

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes

zu dem Abkommen vom 1. Oktober 2008

zwischen der Regierung der Bundesrepublik Deutschland

und der Regierung der Vereinigten Staaten von Amerika

über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität

A. Problem und Ziel

Die Regierung der Bundesrepublik Deutschland hat mit der Regierung der Vereinigten Staaten von Amerika ein Abkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität unterzeichnet. Ziel des Abkommens ist es, die Zusammenarbeit bei der Bekämpfung schwerwiegender Kriminalität, insbesondere des internationalen Terrorismus, zu verbessern und dadurch die Innere Sicherheit in den Vertragsstaaten zu erhöhen.

B. Lösung

Durch den vorliegenden Gesetzentwurf sollen die Voraussetzungen nach Artikel 59 Absatz 2 Satz 1 des Grundgesetzes für das Inkrafttreten des Abkommens geschaffen werden.

C. Alternativen

Keine

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugaufwand

Keine

2. Vollzugaufwand

Für die Wahrnehmung der neuen Aufgaben werden beim Bundeskriminalamt Kosten insbesondere für die technische Realisierung, Pflege und laufende Unterhaltung des automatisierten DNA- und Fingerabdruckdatenaustauschs anfallen. Die Kosten werden entscheidend von den tatsächlich auszutauschenden Datenmengen abhängen. Außerdem wird sich ein erhöhter Personalaufwand ergeben, der derzeit noch nicht abschätzbar ist.

Für die Schaffung der Voraussetzungen der Wirkbetriebsaufnahme des automatisierten DNA- und Fingerabdruckdatenaustauschs entstehen voraussichtlich einmalige Investitionskosten in Höhe von ca. 2,5 Millionen Euro. Die Kosten für den laufenden Unterhalt, insbesondere der personelle Mehrbedarf für die Trefferverifizierung und die Bearbeitung des Nachfolgeschriftverkehrs, hängen entscheidend von der Anzahl der erzielten Treffer ab.

Die Bundesregierung wird berücksichtigen, dass sich der finanzielle Umsetzungs- und Verwaltungsaufwand auf das unbedingt notwendige Maß beschränken soll und erforderliche Sachmittelbedarfe im Rahmen der jeweils betroffenen Einzelpläne grundsätzlich erwirtschaftet werden müssen.

E. Sonstige Kosten

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

F. Bürokratiekosten

Für die Wirtschaft und die Bürgerinnen und Bürger werden keine Informationspflichten neu eingeführt. Der Gesetzentwurf enthält sieben neue Informationspflichten für die Verwaltung.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 25. Mai 2009

An den
Präsidenten des
Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

Entwurf eines Gesetzes zu dem Abkommen vom 1. Oktober 2008 zwischen
der Regierung der Bundesrepublik Deutschland und der Regierung der
Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit
bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Abs. 1 NKRG
ist als Anlage 2 beigefügt.

Der Bundesrat hat in seiner 858. Sitzung am 15. Mai 2009 gemäß Artikel 76
Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus
Anlage 3 ersichtlich Stellung zu nehmen.

Die Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates
wird nachgereicht.

Mit freundlichen Grüßen



Entwurf

**Gesetz
zu dem Abkommen vom 1. Oktober 2008
zwischen der Regierung der Bundesrepublik Deutschland
und der Regierung der Vereinigten Staaten von Amerika
über die Vertiefung der Zusammenarbeit bei der Verhinderung
und Bekämpfung schwerwiegender Kriminalität**

Vom

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Dem in Washington D.C. am 1. Oktober 2008 unterzeichneten Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität wird zugestimmt. Das Abkommen wird nachstehend veröffentlicht.

Artikel 2

- (1) Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.
- (2) Der Tag, an dem das Abkommen nach seinem Artikel 24 in Kraft tritt, ist im Bundesgesetzblatt bekannt zu geben.

Begründung zum Vertragsgesetz

Zu Artikel 1

Auf das Abkommen findet Artikel 59 Absatz 2 Satz 1 des Grundgesetzes Anwendung, da es sich auf Gegenstände der Bundesgesetzgebung bezieht.

Zu Artikel 2

Die Bestimmung des Absatzes 1 entspricht dem Erfordernis des Artikels 82 Absatz 2 Satz 1 des Grundgesetzes.

Nach Absatz 2 ist der Zeitpunkt, in dem das Abkommen nach seinem Artikel 24 in Kraft tritt, im Bundesgesetzblatt bekannt zu geben.

Schlussbemerkung

Auswirkungen auf die Einzelpreise oder das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten, da Kosten für die private Wirtschaft und private Verbraucher nicht entstehen.

Für die Verwaltung werden sieben neue Informationspflichten eingeführt:

- Artikel 6 Absatz 1: Benennung einer nationalen Kontaktstelle für die Durchführung des automatisierten Abrufs daktyloskopischer Daten,
- Artikel 9 Absatz 1: Benennung einer nationalen Kontaktstelle für die Durchführung des automatisierten Abrufs von DNA-Identifizierungsmustern,
- Artikel 10 Absatz 7: Benennung einer nationalen Kontaktstelle für den Datenaustausch zur Verhinderung terroristischer Straftaten,
- Artikel 14 Absatz 3: Mitteilung, falls sich nach dem Abkommen übermittelte oder empfangene Daten als unrichtig oder nicht verlässlich herausstellen,
- Artikel 15 Absatz 1: Protokollierung der nach diesem Abkommen übermittelten oder empfangenen Daten,
- Artikel 15 Absatz 3: Aufbewahrung der Protokolldaten über einen Zeitraum von zwei Jahren,
- Artikel 18: Unterrichtung (auf Anfrage) über die Verarbeitung der nach diesem Abkommen empfangenen Daten und das dadurch erzielte Ergebnis.

Durch die Erfüllung dieser Pflichten entstehen für die Verwaltung Bürokratiekosten.

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar.

Abkommen
zwischen der Regierung der Bundesrepublik Deutschland
und der Regierung der Vereinigten Staaten von Amerika
über die Vertiefung der Zusammenarbeit
bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität

Agreement
between the Government of the Federal Republic of Germany
and the Government of the United States of America
on enhancing cooperation
in preventing and combating serious crime

Die Regierung der Bundesrepublik Deutschland
und

die Regierung der Vereinigten Staaten von Amerika
(im Folgenden die „Vertragsparteien“)

in dem Bestreben, durch partnerschaftliche Zusammenarbeit schwerwiegende Kriminalität, insbesondere den Terrorismus, wirksamer zu bekämpfen,

in dem Bewusstsein, dass der Austausch von Informationen ein wesentlicher Faktor bei der Bekämpfung schwerwiegender Kriminalität, insbesondere des Terrorismus, ist,

in Anerkennung der Bedeutung der Verhütung und Bekämpfung schwerwiegender Kriminalität, insbesondere des Terrorismus, bei gleichzeitiger Achtung der Grundrechte und -freiheiten, insbesondere des Schutzes der Privatsphäre,

dem Beispiel des Vertrags von Prüm vom 27. Mai 2005 über die Vertiefung der grenzüberschreitenden Zusammenarbeit folgend,

in der Erwartung, dass die Vereinigten Staaten von Amerika und andere Mitgliedstaaten der Europäischen Union dieses Abkommen als Beispiel für vergleichbare Abkommen zwischen den Vereinigten Staaten von Amerika und diesen anderen Mitgliedstaaten ansehen könnten, und

in dem Bestreben, die Zusammenarbeit zwischen den Vertragsparteien im Geist der transatlantischen Partnerschaft zu vertiefen und zu stimulieren –

sind wie folgt übereingekommen:

Artikel 1

Begriffsbestimmungen

Für die Zwecke dieses Abkommens bedeuten

1. „DNA-Profil“ (für die Bundesrepublik Deutschland DNA-Identifizierungsmuster) einen Buchstaben- beziehungsweise Zahlencode, der eine Reihe von Identifizierungsmerkmalen des nicht codierenden Teils einer analysierten menschlichen DNA-Probe, das heißt der speziellen chemischen Form an den verschiedenen DNA-Loci, abbildet;
2. „Fundstellendatensätze“ ein DNA-Profil und die damit verbundene Kennung (DNA-Fundstellendatensatz) oder daktyloskopische Daten und die damit verbundene Kennung

The Government of the Federal Republic of Germany
and the

Government of the United States of America
(hereinafter the “Parties”)

Prompted by the desire to cooperate as partners to combat serious crime, particularly terrorism, more effectively,

Recognising that information sharing is an essential component in the fight against serious crime, particularly terrorism,

Recognising the importance of preventing and combating serious crime, particularly terrorism, while respecting fundamental rights and freedoms, notably privacy,

Following the example of the Treaty of Prüm of May 27, 2005 on enhancing cross-border cooperation,

Expecting that the United States of America and other Member States of the European Union may consider this Agreement as a model for similar agreements between the United States of America and those other Member States, and

Seeking to enhance and encourage cooperation between the Parties in the spirit of transatlantic partnership,

Have agreed as follows:

Article 1

Definitions

For the purposes of this Agreement,

1. “DNA profiles” (for the Federal Republic of Germany, “DNA-Identifizierungsmuster” (DNA identification patterns)) shall mean a letter or numerical code representing a number of identifying features of the non-coding part of an analysed human DNA sample, i.e. of the specific chemical form at the various DNA loci;
2. “Reference data” shall mean a DNA profile and the related reference (DNA reference data) or fingerprinting data and the related reference (fingerprinting reference data). Reference

(daktyloskopischer Fundstellendatensatz). Fundstellendatensätze dürfen keine den Betroffenen unmittelbar identifizierenden Daten enthalten. Fundstellendatensätze, die keiner Person zugeordnet werden können (offene Spuren), müssen als solche erkennbar sein;

3. „Personenbezogene Daten“ Informationen über eine bestimmte oder bestimmbare natürliche Person („Betroffener“) und
4. „Verarbeitung personenbezogener Daten“ jede Verarbeitung oder jede Vorgangsreihe von Verarbeitungen im Zusammenhang mit personenbezogenen Daten mit oder ohne Hilfe automatisierter Verfahren, wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, das Konsultieren, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen durch Unkenntlichmachen oder Vernichten von personenbezogenen Daten.

