LAW ENFORCEMENT

Cooperation

Agreement Between the
UNITED STATES OF AMERICA
and AUSTRIA

Signed at Vienna November 15, 2010

with

Annex

NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966 (80 Stat. 271; 1 U.S.C. 113)—

". . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof."

AUSTRIA

Law Enforcement: Cooperation

Agreement signed at Vienna
November 15, 2010;
Entered into force May 4, 2012,
with the exception of Articles 7 through 9.
In accordance with Article 27, Articles 7
through 9 may enter into force in the
future under conditions specified in Article 27.
With annex.

Agreement between the Government of the United States of America and the Government of the Republic of Austria On Enhancing Cooperation in Preventing and Combating Serious Crime

The Government of the United States of America and the Government of the Republic of Austria (hereinafter "Parties"),

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

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

Recognizing the importance of preventing and combating serious crime, particularly terrorism, while respecting fundamental rights and freedoms, notably privacy and the protection of personal data,

Recognizing the interest of the United States of America and the European Union in negotiating an agreement on data protection in the law enforcement context which might give rise to consultations regarding the potential impact of such an agreement on the provisions set forth below,

Inspired by the Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, done at Prüm on May 27, 2005, as well as the related decision of the Council of the European Union of June 23, 2008,

Taking into account the Principles on Privacy and Personal Data Protection for Law Enforcement Purposes elaborated by the EU-U.S. High Level Contact Group,

Recognizing the importance of establishing procedures between the Parties for correcting, blocking and deleting inaccurate personal data, and taking into account that such procedures should involve the competent authorities of the supplying Party, and

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

Have agreed as follows:

Article 1
Definitions

For the purposes of this Agreement,

1. DNA profiles shall mean a letter or numerical code representing a number of identifying features of the non-coding part of an analyzed 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 dactyloscopic data and the related reference (dactyloscopic reference data). Reference 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 recognizable as such.
3. Personal data shall mean any information relating to an identified or identifiable natural person (the "data subject").
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, organization, 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.
5. Blocking shall mean the marking of stored personal data with the aim of limiting their processing in future.
6. Terrorist Offense shall mean conduct punishable in accordance with an international instrument relating to the fight against terrorism which is in force for both Parties.
7. Serious crimes shall mean conduct constituting an offense punishable by a maximum deprivation of liberty of more than one year or a more serious penalty. To ensure compliance with their national laws, the Parties may agree to specify particular serious crimes for which a Party shall not be obligated to supply personal data as described in Articles 6 and 9 of the Agreement.

Article 2
Purpose and Scope of this Agreement

1. The purpose of this Agreement is to enhance the cooperation between the United States of America and the Republic of Austria in preventing and combating serious crime.
2. The querying powers provided for under this Agreement (Articles 4 and 7) shall be used only for the prevention, detection and investigation of a serious crime as defined in Article 1 paragraph 7 and only if particular and legally valid circumstances relating to a specific individual give a reason to inquire whether that individual will commit or has committed such a serious crime.

Article 3
Dactyloscopic data

For the purpose of implementing this Agreement, the Parties shall ensure the availability of reference data from those national automated dactyloscopic identification systems which were established for the prevention and investigation of criminal offenses. These systems and the extent of their application to this Agreement are listed in the Annex, which forms an integral part of this Agreement. Reference data shall only include dactyloscopic data and a reference.

Article 4
Automated querying of dactyloscopic 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 national automated dactyloscopic identification systems, which it has established for that purpose, with the power to conduct automated queries by comparing dactyloscopic data. Queries may be conducted only in individual cases and in compliance with the querying Party's national law.
2. The confirmation of a match of dactyloscopic data with reference data held by the Party in charge of the file shall be carried out by the querying 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 dactyloscopic 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 and shall be supplied in accordance with Article 6.

Article 6
National contact points and implementing agreements

1. For the purpose of the supply of data as referred to in Article 4, and the subsequent supply of further personal data as referred to in Article 5, each Party shall designate one or more national contact points. The contact point shall supply such data in accordance with the national law of the Party designating the contact point. Other available legal assistance channels need not be used unless necessary, for instance to authenticate such data for purposes of its admissibility in judicial proceedings of the requesting Party.
2. The technical and procedural details for the queries conducted pursuant to Article 4 shall be set forth in one or more implementing agreements.

Article 7
Automated querying 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 queries by comparing DNA profiles for the investigation of serious crime. Queries may be conducted only in individual cases and in compliance with the querying Party's national law.
2. Should an automated query show that a DNA profile supplied matches a DNA profile entered in the other Party's file, the querying 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 and shall be supplied in accordance with Article 9.

