der Aufgaben nach Nummer 1 erforderlich und dies unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Sicherheitsinteressen der beteiligten Behörden angemessen ist.

## § 2 Inhalt der Antiterrordatei und Speicherungspflicht

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

1. Personen, die
   a) einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, die einen internationalen Bezug aufweist, oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Absatz 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland angehören oder diese unterstützen,

b) einer Gruppierung, die eine Vereinigung nach Buchstabe a unterstützt, angehören oder

c) eine Gruppierung nach Buchstabe b willentlich in Kenntnis der den Terrorismus unterstützenden Aktivität der Gruppierung unterstützen,

2. Personen, die rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten oder durch ihre Tätigkeiten, insbesondere durch Befürworten solcher Gewaltanwendungen, vorsätzlich hervorrufen, oder

3. a) Vereinigungen, Gruppierungen, Stiftungen oder Unternehmen,

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

bei denen tatsächliche Anhaltspunkte die Annahme begründen, dass sie im Zusammenhang mit einer Person nach Nummer 1 oder Nummer 2 stehen und durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können,

und die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland erforderlich ist. Satz 1 gilt nur für Daten, die die beteiligten Behörden nach den für sie geltenden Rechtsvorschriften automatisiert verarbeiten dürfen.

**§ 3 Zu speichernde Datenarten**

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

1. zu Personen nach § 2 Satz 1 Nummer 1 und 2

a) der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder, die Bezeichnung der Fallgruppe nach § 2 und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),

b) folgende weitere Datenarten (erweiterte Grunddaten):

aa) eigene oder von ihnen genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte,

bb) Adressen für elektronische Post,

cc) Bankverbindungen,

dd) Schließfächer,

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

ff) Familienstand,

gg) Volkszugehörigkeit,

hh) Angaben zur Religionszugehörigkeit, soweit diese im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind,

ii) besondere Fähigkeiten, die nach den auf bestimmten Tatsachen beruhenden Erkenntnissen der beteiligten Behörden der Vorbereitung und Durchführung terroristischer Straftaten nach § 129a Abs. 1 und 2 des Strafgesetzbuchs dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,

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

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

ll) Angaben zur Gefährlichkeit, insbesondere Waffenbesitz oder zur Gewaltbereitschaft der Person,

mm) Fahr- und Flugerlaubnisse,

nn) besuchte Orte oder Gebiete, an oder in denen sich in § 2 Satz 1 Nr. 1 und 2 genannte Personen treffen,

oo) Kontaktpersonen zu den jeweiligen Personen nach § 2 Satz 1 Nr. 1 Buchstabe a oder Nr. 2,

pp) die Bezeichnung der konkreten Vereinigung oder Gruppierung nach § 2 Satz 1 Nr. 1 Buchstabe a oder b,

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

rr) auf tatsächlichen Anhaltspunkten beruhende zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen zu Grunddaten und erweiterten Grunddaten, die bereits in Dateisystemen der beteiligten Behörden gespeichert sind, sofern dies im Einzelfall nach pflichtgemäßem Ermessen geboten und zur Aufklärung oder Bekämpfung des internationalen Terrorismus unerlässlich ist, und

ss) von der Person betriebene oder maßgeblich zum Zweck ihrer Aktivitäten nach § 2 Satz 1 Nummer 1 oder Nummer 2 genutzte Internetseiten,

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

(2) Kontaktpersonen nach Absatz 1 Nummer 1 Buchstabe b Doppelbuchstabe oo sind Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in § 2 Satz 1 Nummer 1 Buchstabe a oder Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind. Angaben zu Kontaktpersonen dürfen ausschließlich als erweiterte Grunddaten nach Absatz 1 Nummer 1 Buchstabe b Doppelbuchstabe oo mit folgenden Datenarten zur Identifizierung und Kontaktaufnahme gespeichert werden: der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, die aktuelle Staatsangehörigkeit, die gegenwärtige Anschrift, Lichtbilder, eigene oder von ihnen genutzte Telekommunikationsanschlüsse sowie Adressen für elektronische Post, sonstige Angaben zur beruflichen Erreichbarkeit.