Artikel 2

Zweck dieses Abkommens

Zweck dieses Abkommens ist die Vertiefung der Zusammenarbeit zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika bei der Bekämpfung und Verhinderung schwerwiegender Kriminalität.

Artikel 3

Daktyloskopische Daten

Zur Durchführung dieses Abkommens gewährleisten die Vertragsparteien, dass Fundstellendatensätze zu dem Bestand der zum Zweck der Verhinderung und Verfolgung von Straftaten errichteten nationalen automatisierten daktyloskopischen Identifizierungssysteme vorhanden sind. Fundstellendatensätze enthalten ausschließlich daktyloskopische Daten und eine Kennung.

Artikel 4

Automatisierter Abruf daktyloskopischer Daten

(1) Zur Verhinderung und Verfolgung schwerwiegender Kriminalität gestatten die Vertragsparteien den in Artikel 6 bezeichneten nationalen Kontaktstellen der anderen Vertragspartei, auf die Fundstellendatensätze ihrer zu diesen Zwecken eingerichteten automatisierten daktyloskopischen Identifizierungssysteme mit dem Recht zuzugreifen, diese automatisiert mittels eines Vergleichs der daktyloskopischen Daten abzurufen. Die Anfrage darf nur im Einzelfall und nach Maßgabe des innerstaatlichen Rechts der abrufenden Vertragspartei erfolgen.

(2) Die endgültige Zuordnung eines daktyloskopischen Datensatzes zu einem Fundstellendatensatz der die Datei führenden Vertragspartei erfolgt durch die abrufenden nationalen Kontaktstellen anhand der automatisiert übermittelten Fundstellendatensätze, die für die eindeutige Zuordnung erforderlich sind.

Artikel 5

Übermittlung weiterer personenbezogener und sonstiger Daten

Im Fall der Feststellung einer Übereinstimmung von daktyloskopischen Daten im Verfahren nach Artikel 4 richtet sich die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener und sonstiger Daten nach dem innerstaatlichen Recht einschließlich der Vorschriften über die Rechtshilfe der ersuchten Vertragspartei.

data must not contain any data from which the data subject can be directly identified. Reference data not traceable to any individual (untraceables) must be recognisable as such;

3. “Personal data” shall mean any information relating to an identified or identifiable natural person (the “data subject”); and
4. “Processing of personal data” shall mean any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, combination or alignment, blocking, or deletion through erasure or destruction of personal data.

Article 2

Purpose of this Agreement

The purpose of this Agreement is to enhance the cooperation between the United States of America and the Federal Republic of Germany in combating and preventing serious crime.

Article 3

Fingerprinting data

For the purpose of implementing this Agreement, the Parties shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offenses. Reference data shall only include fingerprinting data and a reference.

Article 4

Automated searching of fingerprint data

(1) For the prevention and investigation of serious crime, each Party shall allow the other Party’s national contact points, as referred to in Article 6, access to the reference data in the automated fingerprint identification systems which it has established for that purpose, with the power to conduct automated searches by comparing fingerprinting data. Search powers may be exercised only in individual cases and in compliance with the searching Party’s national law.

(2) Firm matching of fingerprinting data with reference data held by the Party in charge of the file shall be carried out by the searching national contact points by means of the automated supply of the reference data required for a clear match.

Article 5

Supply of further personal and other data

Should the procedure referred to in Article 4 show a match between fingerprinting data, the supply of any available further personal data and other data relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Party.

Artikel 6**Nationale Kontaktstellen
und Durchführungsvereinbarungen**

(1) Zur Durchführung der Datenübermittlungen nach Artikel 4 benennt jede Vertragspartei eine oder mehrere nationale Kontaktstellen. Die Befugnisse der nationalen Kontaktstellen richten sich nach dem für sie geltenden innerstaatlichen Recht.

(2) Die Einzelheiten der technischen Ausgestaltung und des Ablaufs eines nach Artikel 4 durchgeführten Abrufverfahrens werden in einer oder mehreren Durchführungsvereinbarungen geregelt.

Artikel 7**Automatisierter Abruf von DNA-Profilen**

(1) Soweit dies nach dem innerstaatlichen Recht beider Vertragsparteien zulässig ist und auf der Basis der Gegenseitigkeit können die Vertragsparteien der in Artikel 9 bezeichneten nationalen Kontaktstelle der anderen Vertragspartei zum Zweck der Verfolgung schwerwiegender Kriminalität den Zugriff auf die Fundstellendatensätze ihrer DNA-Analyse-Dateien mit dem Recht gestatten, diese automatisiert mittels eines Vergleichs der DNA-Profile abzurufen. Die Anfrage darf nur im Einzelfall und nach Maßgabe des innerstaatlichen Rechts der abrufenden Vertragspartei erfolgen.

(2) Wird im Zuge eines automatisierten Abrufs die Übereinstimmung eines übermittelten DNA-Profiles mit einem in der Datei der empfangenden Vertragspartei gespeicherten DNA-Profil festgestellt, so erhält die anfragende nationale Kontaktstelle automatisiert die Fundstellendatensätze, hinsichtlich derer eine Übereinstimmung festgestellt worden ist. Kann keine Übereinstimmung festgestellt werden, so wird dies automatisiert mitgeteilt.

Artikel 8**Übermittlung weiterer
personenbezogener und sonstiger Daten**

Im Fall der Feststellung einer Übereinstimmung von DNA-Profilen im Verfahren nach Artikel 7 richtet sich die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener und sonstiger Daten nach dem innerstaatlichen Recht einschließlich der Vorschriften über die Rechtshilfe der ersuchten Vertragspartei.

Artikel 9**Nationale Kontaktstelle
und Durchführungsvereinbarungen**

(1) Zur Durchführung der Datenübermittlungen nach Artikel 7 benennt jede Vertragspartei eine nationale Kontaktstelle. Die Befugnisse der nationalen Kontaktstelle richten sich nach dem für sie geltenden innerstaatlichen Recht.

(2) Die Einzelheiten der technischen Ausgestaltung und des Ablaufs eines nach Artikel 7 durchgeführten Abrufverfahrens werden in einer oder mehreren Durchführungsvereinbarungen geregelt.

Artikel 10**Übermittlung
personenbezogener und anderer Daten
zur Verhinderung terroristischer Straftaten**

(1) Die Vertragsparteien können zum Zweck der Verhinderung terroristischer Straftaten der betreffenden in Absatz 7 bezeichneten nationalen Kontaktstelle der anderen Vertragspartei nach Maßgabe ihres jeweiligen innerstaatlichen Rechts im Einzelfall auch ohne Ersuchen die in Absatz 2 genannten personenbezogenen Daten übermitteln, soweit dies erforderlich ist, weil bestimmte Tatsachen die Annahme rechtfertigen, dass der Betroffene oder die Betroffenen

Article 6**National contact points and implementing agreements**

(1) For the purpose of the supply of data as referred to in Article 4, each Party shall designate one or more national contact points. The powers of the contact points shall be governed by the national law applicable.

(2) The technical and procedural details for the searching conducted pursuant to Article 4 shall be set forth in one or more implementing agreements.

Article 7**Automated searching of DNA profiles**

(1) If permissible under the national law of both parties and on the basis of reciprocity, the Parties may allow each other's national contact point, as referred to in Article 9, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles for the investigation of serious crime. Searches may be exercised only in individual cases and in compliance with the searching Party's national law.

(2) Should an automated search show that a DNA profile supplied matches a DNA profile entered in the other Party's file, the searching national contact point shall receive by automated notification the reference data for which a match has been found. If no match can be found, automated notification of this shall be given.

Article 8**Supply of further personal and other data**

Should the procedure referred to in Article 7 show a match between DNA profiles, the supply of any available further personal data and other data relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Party.

Article 9**National contact point and implementing agreements**

(1) For the purposes of the supply of data as set forth in Article 7, each Party shall designate a national contact point. The powers of the contact point shall be governed by the national law applicable.

(2) The technical and procedural details for the searching conducted pursuant to Article 7 shall be set forth in one or more implementing agreements.

Article 10**Supply of personal and other data
in order to prevent terrorist offenses**

(1) For the prevention of terrorist offenses, the Parties may, in compliance with their respective national law, in individual cases, even without being requested to do so, supply the other Party's relevant national contact point, as referred to in paragraph 7, with the personal data specified in paragraph 2, in so far as is necessary because particular circumstances give reason to believe that the data subject(s):

- a) terroristische Straftaten oder Straftaten, die mit Terrorismus oder einer terroristischen Gruppe oder Vereinigung in Zusammenhang stehen, begehen wird/werden, soweit solche Straftaten nach dem innerstaatlichen Recht der übermittelnden Vertragspartei definiert sind, oder
- b) eine Ausbildung zur Begehung der unter Buchstabe a genannten Straftaten durchläuft/durchlaufen oder durchlaufen hat/haben.

(2) Die zu übermittelnden personenbezogenen Daten umfassen, soweit vorhanden, Familiennamen, Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, Geschlecht, Geburtsdatum, Geburtsort, aktuelle und frühere Staatsangehörigkeiten, Reisepassnummer, Nummern anderer Ausweispapiere und Fingerabdruckdaten sowie die Darstellung der Tatsachen, aus denen sich die Annahme nach Absatz 1 ergibt.

(3) Mit der Notifikation nach Artikel 24 Satz 1 können die Vertragsparteien einander in einer gesonderten Erklärung die Straftaten notifizieren, die nach ihrem innerstaatlichen Recht als Straftaten im Sinne des Absatzes 1 gelten. Diese Erklärung kann jederzeit durch eine Notifikation gegenüber der anderen Vertragspartei geändert werden.

(4) Die übermittelnde Behörde kann nach Maßgabe ihres innerstaatlichen Rechts Bedingungen für die Verwendung dieser Daten durch die empfangende Behörde festlegen. Wenn die empfangende Behörde die Daten annimmt, ist sie an diese Bedingungen gebunden.

(5) Allgemeine Einschränkungen in Bezug auf die Rechtsnormen der empfangenden Vertragspartei für die Verarbeitung personenbezogener Daten können von der übermittelnden Vertragspartei nicht als Bedingung im Sinne des Absatzes 4 für die Übermittlung von Daten auferlegt werden.