Article 9
National contact point and implementing agreements

1. For the purposes of the supply of data as set forth in Article 7, and the subsequent supply of further personal data as referred to in Article 8, each Party shall designate a national contact point. The contact point shall supply such data in accordance with the national law of the Party designating the contact point. Other available legal assistance channels need not be used unless necessary, for instance to authenticate such data for purposes of its admissibility in judicial proceedings of the requesting Party.
2. The technical and procedural details for the queries 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 serious criminal offenses of a transnational dimension and terrorist offenses

1. For the prevention of serious criminal offenses of a transnational dimension and terrorist offenses, the Parties may, in compliance with their respective national law, in individual cases concerning the interests of either Party, even without being requested to do so, supply the other Party's relevant national contact point, as referred to in paragraph 6, 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. will commit or has committed 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. is undergoing or has undergone training to commit the offenses referred to in subparagraph a; or
c. will commit or has committed a serious criminal offense of a transnational dimension, or participates in an organized criminal group or association.

2. The personal data to be supplied may 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 dactyloscopic data, as well as a description of any conviction or of the circumstances giving rise to the belief referred to in paragraph 1.
3. The supplying Party may, in compliance with its obligations under international law and its national law, impose conditions on the use that may be made of such data by the receiving Party. If the receiving Party accepts such data, it shall be bound by any such conditions.
4. Generic restrictions with respect to the legal standards of the receiving Party for processing personal data may not be imposed by the supplying Party as a condition under paragraph 3 to providing data.
5. In addition to the personal data referred to in paragraph 2, the Parties may provide each other with non-personal data related to the offenses set forth in paragraph 1.
6. 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
General Principles on 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
   a. processing personal data fairly and in accordance with their respective laws;
   b. ensuring that the personal data provided are accurate, up to date, adequate, relevant and not excessive in relation to the specific purpose of the transfer; and
   c. 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.
3. This Agreement sets forth the rights and obligations of the Parties concerning the use of personal data provided under this Agreement, including correction, blockage, and deletion of data pursuant to Article 14. This Agreement, however, shall not give rise to rights on the part of any private person. Rights of individuals existing independently of this Agreement, including rights concerning access to and correction, blockage, and deletion of data, are not affected.

4. Responsibility and powers for legal checks on the supply, receipt, processing, and recording of personal data rest with the independent data protection authorities or, where applicable, oversight bodies, privacy officers, and judicial authorities of the respective Parties as determined by their national law. The Parties shall notify each other of the authorities which shall act as focal points for the implementation of the data protection provisions of this Agreement.

Article 12

Additional Protection for 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 3, each Party may process data obtained under this Agreement only:
   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, given in accordance with the supplying Party's national law.
2. The Parties shall not communicate data provided under this Agreement to any third State, international body or private entity without the prior consent, appropriately documented, of the Party that provided the data and without the appropriate safeguards.
3. A Party may conduct an automated query of the other Party's dactyloscopic or DNA files under Articles 4 or 7, and process data received in response to such a query, including the communication whether or not a hit exists, solely in order to:
   a. establish whether the compared DNA profiles or dactyloscopic data match;
   b. prepare and submit a follow-up request for assistance in compliance with national law, including the legal assistance rules, if those data match; or
   c. conduct record-keeping, as required or permitted by its national law.
4. The Party administering the file may process the data supplied to it by the querying Party during the course of an automated query in accordance with Articles 4 and 7 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Article 15. The data supplied for comparison shall be deleted immediately following data comparison or automated replies to queries unless further processing is necessary for the purposes mentioned under this Article, paragraph 3, subparagraphs (b) or (c).

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 data received under this Agreement that are incorrect or incomplete, or if the collection or further processing of data received under this Agreement contravenes this Agreement or the rules applicable to the supplying Party in an individual case.
2. Where a Party becomes aware that data it has received from the other Party under this Agreement are not accurate, it shall take without undue delay all appropriate measures to safeguard against erroneous reliance on such data, which shall include in particular supplementation, deletion, or correction or, where appropriate as an additional measure, flagging.
3. Each Party shall notify the other without undue delay if it becomes aware that material data it has transmitted to the other Party or received from the other Party under this Agreement are inaccurate or unreliable or are subject to significant doubt.
4. Where there is reason to believe that deletion would prejudice the interests of the data subject or other persons concerned, the data shall be blocked instead of deleted in compliance with national law. Blocked data may be supplied or used solely for the purpose for which the data was retained. Blocked data may be used for any purpose under this Agreement if it is later determined to be accurate.

Article 15
Documentation

1. Each Party shall log every non-automated supply and every non-automated receipt of personal data by the body administering the file and the searching body for the purpose of verifying whether the supply is consistent with this Agreement. Logging shall contain the following:

    a. the reason for the supply;
    b. information on the data supplied;
    c. the date of the supply; and
    d. the name or reference of the searching body and the body administering the file.