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

(4) Das Bundeskriminalamt legt die Kriterien und Kategorien für die zu speichernden Datenarten in den Fällen des Absatzes 1 Nummer 1 Buchstabe b Doppelbuchstabe gg, hh, ii, kk und nn in einer Verwaltungsvorschrift fest. Diese ist in der jeweils aktuellen Fassung im Bundesanzeiger zu veröffentlichen. Das Bundeskriminalamt kann Kriterien für die zu speichernden Datenarten in den weiteren Fällen des Absatzes 1 in derselben Verwaltungsvorschrift vorsehen.

**§ 4 Beschränkte und verdeckte Speicherung**

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

(2) Sind Daten, auf die sich eine Abfrage bezieht, verdeckt gespeichert, wird die Behörde, die die Daten eingegeben hat, automatisiert durch Übermittlung aller Anfragedaten über die Abfrage unterrichtet und hat unverzüglich mit der abfragenden Behörde Kontakt aufzunehmen, um zu klären, ob Erkenntnisse nach § 7 übermittelt werden können. Die Behörde, die die Daten eingegeben hat, sieht von einer Kontaktaufnahme nur ab, wenn Geheimhaltungsinteressen auch nach den 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.

(3) Personenbezogene Daten, die durch

1. Maßnahmen nach § 100a der Strafprozessordnung oder § 51 des Bundeskriminalamtgesetzes,
2. Maßnahmen nach den §§ 100b und 100c der Strafprozessordnung oder § 46 des Bundeskriminalamtgesetzes,
3. Maßnahmen nach § 99 der Strafprozessordnung,
4. Maßnahmen nach § 49 des Bundeskriminalamtgesetzes,
5. Maßnahmen innerhalb von Wohnungen nach § 34 des Bundeskriminalamtgesetzes,
6. Beschränkungen nach § 1 Absatz 1 des Artikel 10-Gesetzes,
7. Maßnahmen nach § 9 Absatz 2 des Bundesverfassungsschutzgesetzes,
8. Maßnahmen nach § 22a oder § 32a des Zollfahndungsdienstgesetzes,
9. Maßnahmen nach § 23a des Zollfahndungsdienstgesetzes oder

durch Maßnahmen nach entsprechenden landesrechtlichen Regelungen erlangt wurden, sind verdeckt zu speichern. Sofern zu einer Person nach § 2 Satz 1 Nummer 1 und 2 oder einer Angabe nach § 2 Satz 1 Nummer 3 sowohl Daten nach Satz 1 als auch andere Daten zu speichern sind, müssen nur die Daten nach Satz 1 verdeckt gespeichert werden oder kann die einstellende Behörde von der Speicherung der Daten nach Satz 1 absehen (beschränkte Speicherung).

**§ 5 Zugriff auf die Daten**

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

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

Auf die zu Personen gespeicherten erweiterten Grunddaten kann die abfragende Behörde im Falle eines Treffers Zugriff erhalten, wenn die Behörde, die die Daten eingegeben hat, dies im Einzelfall auf Ersuchen gewährt. Die Entscheidung hierüber richtet sich nach den jeweils geltenden Übermittlungsvorschriften. Wenn die abfragende Behörde ohne Angabe eines Namens nach § 3 Absatz 1 Nummer 1 Buchstabe a mittels Angaben in den erweiterten Grunddaten sucht, erhält sie im Falle eines Treffers lediglich Zugriff auf die Daten nach § 3 Absatz 1 Nummer 3. Satz 5 gilt entsprechend, wenn die Suche trotz Angabe eines Namens mehrere Treffer erzeugt.

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

oder nach § 11 Abs. 3 in ihrer Verarbeitung einzuschränken. Sind die Daten einem Dritten übermittelt worden, ist dieser unverzüglich darauf hinzuweisen, dass die weitere Verwendung der Daten unzulässig ist.

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

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

**§ 6 Weitere Verwendung der Daten**

(1) Die abfragende Behörde darf die Daten, auf die sie Zugriff erhalten hat, nur zur Prüfung, ob der Treffer der gesuchten Person oder der gesuchten Angabe nach § 2 Satz 1 Nummer 3 zuzuordnen ist, für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus und zu den Zwecken nach § 6a verwenden. Eine Verwendung zu einem anderen Zweck als zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus ist nur zulässig, soweit

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

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

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

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

**§ 6a Erweiterte projektbezogene Datennutzung**

(1) Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts zur Sammlung und Auswertung von Informationen über eine internationale terroristische Bestrebung, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass Straftaten des internationalen Terrorismus nach den §§ 129a, 129b und 211 des Strafgesetzbuchs begangen werden sollen und dadurch Gefahren für Leib, Leben oder Freiheit von Personen drohen, im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären.