(6) Zusätzlich zu den in Absatz 2 bezeichneten personenbezogenen Daten können die Vertragsparteien auch nicht personenbezogene Daten mit Terrorismusbezug übermitteln.

(7) Jede Vertragspartei benennt eine oder mehrere nationale Kontaktstellen für den Austausch personenbezogener und anderer Daten mit der nationalen Kontaktstelle der anderen Vertragspartei nach diesem Artikel. Die Befugnisse der nationalen Kontaktstellen richten sich nach dem für sie geltenden innerstaatlichen Recht.

Artikel 11

Schutz der Privatsphäre und Datenschutz

(1) Die Vertragsparteien erkennen an, dass der Umgang mit und die Verarbeitung von personenbezogenen Daten, die sie voneinander erhalten, für den Schutz des Vertrauens bei der Durchführung dieses Abkommens von entscheidender Bedeutung sind.

(2) Die Vertragsparteien verpflichten sich, personenbezogene Daten nach Treu und Glauben und nach ihren jeweiligen Rechtsvorschriften zu verarbeiten und

- a) sicherzustellen, dass die bereitgestellten personenbezogenen Daten im Verhältnis zu dem konkreten Zweck der Übermittlung angemessen und relevant sind,
- b) die personenbezogenen Daten nur so lange aufzubewahren, als dies für den Zweck, zu dem die Daten in Übereinstimmung mit diesem Abkommen bereitgestellt oder weiterverarbeitet wurden, nötig ist, und
- c) sicherzustellen, dass die empfangende Vertragspartei rechtzeitig auf eventuell unrichtige personenbezogene Daten hingewiesen wird, damit geeignete Korrekturen durchgeführt werden können.

(3) Aus diesem Abkommen erwachsen Privatpersonen keine Rechte, auch nicht das Recht, Beweismittel zu erlangen, zu unterdrücken oder auszuschließen oder den Austausch perso-

- a. will commit terrorist or terrorism-related offenses, or offenses related to a terrorist group or association, as those offenses are defined under the supplying Party's national law or
- b. are undergoing or have undergone training to commit the offenses referred to in subparagraph a.

(2) The personal data to be supplied shall include, if available, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, current and former nationalities, passport number, numbers from other identity documents, and fingerprinting data, as well as a description of the circumstances giving rise to the belief referred to in paragraph 1.

(3) Together with the notification according to Article 24 sentence 1, the Parties may in a separate declaration notify each other of the offenses which under the respective Party's law are considered as offenses within the scope of paragraph 1. This declaration may be altered at any time by notification to the other Party.

(4) The supplying authority may, in compliance with its national law, impose conditions on the use made of such data by the receiving authority. If the receiving authority accepts such data, it shall be bound by any such conditions.

(5) Generic restrictions with respect to the legal standards of the receiving party for processing personal data may not be imposed by the transmitting party as a condition under subparagraph 4 to providing data.

(6) In addition to the personal data referred to in paragraph 2, the Parties may provide each other with non-personal, terrorism-related data.

(7) Each Party shall designate one or more national contact points for the exchange of personal and other data under this Article with the other Party's contact points. The powers of the national contact points shall be governed by the national law applicable.

Article 11

Privacy and Data Protection

(1) The Parties recognize that the handling and processing of personal data that they acquire from each other is of critical importance to preserving confidence in the implementation of this Agreement.

(2) The Parties commit themselves to processing personal data fairly and in accord with their respective laws and:

- a. ensuring that the personal data provided is adequate and relevant in relation to the specific purpose of the transfer;
- b. retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Agreement; and
- c. ensuring that possibly inaccurate personal data is timely brought to the attention of the receiving Party in order that appropriate corrective action is taken.

(3) This Agreement shall not give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data. Rights

nenbezogener Daten zu behindern. Unabhängig von diesem Abkommen bestehende Rechte bleiben jedoch unberührt.

Artikel 12

Übermittlung von personenbezogenen Daten besonderer Kategorien

(1) Personenbezogene Daten, aus denen die Rasse oder ethnische Herkunft, politische Anschauungen, religiöse oder sonstige Überzeugungen oder die Mitgliedschaft in Gewerkschaften hervorgeht oder die die Gesundheit und das Sexualleben betreffen, dürfen nur zur Verfügung gestellt werden, wenn sie für die Zwecke dieses Abkommens besonders relevant sind.

(2) In Anerkennung der besonderen Schutzbedürftigkeit der in Absatz 1 genannten Kategorien personenbezogener Daten treffen die Vertragsparteien geeignete Schutzvorkehrungen, insbesondere geeignete Sicherheitsmaßnahmen, um diese Daten zu schützen.

Artikel 13

Verwendungsbeschränkungen zum Schutz personenbezogener und sonstiger Daten

(1) Unbeschadet des Artikels 10 Absatz 4 darf eine Vertragspartei Daten, die sie nach diesem Abkommen gewonnen hat, verarbeiten

- a) für den Zweck ihrer strafrechtlichen Ermittlungen;
- b) zur Verhinderung einer ernsthaften Bedrohung ihrer öffentlichen Sicherheit;
- c) in ihren nicht strafrechtlichen Gerichts- oder Verwaltungsverfahren, die in direktem Zusammenhang mit den unter Buchstabe a genannten Ermittlungen stehen, sowie
- d) für jeden anderen Zweck, jedoch nur mit der vorherigen Zustimmung der Vertragspartei, die die Daten übermittelt hat.

(2) Die Vertragsparteien geben Daten, die nach diesem Abkommen bereitgestellt wurden, ohne die Zustimmung der Vertragspartei, die die Daten bereitgestellt hat, und ohne geeignete Schutzvorkehrungen nicht an Drittstaaten, internationale Organe oder private Körperschaften weiter.

(3) Eine Vertragspartei darf in den daktyloskopischen Dateien oder DNA-Dateien der anderen Vertragspartei einen automatisierten Abruf nach Artikel 4 oder 7 lediglich dazu durchführen und die als Ergebnis eines solchen Abrufs erhaltenen Daten, einschließlich der Mitteilung über das Vorliegen oder Nichtvorliegen eines Treffers, lediglich dazu verarbeiten, um

- a) festzustellen, ob die verglichenen DNA-Profile oder daktyloskopischen Daten übereinstimmen,
- b) im Fall einer Übereinstimmung der Daten ein Folgeersuchen um Hilfe nach Maßgabe ihres innerstaatlichen Rechts einschließlich der Vorschriften über die Rechtshilfe vorzubereiten und einzureichen oder
- c) Dokumentationsmaßnahmen durchzuführen, soweit diese durch ihr innerstaatliches Recht verlangt oder gestattet werden.

Die Datei führende Vertragspartei darf die ihr nach den Artikeln 4 und 7 von der abrufenden Vertragspartei im Zuge eines automatisierten Abrufs übermittelten Daten lediglich verarbeiten, soweit dies zur Durchführung des Abgleichs, zur automatisierten Beantwortung der Anfrage oder zur Protokollierung nach Artikel 15 erforderlich ist. Nach Beendigung des Datenabgleichs oder nach der automatisierten Beantwortung der Anfrage werden die zu Vergleichszwecken übermittelten Daten unverzüglich gelöscht, soweit nicht die Weiterverarbeitung zu den in Satz 1 dieses Absatzes unter den Buchstaben b und c genannten Zwecken erforderlich ist.

existing independently of this Agreement, however, are not affected.

Article 12

Transmission of Special Categories of Personal Data

(1) Personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership or concerning health and sexual life may only be provided if they are particularly relevant to the purposes of this Agreement.

(2) The Parties, recognizing the special sensitivity of the above categories of personal data, shall take suitable safeguards, in particular appropriate security measures, in order to protect such data.

Article 13

Limitation on processing to protect personal and other data

(1) Without prejudice to Article 10, paragraph 4, a Party may process data obtained under this Agreement:

- a. for the purpose of its criminal investigations;
- b. for preventing a serious threat to its public security;
- c. in its non-criminal judicial or administrative proceedings directly related to investigations set forth in subparagraph a; or
- d. for any other purpose, only with the prior consent of the Party which has transmitted the data.

(2) The Parties shall not communicate data provided under this Agreement to any third State, international body or private entity without the consent of the Party that provided the data and without the appropriate safeguards.

(3) A Party may conduct an automated search of the other Party's fingerprint or DNA files under Articles 4 or 7, and process data received in response to such a search, including the communication whether or not a hit exists, solely in order to:

- a. establish whether the compared DNA profiles or fingerprint data match;
- b. prepare and submit a follow-up request for assistance in compliance with its national law, including the legal assistance rules, if those data match; or
- c. conduct record-keeping, as required or permitted by its national law.

The Party administering the file may process the data supplied to it by the searching Party during the course of an automated search in accordance with Articles 4 and 7 solely where this is necessary for the purposes of comparison, providing automated replies to the search or record-keeping pursuant to Article 15. The data supplied for comparison shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under subparagraphs b. and c. of this paragraph.

Artikel 14**Berichtigung, Sperrung
und Löschung von Daten**

(1) Auf Verlangen der übermittelnden Vertragspartei ist die empfangende Vertragspartei verpflichtet, Daten, die sie nach diesem Abkommen erlangt hat, in Übereinstimmung mit ihrem innerstaatlichen Recht zu korrigieren, zu sperren oder zu löschen, wenn sie unrichtig oder unvollständig sind oder ihre Erhebung oder Weiterverarbeitung im Widerspruch zu diesem Abkommen oder zu den für die übermittelnde Vertragspartei geltenden Vorschriften steht.

(2) Stellt eine Vertragspartei fest, dass Daten, die sie von der anderen Vertragspartei nach diesem Abkommen erhalten hat, unrichtig sind, ergreift sie alle geeigneten Maßnahmen zum Schutz vor fälschlichem Vertrauen auf diese Daten; dies umfasst insbesondere die Ergänzung, Löschung oder Berichtigung solcher Daten.