2. The following shall apply to automated queries for data based on Articles 4 and 7:

    a. Only specially authorized officers of the national contact point may carry out automated queries. Each Party shall maintain records that allow it to identify the individuals initiating or carrying out such queries.
    b. Each Party shall ensure that each supply and receipt of personal data by the body administering the file and the searching body is recorded, including communication of whether or not a hit exists. Recording shall include the following:

        (i) information on the data supplied;

(ii) the date and time of the supply;
(iii) the name or reference of the searching body and the body administering the file; and
(iv) the reason for the query.

3. The data recorded pursuant to paragraphs 1 and 2 shall be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years. After the conservation period the recorded data shall 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 take measures to 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 querying of dactyloscopic 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. 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 queries are conducted.

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 Republic of Austria; or
c. the rights and freedoms of third parties.

Article 18
Verification

In addition to its rights under Article 14, a Party may request that the other Party's data protection or other competent authority according to Article 11 paragraph 4 shall verify that a specific individual's personal data transmitted under this Agreement has been processed in accordance with this Agreement. The authority receiving such a request shall respond in a timely manner to the other Party's competent authority.

Article 19
Requests of persons concerning access to and correction, blockage and deletion of data

Any person seeking information on the use of his or her personal data under this Agreement or exercising a right under national law to correct, block or delete such data may send a request to his or her data protection or other competent authority according to Article 11 paragraph 4 which, in accordance with its national law, shall proceed according to Article 14 paragraph 1 or Article 18.

Article 20
Information

1. The Parties shall inform each other about their national laws on the protection of personal data and of any changes in these laws relevant for the implementation of this Agreement.
2. 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 21
Relation to Other Agreements

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

Article 22
Consultations

1. The Parties shall consult each other regularly on the implementation of the provisions of this Agreement and, without prejudice to Article 26, on any relevant developments

on the EU-U.S. level concerning the protection of personal data in the law enforcement context.

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 23
Expenses

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

Article 24
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 25
Suspension

If either Party considers that the other Party has failed to fulfill an obligation under this Agreement or that developments in a Party's national law undermine the purpose and scope of this Agreement, in particular relating to the protection of personal data, it may suspend the operation of the Agreement in whole or in part. The suspension shall be notified to the other Party through diplomatic channels and shall have effect immediately upon receipt of such notification. The same procedure shall apply to an eventual lifting of a suspension.

Article 26
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 mutual consent of both Parties at any time.

Article 27
Entry into force

1. 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 any steps necessary to bring the Agreement into force.
2. 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 exchange shall occur if the laws of both Parties permit the type of DNA screening contemplated by Articles 7 through 9.

Done at Vienna, this 15th day of November, 2010, in duplicate, in the English and German languages, both texts being equally authentic.

For the Government of the United States of America:

For the Government of the Republic of Austria:

Annex

Automated dactyloscopic identification systems for the purpose of this Agreement are

a) for the Republic of Austria

The Austrian national automated dactyloscopic identification system established according to Section 75 of the Security Police Act (Sicherheitspolizeigesetz) or any comparable system replacing it, to the extent that dactyloscopic data were collected by Austrian law enforcement authorities.

b) for the United States of America

The Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System, or any comparable system replacing it.

Abkommen

zwischen

der Regierung der Republik Österreich

und

der Regierung der Vereinigten Staaten von Amerika

über

die Vertiefung der Zusammenarbeit bei der Verhinderung und

Bekämpfung schwerer Straftaten

Die Regierung der Republik Österreich und die Regierung der Vereinigten Staaten von Amerika (im Folgenden „die Vertragsparteien"),

geleitet von dem Wunsch, durch partnerschaftliche Zusammenarbeit schwere Straftaten, insbesondere den Terrorismus, wirksamer zu bekämpfen,

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

in Anerkennung der Bedeutung der Verhütung und Bekämpfung schwerer Straftaten, insbesondere des Terrorismus, bei gleichzeitiger Achtung der Grundrechte und Grundfreiheiten, insbesondere des Schutzes der Privatsphäre und personenbezogener Daten,

in Anerkennung des Interesses der Europäischen Union und der Vereinigten Staaten von Amerika ein Abkommen über den Datenschutz im Bereich der Strafverfolgung zu verhandeln, das zu Konsultationen betreffend die möglichen Auswirkungen eines solchen Abkommens auf die im folgenden vereinbarten Bestimmungen führen kann,

geleitet durch den Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, unterzeichnet in Prüm am 27. Mai 2005 und den damit zusammenhängenden Beschluss des Rates der Europäischen Union vom 23. Juni 2008,

unter Beachtung der von der EU-US Hochrangigen Kontaktgruppe ausgearbeiteten Prinzipien des Schutzes der Privatsphäre und der personenbezogenen Daten zu Strafverfolgungszwecken und

in Anerkennung der Wichtigkeit, Verfahren zwischen den Vertragsparteien zur Gewährleistung der Berichtigung, Sperrung und Löschung fehlerhafter personenbezogener Daten zu schaffen, und unter Berücksichtigung, dass die zuständigen Behörden der übermittelnden Vertragspartei in diese Verfahren eingebunden werden sollen,

im Bestreben, die Zusammenarbeit zwischen den Vertragsparteien im Geist der Partnerschaft zu verstärken und zu unterstützen,

sind wie folgt übereingekommen:

Artikel 1
Begriffsbestimmungen

Im Sinne dieses Abkommens bezeichnet der Ausdruck:

(1) DNA-Profile: einen Buchstaben- oder 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 (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");

(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 oder Löschen durch Unkenntlichmachen oder Vernichten von personenbezogenen Daten;

(5) Sperren: die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

(6) Terroristische Straftat: ein strafbares Verhalten im Sinne eines internationalen Übereinkommens zur Bekämpfung des Terrorismus, das für beide Vertragsparteien in Kraft ist;

(7) Schwere Straftaten: ein strafbares Verhalten, das mit einer Freiheitsstrafe von mehr als einem Jahr oder einer schwereren Strafe bedroht ist. Um die Einhaltung ihres innerstaatlichen Rechts sicherzustellen, können die Vertragsparteien besondere schwere Straftaten festlegen, für die eine Vertragspartei nicht verpflichtet ist, personenbezogene Daten gemäß Artikel 6 und 9 dieses Abkommens zu übermitteln.

Artikel 2
Zweck und Anwendungsbereich dieses Abkommens

(1) Zweck dieses Abkommens ist die Vertiefung der Zusammenarbeit zwischen der Republik Österreich und den Vereinigten Staaten von Amerika bei der Verhinderung und Bekämpfung schwerer Straftaten.

(2) Die unter diesem Abkommen eingeräumten Befugnisse zum Abruf (Artikel 4 und 7) dürfen nur zum Zwecke der Verhinderung, Aufdeckung und Ermittlung einer schweren Straftat gemäß Artikel 1 Ziffer 7 genutzt werden und nur wenn besondere und rechtsgültige Umstände in Bezug auf eine bestimmte Person Anlass zur Nachforschung geben, ob diese Person eine solche schwere Straftat begehen wird oder begangen hat.

Artikel 3
Daktyloskopische Daten

Zum Zweck der Umsetzung 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. Diese Systeme und der Umfang ihrer Anwendung für das Abkommen sind im Anhang angeführt, der einen integralen Bestandteil dieses Abkommens bildet. Fundstellendatensätze enthalten ausschließlich daktyloskopische Daten und eine Kennung.

Artikel 4

Automatisierter Abruf daktyloskopischer Daten

(1) Zur Verhinderung und Verfolgung von schweren Straftaten gestatten die Vertragsparteien den in Artikel 6 bezeichneten nationalen Kontaktstellen der anderen Vertragspartei auf die Fundstellendatensätze ihrer zu diesem Zweck eingerichteten automatisierten daktyloskopischen Identifizierungssysteme mit dem Recht zuzugreifen, diese automatisiert mittels eines Vergleichs der daktyloskopischen Daten abzurufen. Anfragen dürfen nur im Einzelfall und im Einklang mit dem innerstaatlichen Recht der abrufenden Vertragspartei erfolgen.

(2) Die endgültige Zuordnung eines daktyloskopischen Datums zu einem Fundstellendatensatz der Datei führenden Vertragspartei erfolgt durch die abrufende nationale Kontaktstelle 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 gemäß Artikel 4 erfolgt die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener und sonstiger Daten nach dem innerstaatlichen Recht einschließlich der Vorschriften über die Rechtshilfe der ersuchten Vertragspartei und wird in Übereinstimmung mit Artikel 6 übermittelt.

Artikel 6

Nationale Kontaktstellen und Durchführungsvereinbarungen

(1) Zur Durchführung der Datenübermittlungen gemäß Artikel 4 und für die anschließende Übermittlung weiterer personenbezogener Daten gemäß Artikel 5 benennt jede Vertragspartei eine oder mehrere nationale Kontaktstellen. Die nationale Kontaktstelle übermittelt diese Daten in Übereinstimmung mit dem innerstaatlichen Recht jener Vertragspartei, die die

Kontaktstelle eingerichtet hat. Andere verfügbare Rechtshilfekanäle müssen solange nicht verwendet werden, als dies notwendig ist, um zum Beispiel solche Daten zum Zweck der Zulassung in Strafverfahren der ersuchenden Vertragspartei zu authentifizieren.