(2) Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts für die Verfolgung qualifizierter Straftaten des internationalen Terrorismus im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären. Qualifizierte Straftaten des internationalen Terrorismus sind Taten des internationalen Terrorismus, die einen Straftatbestand nach den §§ 89a, 89b, 91, 102, 129a, 129b, 211 oder 212 des Strafgesetzbuchs erfüllen.

(3) Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts für die Verhinderung von qualifizierten Straftaten des internationalen Terrorismus erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären, und Tatsachen die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll. Absatz 2 Satz 2 gilt entsprechend.

(4) Ein Projekt ist eine gegenständlich abgrenzbare und auf bestimmte Zeiträume bezogene Aufgabe, der durch die Gefahr oder den drohenden Schaden, die am Sachverhalt beteiligten Personen, die Zielsetzung der Aufgabe oder deren Folgewirkungen eine besondere Bedeutung zukommt.

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

1. phonetischer oder unvollständiger Daten,
2. der Suche über eine Mehrzahl von Datenfeldern,
3. der Verknüpfung von Personen, Institutionen, Organisationen, Sachen oder
4. der zeitlichen Eingrenzung der Suchkriterien

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

(6) Die Zugriffsberechtigung ist im Rahmen der projektbezogenen erweiterten Nutzung auf die Personen zu beschränken, die unmittelbar mit Arbeiten auf diesem Anwendungsgebiet betraut sind. Die projektbezogene erweiterte Nutzung der Datei ist auf höchstens zwei Jahre zu befristen. Die Frist kann zweimalig um jeweils bis zu einem Jahr verlängert werden, wenn die Voraussetzungen für die projektbezogene erweiterte Datennutzung fortbestehen und sich aus den mit dem Projekt gewonnenen Erkenntnissen das Bedürfnis für eine Fortführung des Projekts ergibt.

(7) Projektbezogene Datennutzungen dürfen nur auf Antrag angeordnet werden. Der Antrag ist durch den Behördenleiter oder seinen Stellvertreter schriftlich zu stellen und zu begründen. Er muss alle für die Anordnung erforderlichen Angaben enthalten. Zuständig für die Anordnung ist die die Fachaufsicht über die antragstellende Behörde führende oberste Bundesbehörde. Die Anordnung ergeht schriftlich. In ihr sind der Grund der Anordnung, die für die projektbezogene erweiterte Datennutzung erforderlichen Datenarten nach § 3, der Funktionsumfang und die Dauer der projektbezogenen erweiterten Datennutzung anzugeben. Der Funktionsumfang der projektbezogenen erweiterten Datennutzung ist auf das zur Erreichung des Projektziels erforderliche Maß zu beschränken. Die Anordnung ist zu begründen. Aus der Begründung müssen sich die in den Absätzen 1 bis 3 genannten Voraussetzungen ergeben, insbesondere, dass die projektbezogene erweiterte Nutzung erforderlich ist, um weitere Zusammenhänge aufzuklären. Die anordnende Behörde hält Antrag und Anordnung für datenschutzrechtliche Kontrollzwecke zwei Jahre, mindestens jedoch für die Dauer der projektbezogenen erweiterten Nutzung vor.

(8) Eine nach Absatz 7 angeordnete erweiterte Nutzung darf nur mit Zustimmung der G 10-Kommission (§ 15 Absatz 1 bis 4 des Artikel 10-Gesetzes) vollzogen werden. Bei Gefahr im Verzug kann die nach Absatz 7 Satz 4 zuständige Behörde den Vollzug auch bereits vor der Zustimmung der Kommission anordnen. Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt, hat die nach Absatz 7 Satz 4 zuständige Behörde unverzüglich aufzuheben. Die aus der erweiterten Datennutzung gewonnenen Daten und Erkenntnisse unterliegen in diesem Fall einem absoluten Verwendungsverbot und sind unverzüglich zu löschen.

(9) Für Verlängerungen nach Absatz 6 Satz 3 gelten die Absätze 7 und 8 entsprechend.