(3) Stellt eine Vertragspartei fest, dass wesentliche Daten, die sie nach diesem Abkommen der anderen Vertragspartei übermittelt oder von ihr empfangen hat, unrichtig oder nicht verlässlich oder Gegenstand erheblicher Zweifel sind, teilt sie dies der anderen Vertragspartei mit.

Artikel 15**Dokumentation**

(1) Jede Vertragspartei führt ein Protokoll der nach diesem Abkommen an die andere Vertragspartei übermittelten und von ihr erhaltenen Daten. Dieses Protokoll dient dazu,

- a) eine wirksame Datenschutzkontrolle nach Maßgabe des innerstaatlichen Rechts der jeweiligen Vertragspartei zu gewährleisten;
- b) die Vertragsparteien in die Lage zu versetzen, die sich aus den Artikeln 14 und 18 ergebenden Rechte wirksam wahrnehmen zu können;
- c) Datensicherheit zu gewährleisten.

(2) Das Protokoll umfasst

- a) die übermittelten Daten,
- b) das Datum der Übermittlung sowie
- c) im Fall der Weitergabe der Daten an andere Stellen den Empfänger der Daten.

(3) Die Protokolldaten sind durch geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen und zwei Jahre aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unverzüglich zu löschen, soweit innerstaatliches Recht einschließlich anwendbarer Datenschutz- und Datenaufbewahrungsvorschriften nicht entgegensteht.

Artikel 16**Datensicherheit**

(1) Die Vertragsparteien gewährleisten die notwendigen technischen Maßnahmen und organisatorischen Vorkehrungen, um personenbezogene Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder unbefugte Bekanntgabe, unbefugte Veränderung, unbefugten Zugang oder jede unbefugte Form der Verarbeitung zu schützen. Insbesondere gewährleisten die Vertragsparteien, dass nur besonders dazu befugte Personen Zugang zu diesen personenbezogenen Daten haben.

(2) Die Durchführungsvereinbarungen, die das Verfahren für den automatisierten Abruf von daktyloskopischen Daten und DNA-Daten nach den Artikeln 4 und 7 regeln, sehen vor, dass

- a) moderne Technologie in geeigneter Weise eingesetzt wird, um den Schutz, die Sicherheit, die Vertraulichkeit und die Integrität der Daten sicherzustellen,

Article 14**Correction, blockage and deletion of data**

(1) At the request of the supplying Party, the receiving Party shall be obliged to correct, block, or delete, consistent with its national law, data received under this Agreement that is incorrect or incomplete or if its collection or further processing contravenes this Agreement or the rules applicable to the supplying Party.

(2) Where a Party becomes aware that data it has received from the other Party under this Agreement is not accurate, it shall take all appropriate measures to safeguard against erroneous reliance on such data, which shall include in particular supplementation, deletion, or correction of such data.

(3) Each Party shall notify the other if it becomes aware that material data it has transmitted to the other Party or received from the other Party under this Agreement is inaccurate or unreliable or is subject to significant doubt.

Article 15**Documentation**

(1) Each party shall maintain a record of the transmission and receipt of data communicated to the other party under this Agreement. This record shall serve to:

- a. ensure effective monitoring of data protection in accordance with the national law of the respective Party;
- b. enable the Parties to effectively make use of the rights granted to them according to Articles 14 and 18; and
- c. ensure data security.

(2) The record shall include:

- a. the data supplied,
- b. the date of supply and
- c. the recipient of the data in case the data is supplied to other entities.

(3) The recorded data must be protected with suitable measures against inappropriate use and other forms of improper use and must be kept for two years. After the conservation period the recorded data must be deleted immediately, unless this is inconsistent with national law, including applicable data protection and retention rules.

Article 16**Data Security**

(1) The Parties shall ensure that the necessary technical measures and organizational arrangements are utilized to protect personal data against accidental or unlawful destruction, accidental loss or unauthorized disclosure, alteration, access or any unauthorized form of processing. The Parties in particular shall ensure that only those authorized to access personal data can have access to such data.

(2) The implementing agreements that govern the procedures for automated searches of fingerprint and DNA files pursuant to Articles 4 and 7 shall provide:

- a. that appropriate use is made of modern technology to ensure data protection, security, confidentiality and integrity;

- b) bei der Nutzung allgemein zugänglicher Netze Verschlüsselungs- und Authentifizierungsverfahren angewendet werden, die von den dafür zuständigen Stellen anerkannt worden sind, und
- c) ein Mechanismus besteht, um sicherzustellen, dass nur erlaubte Abrufe durchgeführt werden.
- b. that encryption and authorization procedures recognized by the competent authorities are used when having recourse to generally accessible networks; and
- c. for a mechanism to ensure that only permissible searches are conducted.

Artikel 17

Transparenz – Information der Betroffenen

(1) Dieses Abkommen ist nicht so auszulegen, dass dadurch die nach ihren jeweiligen Rechtsvorschriften bestehenden gesetzlichen Verpflichtungen der Vertragsparteien beeinträchtigt werden, wonach sie die betroffene Person über die Zwecke der Datenverarbeitung, die Identität des für die Datenverarbeitung Verantwortlichen, die Empfänger oder Empfängerkategorien sowie über ihr Recht, die sie betreffenden Daten einzusehen und zu berichtigen, zu informieren haben, sowie ihr jede weitere Information zu geben, wie Informationen über die Rechtsgrundlage des Verarbeitungsvorgangs, für den die Daten vorgesehen sind, über die Fristen für die Datenspeicherung und das Recht, Rechtsmittel einzulegen, soweit solche weiteren Informationen notwendig sind, unter Berücksichtigung der Zwecke und der konkreten Umstände, unter denen die Daten verarbeitet werden, um gegenüber der betroffenen Person eine faire Verarbeitung zu gewährleisten.

(2) Solche Informationen dürfen in Übereinstimmung mit den jeweiligen Rechtsvorschriften der Vertragsparteien verweigert werden, einschließlich der Fälle, in denen

- a) die Zwecke der Verarbeitung,
- b) Ermittlungen oder strafrechtliche Verfolgungsmaßnahmen der zuständigen Behörden in der Bundesrepublik Deutschland oder in den Vereinigten Staaten von Amerika oder
- c) die Rechte und Freiheiten Dritter
- durch die Bereitstellung dieser Informationen gefährdet würden.

Artikel 18

Unterrichtung

Die empfangende Vertragspartei unterrichtet die übermittelnde Vertragspartei auf Anfrage über die Verarbeitung der übermittelten Daten und das dadurch erzielte Ergebnis. Die empfangende Vertragspartei stellt sicher, dass ihre Antwort der übermittelnden Vertragspartei zeitnah mitgeteilt wird.

Artikel 19

Verhältnis zu anderen Übereinkünften

Dieses Abkommen ist nicht so auszulegen, dass es Bestimmungen anderer Verträge, Abkommen oder des innerstaatlichen Rechts oder bestehende Strafverfolgungsbeziehungen, die den Austausch von Informationen zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika zulassen, beschränkt oder beeinträchtigt.

Artikel 20

Konsultationen

(1) Die Vertragsparteien konsultieren sich gegenseitig regelmäßig über die Durchführung dieses Abkommens.

(2) Im Fall von Streitigkeiten über die Auslegung oder Anwendung dieses Abkommens konsultieren sich die Vertragsparteien, um deren Beilegung zu erleichtern.

Artikel 21

Ausgaben

Jede Vertragspartei trägt die Ausgaben, die ihren Behörden bei der Umsetzung dieses Abkommens entstehen. In Sonderfällen können die Vertragsparteien andere Regelungen vereinbaren.

Article 17

Transparency – Providing information to the data subjects

(1) Nothing in this Agreement shall be interpreted to interfere with the Parties' legal obligations, as set forth by their respective laws, to provide data subjects with information as to the purposes of the processing and the identity of the data controller, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him or her and any further information such as the legal basis of the processing operation for which the data are intended, the time limits for storing the data and the right of recourse, in so far as such further information is necessary, having regard for the purposes and the specific circumstances in which the data are processed, to guarantee fair processing with respect to data subjects.

(2) Such information may be denied in accordance with the respective laws of the Parties, including if providing this information may jeopardize:

- a. the purposes of the processing;
- b. investigations or prosecutions conducted by the competent authorities in the United States of America or by the competent authorities in the Federal Republic of Germany; or
- c. the rights and freedoms of third parties.

Article 18

Information

Upon request, the receiving Party shall inform the supplying Party of the processing of supplied data and the result obtained. The receiving Party shall ensure that its answer is communicated to the supplying Party in a timely manner.

Article 19

Relation to Other Agreements

Nothing in this Agreement shall be construed to limit or prejudice the provisions of any other treaty, agreement, or domestic law, or to affect any working law enforcement relationship allowing for information sharing between the Federal Republic of Germany and the United States of America.

Article 20

Consultations

(1) The Parties shall consult each other regularly on the implementation of the provisions of this Agreement.

(2) In the event of any dispute regarding the interpretation or application of this Agreement, the Parties shall consult each other in order to facilitate its resolution.

Article 21

Expenses

Each Party shall bear the expenses incurred by its authorities in implementing this Agreement. In special cases, the Parties concerned may agree on different arrangements.

Artikel 22**Kündigung des Abkommens**

Dieses Abkommen kann von jeder Vertragspartei unter Einhaltung einer dreimonatigen Kündigungsfrist schriftlich gekündigt werden. Auf die bereits übermittelten Daten findet dieses Abkommen weiter Anwendung.

Artikel 23**Änderungen**

(1) Die Vertragsparteien nehmen auf Ersuchen einer Vertragspartei Konsultationen über Änderungen dieses Abkommens auf.

(2) Dieses Abkommen kann jederzeit durch schriftliche Übereinkunft der Vertragsparteien geändert werden.