(2) Die technischen und prozeduralen Einzelheiten eines gemäß 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 Grundlage der Gegenseitigkeit können die Vertragsparteien der gemäß Artikel 9 benannten nationalen Kontaktstelle der anderen Vertragspartei zum Zweck der Verfolgung schwerer Straftaten 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 im Einklang mit dem innerstaatlichen Recht der abrufenden Vertragspartei erfolgen.

(2) Wird im Zuge eines automatisierten Abrufs die Übereinstimmung eines übermittelten DNA-Profils 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 gemäß Artikel 7 erfolgt die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener und sonstiger Daten nach dem innerstaatlichen Recht einschließlich der Vorschriften über die Rechtshilfe der ersuchten Vertragspartei und wird in Übereinstimmung mit Artikel 9 übermittelt.

Artikel 9

Nationale Kontaktstelle und Durchführungsvereinbarungen

(1) Zur Durchführung der Datenübermittlungen gemäß Artikel 7 und der anschließenden Übermittlung weiterer personenbezogener Daten gemäß Artikel 8, benennt jede Vertragspartei eine nationale Kontaktstelle. Die nationale Kontaktstelle übermittelt diese Daten in Übereinstimmung mit dem innerstaatlichen Recht jener Vertragspartei, die die Kontaktstelle benannt hat. Andere verfügbare Rechtshilfekanäle müssen solange nicht verwendet werden, als dies notwendig ist, um zum Beispiel solche Daten zum Zweck der Zulassung in Strafverfahren der ersuchenden Vertragspartei zu authentifizieren.

(2) Die technischen und prozeduralen Einzelheiten eines gemäß Artikel 7 durchgeführten Abrufverfahrens werden in einer oder mehreren Durchführungsvereinbarungen geregelt.

Artikel 10

Übermittlung personenbezogener und anderer Daten zur Verhinderung schwerer Straftaten mit einer transnationalen Dimension und terroristischer Straftaten

(1) Die Vertragsparteien können zum Zweck der Verhinderung schwerer Straftaten mit einer transnationalen Dimension und terroristischer Straftaten der gemäß Absatz 6 benannten relevanten nationalen Kontaktstelle der anderen Vertragspartei im Einklang mit ihrem jeweiligen innerstaatlichen Recht in Einzelfällen, die die Interessen einer der Vertragsparteien betreffen, auch ohne Ersuchen die in Absatz 2 genannten personenbezogenen Daten übermitteln, soweit dies erforderlich ist, weil bestimmte Tatsachen die Annahme rechtfertigen, dass der oder die Betroffenen:

a. terroristische Straftaten oder Straftaten, die mit Terrorismus oder einer terroristischen Gruppe oder Vereinigung in Zusammenhang stehen, begehen werden oder begangen haben, soweit solche Straftaten nach dem innerstaatlichen Recht der übermittelnden Vertragspartei definiert sind, oder

b. eine Ausbildung zur Begehung der unter Buchstabe a genannten Straftaten durchlaufen oder durchlaufen haben oder

c. schwere Straftaten mit einer transnationalen Dimension begehen werden oder begangen haben oder an einer organisierten kriminellen Gruppe oder Vereinigung beteiligt sind.

(2) Die zu übermittelnden personenbezogenen Daten können, soweit vorhanden, Familienname, Vornamen, frühere Namen, andere Namen, Aliasnamen, abweichende Namensschreibweisen, Geschlecht, Geburtsdatum und Geburtsort, aktuelle und frühere Staatsangehörigkeiten, Reisepassnummer, Nummern anderer Ausweispapiere und Fingerabdruckdaten sowie die Darstellung jeder Verurteilung oder jeglicher Umstände, aus denen sich die Annahme nach Absatz 1 ergibt, umfassen.

(3) Die übermittelnde Vertragspartei kann im Einklang mit ihren Verpflichtungen, die sich aus dem Völkerrecht und ihrem innerstaatlichen Recht ergeben, Bedingungen für die Verwendung dieser Daten durch die empfangende Vertragspartei festlegen. Wenn die empfangende Vertragspartei die Daten annimmt, ist sie an diese Bedingungen gebunden.

(4) Allgemeine Einschränkungen in Bezug auf die rechtlichen Standards der empfangenden Vertragspartei für die Verarbeitung personenbezogener Daten können von der übermittelnden Vertragspartei nicht als Bedingung im Sinne des Absatzes 3 für die Übermittlung von Daten auferlegt werden.

(5) Zusätzlich zu den in Absatz 2 bezeichneten personenbezogenen Daten können die Vertragsparteien auch nicht personenbezogene Daten, die zu den in Absatz 1 angeführten Straftaten in Bezug stehen, übermitteln.

