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

The Government of the Republic of Austria and the Government of the United States of America (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 European Union and the United States of America 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 Republic of Austria and the United States of America 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 Republic of Austria or by the competent authorities in the United States of America; 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 Republic of Austria and the United States of America.

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 agreement of the 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 15 day of November 2010, in duplicate in the German and English languages, both texts being equally authentic.

For the Government of the Republic of Austria:	For the Government of the United States of America:
Elisabeth Tichy-Fisslberger m.p.	William Carlton Eacho m.p.

Annex

Pursuant to Article 3, 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 system of the same scope 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 system of the same scope replacing it.