Artikel 24**Inkrafttreten**

Dieses Abkommen tritt, mit Ausnahme der Artikel 7 bis 9, an dem Tag des Eingangs der letzten Note in Kraft, die den diplomatischen Notenwechsel abschließt, mit dem die Vertragsparteien einander notifizieren, dass sie die für das Inkrafttreten des Abkommens erforderlichen Schritte unternommen haben. Die Artikel 7 bis 9 dieses Abkommens treten nach dem Abschluss der in Artikel 9 genannten Durchführungsvereinbarung oder Durchführungsvereinbarungen und an dem Tag des Eingangs der letzten Note in Kraft, die den diplomatischen Notenwechsel zwischen den Vertragsparteien abschließt, mit dem festgestellt wird, dass jede Vertragspartei in der Lage ist, diese Artikel auf der Basis der Gegenseitigkeit durchzuführen. Dies erfolgt, wenn das Recht beider Vertragsparteien den DNA-Datenaustausch nach den Artikeln 7 bis 9 erlaubt.

Geschehen zu Washington D.C. am 1. Oktober 2008 in zwei Urschriften, jede in deutscher und englischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist.

Article 22**Termination of the Agreement**

This Agreement may be terminated by either Party with three months' notice in writing to the other Party. The provisions of this Agreement shall continue to apply to data supplied prior to such termination.

Article 23**Amendments**

(1) The Parties shall enter into consultations with respect to the amendment of this Agreement at the request of either Party.

(2) This Agreement may be amended by written agreement of the Parties at any time.

Article 24**Entry into force**

This Agreement shall enter into force, with the exception of Articles 7 through 9, on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each has taken the steps necessary to bring the Agreement into force. Articles 7 through 9 of this Agreement shall enter into force following the conclusion of the implementing agreement(s) referenced in Article 9 and on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each Party is able to implement those articles on a reciprocal basis. This shall occur if the laws of both Parties permit the type of DNA screening contemplated by Articles 7 to 9.

Done at Washington D.C. on October 1st 2008, in duplicate, in the German and English languages, both texts being equally authentic.

Für die Regierung der Bundesrepublik Deutschland
For the Government of the Federal Republic of Germany

Scharioth

Für die Regierung der Vereinigten Staaten von Amerika
For the Government of the United States of America

Burns

Denkschrift

I. Allgemeines

Die wirksame Bekämpfung der schwerwiegenden Kriminalität und insbesondere des Terrorismus erfordert eine enge grenzüberschreitende Zusammenarbeit. Vor diesem Hintergrund haben die Regierung der Bundesrepublik Deutschland und die Regierung der Vereinigten Staaten von Amerika am 1. Oktober 2008 in Washington D.C. ein Abkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität unterzeichnet.

Mit dem Abkommen sollen insbesondere die Rechtsgrundlagen für einen verbesserten Informationsaustausch geschaffen werden. Das Abkommen orientiert sich dabei an dem Vorbild des am 27. Mai 2005 zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich geschlossenen Prümer Vertrags, der zu einer erheblichen Verbesserung des Informationsaustauschs zwischen den Vertragsstaaten geführt hat. Das Abkommen sieht ebenso wie der Prümer Vertrag den automatisierten Abruf von Fingerabdruck- und DNA-Daten im sogenannten Hit-/No-Hit-Verfahren sowie den Austausch von Daten zu sogenannten terroristischen Gefährdern vor.

Die Bestimmungen des Abkommens sind detailliert gefasst und enthalten präzise Beschreibungen der Voraussetzungen und des Verfahrens des Datenaustauschs. Gleichwohl bedarf es zur Umsetzung einzelner Bestimmungen des Abkommens in das deutsche Recht ergänzender Regelungen, die in einem von diesem Gesetz gesonderten Ausführungsgesetz getroffen werden. Die Einzelheiten der technischen Umsetzung des automatisierten Datenaustauschs werden in einer oder mehreren Durchführungsvereinbarungen geregelt, die sich an der Durchführungsvereinbarung zum Prümer Vertrag orientieren werden. Eine Anpassung bestehender Gesetze ist zur Umsetzung des Abkommens nicht erforderlich.

II. Besonderes

Zu Artikel 1 – Begriffsbestimmungen

Artikel 1 stellt das einheitliche Verständnis bestimmter zentraler Begriffe sicher.

Nummer 1 definiert den Begriff „DNA-Profil“. Die Definition ist wortgleich zu der Definition in Ziffer 2.4 der Durchführungsvereinbarung zum Prümer Vertrag.

Nummer 2 definiert den Begriff „Fundstellendatensätze“. Die Definition entspricht Artikel 2 Absatz 2 Sätze 2 bis 4 und Artikel 8 Sätze 2 bis 4 des Prümer Vertrags. Im Unterschied zum Prümer Vertrag wird die Definition hier in einer Vorschrift zusammengefasst und im Rahmen der allgemeinen Begriffsbestimmungen vorangestellt. Die Definition stellt insbesondere klar, dass Fundstellendatensätze keine den Betroffenen unmittelbar identifizierenden Daten enthalten dürfen, wie z. B. Namen, Geburtstag, Geburtsort oder Angaben zur Tat. Es handelt sich folglich um so genannte pseudonymisierte Daten. Hierdurch wird in Verbindung mit Artikeln 4 und 7 des Abkommens gewährleistet, dass lediglich ein einge-

schränkter Zugriff auf die nationalen DNA-Analysedateien bzw. die nationalen Fingerabdruckdateien eingeräumt wird.

Nummer 3 definiert personenbezogene Daten als Informationen über eine bestimmte oder bestimmbar natürliche Person. Die Definition ist an § 3 Absatz 1 Bundesdatenschutzgesetz (BDSG) angelehnt.

Nummer 4 definiert den Begriff der Verarbeitung personenbezogener Daten. Die Definition entspricht Artikel 33 Absatz 1 Nummer 1 des Prümer Vertrags und umfasst anders als im deutschen Recht (§ 3 Absatz 4 Satz 1 BDSG) auch die Erhebung und die Nutzung personenbezogener Daten.

Zu Artikel 2 – Zweck des Abkommens

Artikel 2 bestimmt den Abkommenszweck. Dieser ist im Unterschied zum Prümer Vertrag auf die Bekämpfung und Verhinderung schwerwiegender Kriminalität begrenzt. Aufgrund der geographischen Entfernung zwischen den Vertragsstaaten spielt die Bekämpfung von Klein- und mittlerer Kriminalität in der Zusammenarbeit lediglich eine untergeordnete Rolle.

Zu Artikel 3 – Daktyloskopische Daten

Artikel 3 entspricht Artikel 8 Sätze 1 und 2 des Prümer Vertrags. Er enthält die Verpflichtung der Vertragsparteien, für die Zwecke der Durchführung des Vertrags sicherzustellen, dass zum Bestand der zum Zwecke der Verhinderung und Verfolgung von Straftaten eingerichteten nationalen Fingerabdruckidentifizierungssysteme (AFIS) Fundstellendatensätze vorhanden sind. Dies betrifft in Deutschland das beim Bundeskriminalamt geführte AFIS. Die Formulierung „für die Zwecke der Durchführung des Abkommens“ stellt klar, dass Fundstellendatensätze nur eingerichtet werden müssen, um der anderen Vertragspartei den Hit-/No-Hit-Zugriff zu ermöglichen, die Vertragsparteien jedoch nicht verpflichtet sind, ihre Datenbanken auch für die innerstaatliche Nutzung umzustrukturieren. Eine Definition des Begriffs „Fundstellendatensätze“ findet sich in Artikel 1 Nummer 2.

Zu Artikel 4 – Automatisierter Abruf daktyloskopischer Daten

Artikel 4 entspricht Artikel 9 des Prümer Vertrags und regelt die Voraussetzungen und das Verfahren für den automatisierten Abruf daktyloskopischer Daten.

Ein automatisierter Abruf ist ein Direktzugriff auf eine automatisierte Datenbank einer anderen Stelle, der in der Weise erfolgt, dass ein Ersuchen um Übermittlung personenbezogener Daten („Anfrage“) vollständig automatisiert, also ohne menschliches Zutun, beantwortet wird. Die anfragende Stelle recherchiert also selbst unmittelbar in der Datenbank der anderen Stelle, indem sie einen Anfragedatensatz (nach diesem Abkommen ein Fingerabdruck oder ein DNA-Profil) elektronisch an die andere Stelle übermittelt und daraufhin einen automatisch generierten Antwortdatensatz (nach diesem Abkommen ein Fundstellendatensatz) zurückerhält.

Absatz 1 Satz 1 erlaubt der jeweiligen nationalen Kontaktstelle der Vertragsparteien, auf die zur Verhinderung

und Verfolgung von Straftaten eingerichteten automatisierten Fingerabdruckidentifizierungssysteme (AFIS) der jeweils anderen Vertragspartei zuzugreifen, soweit dies zur Verhinderung oder Verfolgung einer schwerwiegenden Straftat erforderlich ist. Dieses Zugriffsrecht ist auf die Fundstellendatensätze nach Artikel 1 Nummer 2 in Verbindung mit Artikel 3 begrenzt. Nach Satz 2 darf die Anfrage nur im Einzelfall erfolgen. Ein Massenabgleich ist folglich unzulässig.

Absatz 2 bestimmt, dass die endgültige Zuordnung eines daktyloskopischen Datums zu einem Fundstellendatensatz der Datei führenden Vertragspartei durch die abrufende nationale Kontaktstelle anhand der automatisiert übermittelten Fundstellendatensätze, die für die eindeutige Zuordnung erforderlich sind, erfolgt. Anders als bei DNA-Identifizierungsmustern ist es aufgrund des unterschiedlichen technischen Verfahrens nicht immer möglich, bereits beim ersten automatisierten Vergleich eine eindeutige Zuordnung des übermittelten daktyloskopischen Datums zu dem entsprechenden Fundstellendatensatz bei der empfangenden Vertragspartei vorzunehmen. Zur endgültigen Zuordnung kann es daher notwendig sein, mehrere annähernd übereinstimmende Fundstellendatensätze von der Datei führenden Partei an die abrufende Partei automatisiert zu übermitteln. Bei der abrufenden Vertragspartei erfolgt dann durch einen Daktyloskopen die eindeutige Zuordnung des daktyloskopischen Datums zu einem der übermittelten Fundstellendatensätze (Verifizierung).