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

Artikel 11

Allgemeine Prinzipien des Datenschutzes

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

(2) Die Vertragsparteien verpflichten sich

a. personenbezogene Daten nach Treu und Glauben und gemäß ihren jeweiligen Rechtsvorschriften zu verarbeiten;

b. sicherzustellen, dass die bereitgestellten personenbezogenen Daten richtig, aktuell, angemessen und relevant sind sowie nicht über den konkreten Zweck der Übermittlung hinausgehen;

c. die personenbezogenen Daten nur so lange aufzubewahren, als dies für den Zweck, zu dem die Daten in Übereinstimmung mit diesem Abkommen bereitgestellt oder weiter verarbeitet wurden, nötig ist.

(3) Dieses Abkommen regelt die Rechte und Pflichten der Vertragsparteien in Bezug auf den Gebrauch personenbezogener Daten einschließlich der Berichtigung, Sperrung und Löschung gemäß Artikel 14. Privatpersonen erwachsen jedoch keine Rechte aus diesem Abkommen. Unabhängig von diesem Abkommen bestehende Rechte von Privatpersonen, einschließlich des Rechts auf Auskunft und des Rechts auf Berichtigung, Sperrung und Löschung von Daten, bleiben unberührt.

(4) Die Zuständigkeit und die Befugnisse für rechtliche Kontrollen der Übermittlung, des Empfangs, der Verarbeitung und der Speicherung von personenbezogenen Daten obliegen gemäß den Vorschriften ihres innerstaatlichen Rechts den unabhängigen Datenschutzbehörden oder, wo anwendbar, den Aufsichtsbehörden, den Datenschutzbeamten und den gerichtlichen Behörden der jeweiligen Vertragspartei. Die Vertragsparteien benennen jene Behörden, die als Kontaktstellen für die Umsetzung der Datenschutzbestimmungen dieses Abkommens eingesetzt werden.

Artikel 12

Zusätzlicher Schutz bei der 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 oben genannten Kategorien personenbezogener Daten treffen die Vertragsparteien geeignete Schutzvorkehrungen, insbesondere geeignete Sicherheitsmaßnahmen, um solche Daten zu schützen.

Artikel 13

Verwendungsbeschränkungen zum Schutz personenbezogener
und sonstiger Daten

(1) Unbeschadet des Artikels 10 Absatz 3 darf jede Vertragspartei Daten, die sie nach diesem Abkommen gewonnen hat, nur 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; oder

d. für jeden anderen Zweck, jedoch nur mit der vorherigen Zustimmung der Vertragspartei, die die Daten übermittelt hat, in Übereinstimmung mit dem innerstaatlichen Recht der übermittelnden Vertragspartei.

(2) Die Vertragsparteien geben Daten, die nach diesem Abkommen bereitgestellt wurden, nicht ohne die vorherige, in geeigneter Weise dokumentierte Zustimmung der Vertragspartei, die die Daten bereitgestellt hat und ohne geeignete Schutzvorkehrungen an Drittstaaten, internationale Organe oder Private weiter.

(3) Eine Vertragspartei darf in den daktyloskopischen Dateien oder DNA-Dateien der anderen Vertragspartei einen automatisierten Abruf gemäß 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, ausschließlich 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 im Einklang mit dem innerstaatlichen Recht einschließlich der Vorschriften über die Rechtshilfe vorzubereiten und zu übermitteln oder

c. die Protokollierung durchzuführen, soweit diese durch das innerstaatliche Recht verlangt wird oder zulässig ist.

(4) Die Datei führende Vertragspartei darf die ihr gemäß den Artikeln 4 und 7 von der abrufenden Vertragspartei im Zuge eines automatisierten Abrufs übermittelten Daten ausschließlich verarbeiten, soweit dies zur Durchführung des Abgleichs, zur automatisierten Beantwortung der Anfrage oder zur Protokollierung gemäß 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 Absatz 3 Buchstaben b und c dieses Artikels genannten Zwecken erforderlich ist.

Artikel 14

Berichtigung, Sperrung und Löschung von Daten

(1) Auf Verlangen der übermittelnden Vertragspartei ist die empfangende Vertragspartei verpflichtet, Daten, die sie gemäß diesem Abkommen erlangt hat, zu berichtigen, zu sperren oder zu löschen, wenn sie unrichtig oder unvollständig sind oder ihre Erhebung oder Weiterverarbeitung im Einzelfall 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 gemäß diesem Abkommen erhalten hat, unrichtig sind, ergreift sie ohne unnötigen Aufschub alle geeigneten Maßnahmen zum Schutz vor fälschlichem Vertrauen auf diese Daten; dies umfasst insbesondere die Ergänzung, Löschung oder Berichtigung oder, wenn zweckdienlich, als zusätzliche Maßnahme die Kennzeichnung solcher Daten.