(10) Die alleinige datenschutzrechtliche Verantwortung für die Durchführung des Projekts trägt die antragstellende Behörde. Die Übermittlung von aus einem Projekt gewonnenen Erkenntnissen richtet sich nach den allgemeinen Übermittlungsvorschriften. § 6 Absatz 4 Satz 1 gilt für aus einem Projekt nach Absatz 1 gewonnene Erkenntnisse entsprechend.

(11) Die nach § 1 Absatz 1 berechtigten Landesbehörden sind nach Maßgabe landesrechtlicher Regelungen, die den Vorgaben der Absätze 1 bis 10 entsprechen, befugt, die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten zu den in den Absätzen 1 bis 3 genannten Zwecken erweitert zu nutzen. Satz 1 gilt auch für Landesbehörden, die durch eine Rechtsverordnung nach § 1 Absatz 2 zur Teilnahme an der Datei berechtigt werden.

**§ 7 Übermittlung von Erkenntnissen**

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

**§ 8 Datenschutzrechtliche Verantwortung**

(1) Die datenschutzrechtliche Verantwortung für die in der Antiterrordatei gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten trägt die Behörde, die die Daten eingegeben hat. Die Behörde, die die Daten eingegeben hat, muss erkennbar sein. Die Verantwortung für die Zulässigkeit der Abfrage trägt die abfragende Behörde.

(2) Nur die Behörde, die die Daten eingegeben hat, darf diese Daten ändern, berichtigen, in ihrer Verarbeitung einschränken oder löschen.

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

**§ 9 Protokollierung, technische und organisatorische Maßnahmen**

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

(2) Das Bundeskriminalamt hat die nach § 64 des Bundesdatenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen zu treffen.

(3) Das Bundeskriminalamt berichtet dem Deutschen Bundestag alle drei Jahre, erstmalig zum 1. August 2017, über den Datenbestand und die Nutzung der Antiterrordatei. Der Bericht ist zeitgleich mit der Zuleitung an den Deutschen Bundestag über den Internetauftritt des Bundeskriminalamts zu veröffentlichen.

**§ 10 Datenschutzrechtliche Kontrolle, Auskunft an den Betroffenen**

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 9 Absatz 1 des Bundesdatenschutzgesetzes der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die von den Ländern in die Antiterrordatei eingegebenen Datensätze können auch von den jeweiligen Landesbeauftragten für den Datenschutz im Zusammenhang mit der Wahrnehmung ihrer Prüfungsaufgaben in den Ländern kontrolliert werden, soweit die Länder nach § 8 Absatz 1 verantwortlich sind. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit arbeitet insoweit mit den Landesbeauftragten für den Datenschutz zusammen.

(2) Die in Absatz 1 genannten Stellen sind im Rahmen ihrer jeweiligen Zuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes zu kontrollieren.

(3) Über die nicht verdeckt gespeicherten Daten erteilt das Bundeskriminalamt die Auskunft nach § 57 des Bundesdatenschutzgesetzes im Einvernehmen mit der Behörde, die die datenschutzrechtliche Verantwortung nach § 8 Abs. 1 Satz 1 trägt und die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Rechtsvorschriften prüft. Die Auskunft zu verdeckt gespeicherten Daten richtet sich nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften.

**§ 11 Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten**

(1) Unrichtige Daten sind zu berichtigen.

(2) Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des internationalen Terrorismus nicht mehr erforderlich ist. Sie sind spätestens zu löschen, wenn die zugehörigen Erkenntnisse nach den für die beteiligten Behörden jeweils geltenden Rechtsvorschriften zu löschen sind.

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

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

### § 12 Festlegungen für die gemeinsame Datei

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

1. den Bereichen des erfassten internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland,
2. den weiteren beteiligten Polizeivollzugsbehörden nach § 1 Abs. 2,
3. der Art der zu speichernden Daten nach § 3 Abs. 1,
4. der Eingabe der zu speichernden Daten,
5. den zugriffsberechtigten Organisationseinheiten der beteiligten Behörden,
6. den Einteilungen der Zwecke und der Dringlichkeit einer Abfrage und
7. der Protokollierung.

Die Festlegungen bedürfen der Zustimmung des Bundesministeriums des Innern, für Bau und Heimat, des Bundeskanzleramts, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen und der für die beteiligten Behörden der Länder zuständigen obersten Landesbehörden. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor den Festlegungen anzuhören.

### § 13 Einschränkung von Grundrechten

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