Zu Artikel 5 – Übermittlung weiterer personenbezogener und sonstiger Daten

Artikel 5 stellt klar, dass das vorliegende Abkommen nicht für den Datenaustausch gilt, der sich ggf. an einen bei dem automatisierten Vergleich erzielten Treffer anschließt. Wie auch beim Prümer Vertrag richtet sich die Übermittlung weiterer personenbezogener und sonstiger Daten, etwa die Personalien des Betroffenen, nach dem innerstaatlichen Recht der übermittelnden Vertragspartei. Insbesondere sind bei einer Datenübermittlung zu Strafverfolgungszwecken die rechtshilferechtlichen Bestimmungen anzuwenden.

Zu Artikel 6 – Nationale Kontaktstellen und Durchführungsvereinbarungen

Absatz 1 verpflichtet die Vertragsparteien, zur Durchführung der Datenübermittlung eine oder mehrere nationale Kontaktstellen zu benennen. Deutschland wird als nationale Kontaktstelle das Bundeskriminalamt benennen. Die automatisierten Abrufe erfolgen ausschließlich über die nationalen Kontaktstellen. Hinsichtlich der Befugnisse der Kontaktstellen verweist das Abkommen auf das jeweils für sie geltende innerstaatliche Recht.

Absatz 2 verweist hinsichtlich der Einzelheiten der technischen Ausgestaltung und des Ablaufs des automatisierten Abrufverfahrens auf eine oder mehrere Durchführungsvereinbarungen. In diesen Durchführungsvereinbarungen werden insbesondere die Fragen der einheitlichen Datenformate, der Systeminfrastruktur und der Kommunikationsinfrastruktur zu regeln sein.

Zu Artikel 7 – Automatisierter Abruf von DNA-Profilen

Parallel zu der Regelung in Artikel 4 für den Bereich der daktyloskopischen Daten schafft Artikel 7 die Grundlage

für den automatisierten Abruf von DNA-Profilen. Im Unterschied zu der Regelung in Artikel 4 ist der automatisierte Abruf von DNA-Profilen jedoch auf Strafverfolgungszwecke beschränkt. Der Zusatz „Soweit dies nach dem innerstaatlichen Recht beider Vertragsparteien zulässig ist und auf der Basis der Gegenseitigkeit“ trägt dem Umstand Rechnung, dass es sich bei den Regelungen zum automatisierten DNA-Datenaustausch zunächst nur um Vorratsregelungen handelt, da es den Vereinigten Staaten von Amerika zum Zeitpunkt des Vertragsschlusses rechtlich noch nicht möglich ist, deutschen Stellen Zugang zu ihrer DNA-Analysedatei zu gewähren. Durch den Zusatz in Artikel 7 Absatz 1 in Verbindung mit der gestaffelten Inkrafttretensregelung des Artikels 24 wird klargestellt, dass die Regelung erst dann Anwendung findet, wenn die Vertragsparteien sich gegenseitig einen automatisierten Zugriff gewähren. Die Bundesrepublik Deutschland wird also nicht einseitig in Vorleistung treten. Sobald auf beiden Seiten die Voraussetzungen für die Durchführung des automatisierten DNA-Datenaustauschs vorliegen, werden die Artikel 7 bis 9 nach dem in Artikel 24 festgelegten Verfahren nachträglich in Kraft gesetzt.

Zu Artikel 8 – Übermittlung weiterer personenbezogener und sonstiger Daten

Artikel 8 stellt – wie Artikel 5 für den Bereich des automatisierten Fingerabdruckdatenaustauschs – klar, dass das vorliegende Abkommen nicht für den Datenaustausch gilt, der sich ggf. an einen bei dem automatisierten Abruf erzielten Treffer anschließt. Wie auch beim Prümer Vertrag richtet sich die Übermittlung weiterer personenbezogener und sonstiger Daten, etwa die Personalien des Betroffenen, nach dem innerstaatlichen Recht der übermittelnden Vertragspartei, insbesondere den rechtshilferechtlichen Bestimmungen.

Zu Artikel 9 – Nationale Kontaktstelle und Durchführungsvereinbarungen

Absatz 1 verpflichtet die Vertragsparteien, zur Durchführung der Datenübermittlung eine nationale Kontaktstelle zu benennen. Deutschland wird als nationale Kontaktstelle das Bundeskriminalamt benennen. Die automatisierten Abrufe erfolgen ausschließlich über die nationalen Kontaktstellen. Hinsichtlich der Befugnisse der Kontaktstellen verweist das Abkommen auf das jeweils für sie geltende innerstaatliche Recht.

Absatz 2 verweist hinsichtlich der Einzelheiten der technischen Ausgestaltung und des Ablaufs des automatisierten Abrufverfahrens auf eine oder mehrere Durchführungsvereinbarungen. In diesen Durchführungsvereinbarungen werden insbesondere die Fragen der einheitlichen Datenformate, der Systeminfrastruktur und der Kommunikationsinfrastruktur zu regeln sein.

Zu Artikel 10 – Übermittlung personenbezogener und anderer Daten zur Verhinderung terroristischer Straftaten

Artikel 10 ist an Artikel 16 des Prümer Vertrags angelehnt und sieht die Spontanübermittlung personenbezogener und sonstiger Daten zur Verhinderung terroristischer Straftaten vor.

Nach Absatz 1 ist die Übermittlung personenbezogener Daten zur Verhinderung terroristischer Straftaten im Einzelfall auch ohne Ersuchen möglich. Die Übermittlung erfolgt nach Maßgabe des innerstaatlichen Rechts der übermittelnden Vertragspartei.

Im Unterschied zu Artikel 16 des Prümer Vertrags verweist Artikel 10 hinsichtlich der Definition des Begriffs „terroristische Straftat“ nicht auf den Rahmenbeschluss 2002/475/JI des Rates der Europäischen Union, sondern auf das innerstaatliche Recht der übermittelnden Vertragspartei. Ein Verweis auf einen europäischen Rechtsakt kam im Verhältnis zu den Vereinigten Staaten von Amerika nicht in Betracht. Absatz 3 sieht jedoch vor, dass sich die Vertragsparteien einander in einer gesonderten Erklärung die Straftaten notifizieren können, die nach ihrem innerstaatlichen Recht als Straftaten im Sinne des Absatzes 1 gelten. Die Bundesrepublik Deutschland wird von dieser Möglichkeit Gebrauch machen.

Absatz 2 präzisiert die zu übermittelnden Daten.

Absatz 3 sieht vor, dass sich die Vertragsparteien einander in einer gesonderten Erklärung die Straftaten notifizieren können, die nach ihrem innerstaatlichen Recht als Straftaten im Sinne des Absatzes 1 gelten (s. o. zu Absatz 1).

Nach Absatz 4 kann die übermittelnde Behörde nach Maßgabe des für sie geltenden innerstaatlichen Rechts verbindliche Bedingungen für die Verwendung der übermittelten Daten durch die empfangende Behörde festlegen, etwa dass die Daten binnen einer bestimmten Frist zu löschen sind und nicht zur Verhängung der Todesstrafe verwandt werden dürfen.

Absatz 5 schränkt die Möglichkeit der Festlegung von Bedingungen nach Absatz 4 dahingehend ein, dass als Bedingung nach Absatz 4 nicht die Schaffung eines bestimmten Datenschutzregimes auferlegt werden darf.

Absatz 6 stellt klar, dass nicht nur personenbezogene Daten, sondern auch sonstige Daten mit Terrorismusbezug übermittelt werden können, etwa allgemeine Informationen über eine terroristische Vereinigung.

Absatz 7 bestimmt, dass jede Vertragspartei eine oder mehrere nationale Kontaktstellen für den Datenaustausch nach diesem Artikel benennt. Die Befugnisse der Kontaktstellen richten sich nach dem für sie geltenden innerstaatlichen Recht.

Zu Artikel 11 – Schutz der Privatsphäre und Datenschutz

Artikel 11 ist an Artikel 9 des USA-Eurojust-Kooperationsübereinkommens vom 7. September 2006 (Dok.-Nr. 12426/1/06 REV 1) angelehnt und gewährleistet einen einheitlichen datenschutzrechtlichen Mindeststandard. Anders als im Prümer Vertrag, der insoweit auf das Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (BGBl. 1985 II S. 538, 1134) und auf das Zusatzprotokoll zu diesem Übereinkommen aus dem Jahre 2001 verweist (Artikel 34), werden in Artikel 11 die wesentlichen datenschutzrechtlichen Grundsätze, die sich aus den o. g. Rechtstexten ergeben, ausformuliert. Ein Verweis wie im Prümer Vertrag kam in dem vorliegenden Abkommen nicht in Betracht, da die Vereinigten Staaten von Amerika dem Übereinkommen des Europarats vom 28. Januar 1981

sowie dem Zusatzprotokoll aus dem Jahre 2001 bislang nicht beigetreten sind.

Absatz 1 bringt den hohen Stellenwert des Datenschutzes bei der Durchführung des Abkommens zum Ausdruck.

Nach Absatz 2 sind die Vertragsparteien verpflichtet, personenbezogene Daten nach Treu und Glauben und in Übereinstimmung mit ihrem jeweiligen innerstaatlichen Recht zu verarbeiten.

Buchstabe a regelt den Verhältnismäßigkeitsgrundsatz. Die Vertragsparteien haben insbesondere sicherzustellen, dass die bereitgestellten personenbezogenen Daten im Verhältnis zu dem konkreten Zweck der Übermittlung angemessen und relevant sind.

Buchstabe b trägt ebenfalls dem Grundsatz der Verhältnismäßigkeit Rechnung, indem er die Vertragsparteien verpflichtet, die personenbezogenen Daten nur so lange aufzubewahren, wie dies für den Zweck, zu dem die Daten in Übereinstimmung mit dem Abkommen bereit gestellt oder weiterverarbeitet wurden, erforderlich ist.

Buchstabe c verpflichtet die Vertragsparteien sicherzustellen, dass die empfangende Vertragspartei rechtzeitig auf eventuell unrichtige personenbezogene Daten hingewiesen wird. Dies entspricht der in Artikel 5 Buchstabe d des Übereinkommens des Europarats vom 28. Januar 1981 (BGBl. 1985 II S. 538, 1134) vorgesehenen Verpflichtung, auf die Richtigkeit und Aktualität personenbezogener Daten zu achten.