(3) Stellt eine Vertragspartei fest, dass wesentliche Daten, die sie gemäß 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 ohne unnötigen Aufschub mit.

(4) Wenn es Grund zur Annahme gibt, dass durch eine Löschung Interessen des Betroffenen oder anderer betroffener Personen beeinträchtigt werden, sind diese Daten in Übereinstimmung mit dem innerstaatlichen Recht zu sperren anstatt zu löschen. Gesperrte Daten dürfen nur für den Zweck, für den die Löschung unterblieben ist, übermittelt oder genutzt werden. Gesperrte Daten können für jegliche Zwecke gemäß diesem Abkommen verwendet werden, wenn später festgestellt wird, dass sie richtig sind.

Artikel 15

Dokumentation

(1) Jede Vertragspartei gewährleistet, dass jede nicht automatisierte Übermittlung und jeder nicht automatisierte Empfang von personenbezogenen Daten durch die die Datei führende

Stelle und die anfragende Stelle zur Kontrolle der Zulässigkeit der Übermittlung gemäß diesem Abkommen dokumentiert werden. Die Dokumentation umfasst folgende Angaben:

a. den Anlass der Übermittlung,

b. Informationen über die übermittelten Daten,

c. das Datum der Übermittlung und

d. die Bezeichnung oder Kennung der anfragenden und der Datei führenden Stelle.

(2) Für den automatisierten Abruf der Daten auf Grund der Artikel 4 und 7 gilt Folgendes:

a. Der automatisierte Abruf darf nur durch eigens ermächtigte Beamte der nationalen Kontaktstellen erfolgen. Jede Vertragspartei führt Aufzeichnungen, die es ermöglichen, jene Person zu identifizieren, die den automatisierten Abruf veranlasst oder durchgeführt hat.

b. Jede Vertragspartei gewährleistet, dass jede Übermittlung und jeder Empfang von Daten von der Datei führenden Stelle und der anfragenden Stelle protokolliert werden, einschließlich der Mitteilung des Vorliegens oder Nichtvorliegens eines Treffers. Die Protokollierung umfasst folgende Angaben:

(i) Informationen über die übermittelten Daten;

(ii) das Datum und den Zeitpunkt der Übermittlung;

(iii) die Bezeichnung oder Kennung der anfragenden und der Datei führenden Stelle; und

(iv) den Grund für den Abruf.

(3) Daten, die gemäß Absatz 1 und 2 protokolliert werden, sind durch geeignete Maßnahmen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen und zwei Jahre aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unverzüglich zu

löschen, sofern dies nicht dem innerstaatlichen Recht, einschließlich der anwendbaren Datenschutz- und Aufbewahrungsvorschriften, widerspricht.

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, Veränderung, Zugang oder jede unbefugte Form der Verarbeitung zu schützen. Insbesondere gewährleisten die Vertragsparteien, dass nur eigens 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 gemäß 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,

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.

Artikel 17

Transparenz – Bereitstellen von Information an die Betroffenen

(1) Dieses Abkommen ist nicht so auszulegen, dass dadurch die sich aus ihren jeweiligen Rechtsvorschriften ergebenden 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 und 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 über das Recht, Rechtsmittel einzulegen, soweit solche weiteren Informationen notwendig sind, um unter Berücksichtigung der Zwecke und konkreten Umstände, unter denen die Daten verarbeitet werden, gegenüber dem Betroffenen eine Verarbeitung nach Treu und Glauben 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 Republik Österreich oder der zuständigen Behörden in den Vereinigten Staaten von Amerika, oder

c. die Rechte und Freiheiten Dritter

durch die Bereitstellung dieser Informationen gefährdet würden.

Artikel 18
Überprüfung

Zusätzlich zu ihren Rechten gemäß Artikel 14 kann eine Vertragspartei von der Datenschutzbehörde oder einer anderen zuständigen Behörde der anderen Vertragspartei verlangen, dass diese gemäß Artikel 11 Absatz 4 überprüft, ob die personenbezogenen Daten eines bestimmten Betroffenen, die auf Grund dieses Abkommens übermittelt wurden, in Übereinstimmung mit diesem Abkommen verarbeitet wurden. Die Behörde, die einen solchen Antrag erhält, hat der zuständigen Behörde der anderen Vertragspartei zügig zu antworten.