Absatz 3 stellt klar, dass das Abkommen keine Individualrechte begründet. Aufgrund anderweitiger rechtlicher Bestimmungen bestehende subjektive Rechte bleiben unberührt.

Zu Artikel 12 – Übermittlung von personenbezogenen Daten besonderer Kategorien

Artikel 12 stellt personenbezogene Daten, aus denen die Rasse oder ethnische Herkunft, politische Anschauungen, religiöse oder sonstige Überzeugungen oder die Mitgliedschaft in einer Gewerkschaft hervorgehen oder die die Gesundheit oder das Sexualleben betreffen, unter besonderen Schutz. Bei diesem Katalog besonders sensibler Datenkategorien handelt es sich um einen Standardkatalog, der sich so oder so ähnlich in zahlreichen nationalen und internationalen Rechtstexten wiederfindet, beispielsweise in § 3 Absatz 9 Bundesdatenschutzgesetz, Artikel 6 des Übereinkommens des Europarats vom 28. Januar 1981 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sowie Artikel 11 USA-Eurojust-Kooperationsabkommen und Artikel 6 USA-Europol-Abkommen. Diese Kataloge orientieren sich an dem Diskriminierungsverbot des Artikels 14 der Europäischen Menschenrechtskonvention (EMRK).

Nach Absatz 1 dürfen solche besonders sensiblen personenbezogenen Daten nur übermittelt werden, wenn sie für die Zwecke des Abkommens besonders relevant sind. Für die genannten Datenkategorien gelten folglich besondere Anforderungen im Hinblick auf die Erforderlichkeit und Verhältnismäßigkeit der Datenübermittlung.

Absatz 2 verpflichtet die Vertragsparteien, geeignete Schutzvorkehrungen, insbesondere geeignete Sicher-

heitsmaßnahmen zu treffen, um den Schutz der genannten besonders sensiblen Daten sicherzustellen.

Zu Artikel 13 – Verwendungsbeschränkungen zum Schutz personenbezogener und sonstiger Daten

Artikel 13 regelt die Zweckbindung der nach diesem Abkommen übermittelten Daten.

Absatz 1 bestimmt, dass die empfangende Vertragspartei die Daten grundsätzlich nur für ihre strafrechtlichen Ermittlungen (Buchstabe a), für damit in direktem Zusammenhang stehende nicht strafrechtliche Gerichts- und Verwaltungsverfahren (Buchstabe c, beispielsweise ausländerrechtliche Verfahren) sowie zur Verhinderung einer ernsthaften Bedrohung ihrer öffentlichen Sicherheit (Buchstabe b) verarbeiten darf. Eine Verarbeitung zu anderen Zwecken ist nur mit vorheriger Zustimmung der übermittelnden Vertragspartei zulässig. Durch die Formulierung „Unbeschadet des Artikels 10 Absatz 4“ wird klargestellt, dass die von der übermittelnden Vertragspartei nach Artikel 10 Absatz 4 des Abkommens festgelegten Bedingungen von der Regelung des Absatzes 1 unberührt bleiben.

Absatz 2 regelt die Weitergabe der nach diesem Abkommen übermittelten Daten an Dritte. Die empfangende Vertragspartei darf die ihr übermittelten Daten nur mit Zustimmung der übermittelnden Vertragspartei und nur unter geeigneten Schutzvorkehrungen an Drittstaaten, internationale Organisationen oder private Körperschaften weitergeben.

Absatz 3 ist Artikel 35 Absatz 2 des Prümer Vertrages nachgebildet und enthält eine spezielle Zweckbindungsregelung für die im Rahmen des automatisierten Fingerabdruck- und DNA-Datenabrufs übermittelten Daten. Absatz 3 Satz 1 beinhaltet eine abschließende Aufzählung der Zwecke, für die die durch den Abruf erlangten Daten durch die abrufende Vertragspartei verwendet werden dürfen. Absatz 3 Satz 2 enthält eine entsprechend strikte Zweckbindungsregelung für die im Zuge des automatisierten Fingerabdruck- und DNA-Datenabrufs an die Datei führende Vertragspartei übermittelten Anfragedaten. Absatz 3 Satz 3 bezieht sich sowohl auf die Datei führende als auch auf die anfragende Vertragspartei und bestimmt, dass die zu Vergleichszwecken übermittelten Anfragedaten nach der automatisierten Beantwortung der Anfrage unverzüglich zu löschen sind, soweit ihre Weiterverarbeitung nicht zu den in Satz 1 Buchstabe b und c genannten Zwecken, also zur Vorbereitung eines Folgeersuchens (Buchstabe b) oder zur Dokumentation (Buchstabe c), erforderlich ist.

Zu Artikel 14 – Berichtigung, Sperrung und Löschung von Daten

Artikel 14 entspricht u. a. dem in Artikel 5 Buchstabe d des Übereinkommens des Europarats vom 28. Januar 1981 (BGBl. 1985 II S. 538, 1134) verankerten datenschutzrechtlichen Grundsatz der Richtigkeit und Aktualität personenbezogener Daten.

Absatz 1 verpflichtet die empfangende Vertragspartei, auf Verlangen der übermittelnden Vertragspartei Daten, die sie nach diesem Abkommen erlangt hat, in Übereinstimmung mit ihrem innerstaatlichen Recht zu berichtigen, zu sperren oder zu löschen, wenn sie unrichtig oder

unvollständig sind oder ihre Erhebung oder Weiterverarbeitung im Widerspruch zu diesem Abkommen oder zu den für die übermittelnde Vertragspartei geltenden Vorschriften steht. Absatz 1 begründet folglich einen völkerrechtlichen Berichtigungs-, Sperrungs- und Lösungsanspruch der Vertragsparteien. Dieser Anspruch besteht zum einen im Interesse der übermittelnden Vertragspartei selbst, kann von dieser aber auch im Interesse eines Betroffenen geltend gemacht werden. Ein unmittelbarer Berichtigungs-, Sperrungs- und Lösungsanspruch des Betroffenen selbst wird durch das Abkommen hingegen nicht geschaffen (siehe auch Artikel 11 Absatz 3). Die Bundesrepublik Deutschland wird jedoch in einem Ausführungsgesetz einen Rechtsanspruch des Betroffenen verankern, auf dessen Grundlage der Betroffene von der Bundesrepublik Deutschland unter bestimmten Voraussetzungen die Geltendmachung des völkerrechtlichen Auskunftsanspruchs gegenüber den Vereinigten Staaten von Amerika verlangen kann. Auf diese Weise werden die Rechte des Betroffenen auch ohne einen unmittelbaren Auskunftsanspruch ausreichend gewahrt.

Absatz 2 verpflichtet die empfangende Vertragspartei auch unabhängig von einem vorherigen Verlangen der übermittelnden Vertragspartei nach Absatz 1, alle geeigneten Maßnahmen zum Schutz vor fälschlichem Vertrauen auf unrichtige Daten zu ergreifen, wenn sie feststellt, dass Daten, die sie von der anderen Vertragspartei erhalten hat, unrichtig sind. Als geeignete Maßnahmen nennt Absatz 2 insbesondere die Ergänzung, Löschung oder Berichtigung solcher Daten.

Absatz 3 verpflichtet sowohl die empfangende als auch die übermittelnde Vertragspartei, der jeweils anderen Vertragspartei mitzuteilen, falls Daten, die sie nach diesem Abkommen erlangt oder übermittelt hat, unrichtig oder nicht verlässlich sind oder erhebliche Zweifel an ihrer Richtigkeit oder Verlässlichkeit bestehen. Die Mitteilungspflicht beschränkt sich dabei auf wesentliche Daten.

Zu Artikel 15 – Dokumentation

Artikel 15 regelt die Protokollierung des Datenaustauschs nach diesem Abkommen. Die Regelung greift die wesentlichen Elemente der Protokollierungsvorschrift des Prümer Vertrages (Artikel 39) auf und dient insbesondere der Gewährleistung einer wirksamen Kontrolle der Datenübermittlungen nach dem Abkommen.

Absatz 1 Satz 1 verpflichtet die Vertragsparteien zur vollständigen, das heißt nicht nur stichprobenartigen Protokollierung der nach diesem Abkommen übermittelten und empfangenen Daten („Vollprotokollierung“). Absatz 1 Satz 2 bestimmt die Zwecke der Protokollierung. Hierzu gehört u. a. die Gewährleistung einer wirksamen Datenschutzkontrolle, die nach Maßgabe des innerstaatlichen Rechts der jeweiligen Vertragspartei erfolgt.

Absatz 2 definiert den Umfang der Protokollierungspflicht, der für die übermittelnde und die empfangende Vertragspartei identisch ist. Diese doppelte Protokollierung gewährleistet ein besonders hohes Maß an Nachverfolgbarkeit und Kontrollmöglichkeit.

Absatz 3 regelt den Schutz der protokollierten Daten sowie die Aufbewahrungsfrist, die wie beim Prümer Vertrag (Artikel 39 Absatz 4) zwei Jahre beträgt. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unver-

züglich zu löschen. Von der Löschung darf nur abgesehen werden, wenn innerstaatliches Recht der Löschung entgegensteht.

Zu Artikel 16 – Datensicherheit

Artikel 16 lehnt sich an Artikel 38 des Prümer Vertrags an.

Absatz 1 verpflichtet die Vertragsparteien, die notwendigen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit zu ergreifen. Die Regelung ist an Artikel 7 des Übereinkommens des Europarats vom 28. Januar 1981 (BGBl. 1985 II S. 538, 1134) und § 9 BDSG angelehnt.

Absatz 2 enthält Vorgaben für die Durchführungsvereinbarungen zur technischen und organisatorischen Ausgestaltung des automatisierten Abrufverfahrens nach Artikeln 4 und 7, insbesondere im Hinblick auf die Anwendung von Verschlüsselungs- und Authentifizierungsverfahren im Falle der Nutzung allgemein zugänglicher Netze und die Verhinderung unerlaubter Abrufe.

Zu Artikel 17 – Transparenz – Information der Betroffenen

Artikel 17 betrifft die nach anderen Vorschriften bestehenden Rechte und Pflichten im Hinblick auf die Information des Betroffenen. Die Regelung entspricht Artikel 14 des USA-Eurojust-Kooperationsabkommens und trägt dem innerstaatlichen Recht der Vereinigten Staaten von Amerika, insbesondere dem „Privacy Act“, Rechnung.

Absatz 1 stellt klar, dass das Abkommen bestehende gesetzliche Informationspflichten gegenüber dem Betroffenen unberührt lässt.

Absatz 2 benennt Fälle, in denen dem Betroffenen in Übereinstimmung mit dem Recht der jeweiligen Vertragspartei die in Absatz 1 aufgeführten Informationen verweigert werden können.

Zu Artikel 18 – Unterrichtung

Artikel 18 verpflichtet die empfangende Vertragspartei, die übermittelnde Vertragspartei auf Anfrage über die Verarbeitung der übermittelten Daten und das dadurch erzielte Ergebnis zu unterrichten. Artikel 18 enthält folglich einen völkerrechtlichen Auskunftsanspruch der Vertragsparteien. Der Anspruch besteht zum einen im Interesse der übermittelnden Vertragspartei selbst, kann von dieser aber auch im Interesse eines Betroffenen geltend gemacht werden. Ein unmittelbarer Auskunftsanspruch des Betroffenen wird durch das Abkommen hingegen nicht geschaffen (siehe auch Artikel 11 Absatz 3). Die Bundesrepublik Deutschland wird jedoch in einem Ausführungsgesetz einen Rechtsanspruch des Betroffenen verankern, auf dessen Grundlage der Betroffene von der Bundesrepublik Deutschland unter bestimmten Voraussetzungen die Geltendmachung des völkerrechtlichen Auskunftsanspruchs gegenüber den Vereinigten Staaten von Amerika verlangen kann. Auf diese Weise werden die Rechte des Betroffenen auch ohne einen unmittelbaren Auskunftsanspruch ausreichend gewahrt.

Zu Artikel 19 – Verhältnis zu anderen Übereinkommen

Artikel 19 stellt klar, dass durch das Abkommen bestehende Bestimmungen, die den Informationsaustausch zwischen den Vertragsparteien zulassen, weder beschränkt noch beeinträchtigt werden.

Zu Artikel 20 – Konsultationen

Absatz 2 regelt, dass Streitigkeiten über das Abkommen im Verhandlungswege gelöst werden.

Zu Artikel 21 – Ausgaben

Artikel 21 bestimmt, dass jede Vertragspartei die ihren Behörden bei der Umsetzung des Abkommens entstehenden Ausgaben selbst trägt, wobei abweichende Regelungen in besonderen Fällen möglich sind. Die Regelung ist inhaltsgleich zu der entsprechenden Regelung im Prümer Vertrag (Artikel 46).

Zu Artikel 22 – Kündigung des Abkommens

Nach Artikel 22 Satz 1 kann das Abkommen unter Einhaltung einer dreimonatigen Kündigungsfrist schriftlich gekündigt werden. Satz 2 stellt klar, dass das Abkommen auch nach einer Kündigung auf die bereits übermittelten Daten weiterhin Anwendung findet. Hierdurch wird insbesondere die Fortgeltung der datenschutzrechtlichen Bestimmungen sichergestellt.

Zu Artikel 23 – Änderungen

Absatz 1 sieht vor, dass die Vertragsparteien Konsultationen über Änderungen des Abkommens aufnehmen, wenn eine Vertragspartei hierum ersucht.

Nach Absatz 2 gilt für Änderungen des Abkommens das Schriftformerfordernis.

Zu Artikel 24 – Inkrafttreten

Artikel 24 enthält eine gestaffelte Inkrafttretensregelung. Die Regelungen zum automatisierten DNA-Datenaustausch (Artikel 7 bis 9) werden erst zu einem späteren Zeitpunkt in Kraft gesetzt. Diese gestaffelte Inkrafttretensregelung trägt dem Umstand Rechnung, dass es sich bei den Regelungen zum automatisierten DNA-Datenaustausch zunächst nur um Vorratsregelungen handelt, da es den Vereinigten Staaten von Amerika zum Zeitpunkt des Vertragsschlusses rechtlich noch nicht möglich ist, deutschen Stellen Zugang zu ihrer DNA-Analysedatei zu gewähren. Durch die gestaffelte Inkrafttretensregelung wird klargestellt, dass die Regelungen erst dann Anwendung finden, wenn die Vertragsparteien sich gegenseitig einen automatisierten Zugriff gewähren. Die Bundesrepublik Deutschland wird also nicht einseitig in Vorleistung treten. Sobald auf beiden Seiten die Voraussetzungen für die Durchführung des automatisierten DNA-Datenaustauschs vorliegen, werden die Artikel 7 bis 9 nach dem in Artikel 24 festgelegten Verfahren nachträglich in Kraft gesetzt.

Anlage 2**Stellungnahme des Nationalen Normenkontrollrates**

Der Nationale Normenkontrollrat hat das Regelungsvorhaben auf Bürokratiekosten, die durch Informationspflichten begründet werden, geprüft.

Mit den Regelungsvorhaben werden 8 Informationspflichten für die Verwaltung und zwei Informationspflichten für Bürgerinnen und Bürger neu eingeführt.

Das Ressort hat die in den Gesetzentwürfen enthaltenen Informationspflichten nachvollziehbar dargestellt.

Anhaltspunkte für kostengünstigere Regelungsalternativen zur Umsetzung des Abkommens liegen nicht vor. Der Nationale Normenkontrollrat hat daher im Rahmen seines gesetzlichen Prüfauftrags keine Bedenken gegen die Regelungsvorhaben.

Anlage 3

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 858. Sitzung am 15. Mai 2009 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Für eine zielführende Verhütung und Bekämpfung schwerwiegender Kriminalität, insbesondere des internationalen Terrorismus, ist eine partnerschaftliche Zusammenarbeit der Bundesrepublik Deutschland mit anderen Staaten von wesentlicher Bedeutung.
2. Dabei müssen die Grundrechte als hohes Gut eines freiheitlichen Rechtsstaates gewahrt bleiben. Der in dem Abkommen vom 1. Oktober 2008 vorgesehene intensive Austausch personenbezogener Daten setzt insbesondere eine umfassende Auseinandersetzung mit dem verfassungsrechtlich geschützten Recht auf informationelle Selbstbestimmung voraus.
3. Die datenschutzrechtlichen Anforderungen sind vor allem im Hinblick auf die unterschiedlichen Datenschutzstandards der Vertragsparteien zu bewerten. Für die polizeiliche und justizielle Zusammenarbeit innerhalb der Europäischen Union gelten die allgemeinen Grundsätze des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008. Eine vergleichbare Grundlage fehlt im Verhältnis zu den Vereinigten Staaten von Amerika.
4. Vor diesem Hintergrund ist Artikel 12 des Abkommens kritisch zu betrachten. Mit der Regelung sollte eigentlich die Übermittlung von personenbezogenen Daten besonderer Kategorien an strengere Anforderungen geknüpft werden. Die Voraussetzungen sind jedoch nicht hinreichend bestimmt.
 - a) Zum einen wird eine „besondere Relevanz“ der Daten gefordert, ein unbestimmter Rechtsbegriff, der auch nicht weiter definiert wird. Zum anderen wird der Übermittlungszweck nicht hinreichend präzisiert, sondern pauschal auf „die Zwecke dieses Abkommens“ verwiesen.

Außerdem gilt die Sonderregelung des Artikels 12 nicht für Datenübermittlungen nach Artikel 5 und 8 (vgl. Denkschrift des Abkommens, S. 14), sondern bezieht sich ausschließlich auf Spontanübermittlungen nach Artikel 10. Die Spontanübermittlung ist aber wegen ihres besonderen Charakters ausdrücklich nur auf den Zweck der Verhinderung terroristischer

straftaten begrenzt. Diese Zweckbeschränkung geht nicht aus Artikel 12 hervor.

- b) Schließlich sind auch die in Artikel 12 aufgezählten Datenkategorien zu weit gefasst. Diese entsprechen zwar dem Standardkatalog der allgemeinen Datenschutzgesetze (vgl. § 3 Absatz 9 BDSG). Dabei bleibt jedoch unberücksichtigt, dass die Zweckbestimmung dieser Gesetze wesentlich breiter gefasst ist. Artikel 12 zielt dagegen ausschließlich auf einen konkreten Zweck ab, nämlich die Verhinderung terroristischer Straftaten nach Artikel 10.

Insoweit ist festzustellen, dass zu dem konkreten Zweck der Verhinderung terroristischer Straftaten eine Übermittlung von Daten über die Mitgliedschaft in einer Gewerkschaft unter keinem Gesichtspunkt von Relevanz sein kann. Auch die Übermittlung von Daten über die Gesundheit bzw. das Sexualleben ist vor diesem Hintergrund bedenklich.
5. Darüber hinaus legt das Abkommen keine verbindlichen Lösungs- bzw. Prüffristen fest. Artikel 11 Absatz 2 des Abkommens sieht lediglich vor, die übermittelten Daten nur so lange aufzubewahren, als dies für den jeweiligen Zweck nötig ist. Für die polizeiliche und justizielle Zusammenarbeit innerhalb der Europäischen Union sind solche Fristen vorgegeben. Nach Artikel 5 des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 sind für die Löschung oder regelmäßige Überprüfung der Notwendigkeit der Speicherung Fristen festzulegen, deren Einhaltung durch verfahrensrechtliche Vorkehrungen sicherzustellen sind. Dadurch wird eine sachgerechte zeitliche Begrenzung der Datenspeicherung gewährleistet.
6. Schließlich fehlt eine verbindliche Definition der schwerwiegenden Kriminalität sowie der terroristischen Straftaten als Grundvoraussetzung für den Datenaustausch auf der Grundlage des Abkommens. Artikel 10 Absatz 3 des Abkommens sieht zwar eine Notifizierung der Straftaten vor. Diese kann jedoch jederzeit einseitig von den Vertragsparteien geändert werden.
7. Die Bundesregierung wird gebeten, bei der Durchführung des Abkommens auf die Einhaltung eines hohen Datenschutzniveaus hinzuwirken und die genannten Aspekte bei künftigen Verhandlungen zu berücksichtigen.