Artikel 19

Antrag von Personen auf Zugang zu und Berichtigung, Sperrung und Löschung von Daten

Jede Person, die Informationen über die Nutzung ihrer personenbezogenen Daten gemäß diesem Abkommen verlangt oder das ihr gemäß den innerstaatlichen Gesetzen zustehende Recht auf Berichtigung, Sperrung oder Löschung solcher Daten ausüben will, kann einen Antrag an ihre Datenschutzbehörde oder eine andere zuständige Behörde gemäß Artikel 11 Absatz 4 richten, die in Übereinstimmung mit ihrem innerstaatlichen Recht gemäß Artikel 14 Absatz 1 oder Artikel 18 vorzugehen hat.

Artikel 20

Unterrichtung

(1) Die Vertragsparteien unterrichten einander über ihre innerstaatlichen Gesetze zum Schutz personenbezogener Daten und jede Änderung dieser Gesetze, die für die Umsetzung dieses Abkommens von Bedeutung sind.

(2) 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 zügig mitgeteilt wird.

Artikel 21

Verhältnis zu anderen Verträgen

Dieses Abkommen ist nicht so auszulegen, dass es Bestimmungen irgendeines anderen Vertrags, sonstigen Abkommens, von bestehenden Absprachen im Bereich der Strafverfolgung oder des innerstaatlichen Rechts, die den Austausch von Informationen zwischen der Republik Österreich und den Vereinigten Staaten von Amerika zulassen, beschränkt oder beeinträchtigt.

Artikel 22

Konsultationen

(1) Die Vertragsparteien konsultieren einander regelmäßig über die Umsetzung der Bestimmungen dieses Abkommens und, unbeschadet des Artikel 26, über jegliche maßgeblichen Entwicklungen auf der EU-US Ebene hinsichtlich des Schutzes personenbezogener Daten im Bereich der Strafverfolgung.

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

Artikel 23

Kosten

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

Artikel 24

Kündigung des Abkommens

Dieses Abkommen kann von jeder Vertragspartei unter Einhaltung einer dreimonatigen Kündigungsfrist schriftlich gekündigt werden. Auf die vor der Kündigung übermittelten Daten finden die Bestimmungen dieses Abkommens weiterhin Anwendung.

Artikel 25

Aussetzung

Wenn eine der Vertragsparteien der Ansicht ist, dass die andere Vertragspartei ihren Verpflichtungen auf Grund dieses Abkommens nicht nachgekommen ist oder wenn

Entwicklungen im innerstaatlichen Recht einer der Vertragsparteien den Zweck und den Anwendungsbereich dieses Abkommens, insbesondere in Bezug auf den Schutz personenbezogener Daten, untergraben, kann sie die Anwendung des Abkommens oder von Teilen des Abkommens aussetzen. Die Aussetzung ist der anderen Vertragspartei im diplomatischen Wege mitzuteilen und wird sofort mit Einlangen der Mitteilung wirksam. Dasselbe Verfahren ist bei einer möglichen Aufhebung der Aussetzung anzuwenden.

Artikel 26
Änderungen

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

(2) Dieses Abkommen kann jederzeit im gegenseitigen schriftlichen Einvernehmen beider Vertragsparteien geändert werden.

Artikel 27
Inkrafttreten

(1) Dieses Abkommen tritt, mit Ausnahme der Artikel 7 bis 9, an dem Tag des Eingangs der späteren Note in Kraft, die das Verfahren im diplomatischen Wege abschließt, mit dem die Vertragsparteien einander mitteilen, dass sie jegliche für das Inkrafttreten des Abkommens erforderlichen Schritte gesetzt haben.

(2) 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 späteren Note in Kraft, die das Verfahren im diplomatischen Wege zwischen den Vertragsparteien abschließt, mit dem festgestellt wird, dass jede Vertragspartei in der Lage ist, diese Artikel auf der Grundlage der Gegenseitigkeit durchzuführen. Dies erfolgt, wenn das Recht beider Vertragsparteien den DNA-Datenaustausch gemäß den Artikeln 7 bis 9 erlaubt.

Geschehen zu Wien am 15. November 2010 in zwei Urschriften, jede in deutscher und englischer Sprache, wobei jeder Wortlaut gleichermaßen authentisch ist.

Für die Regierung der
Vereinigten Staaten von Amerika

Für die Regierung der
Republik Österreich

Anhang

Gemäß Artikel 3 dieses Abkommens sind automatisierte daktyloskopische Identifizierungssysteme:

a) Für die Republik Österreich

Das österreichische nationale Automatisierte Fingerabdruckidentifizierungssystem, das auf der Grundlage des § 75 des Sicherheitspolizeigesetzes eingerichtet wurde oder jedes vergleichbare System, das es ersetzen wird, für jene daktyloskopischen Daten, die von österreichischen Sicherheitsbehörden gesammelt wurden.

b) Für die Vereinigten Staaten von Amerika

Das *Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System* oder jedes vergleichbare System, das es ersetzen wird.