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

The Government of the United States of America and the Government of Malta (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,

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 June 18, 2007 European Council decision, 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. Criminal justice purpose shall include activities defined as the administration of criminal justice, which means the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation activities of accused persons or criminal offenders. The administration of criminal justice also includes criminal identification activities.
2. DNA profiles (DNA identification patterns) 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.
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. 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 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.
6. Serious crimes shall mean, for purposes of implementing this Agreement, 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 of this Agreement

The purpose of this Agreement is to enhance the cooperation between the United States and Malta in preventing and combating 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 querying 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 7, access to the reference data in the automated fingerprint identification system, which it has established for that purpose, with the power to conduct automated queries by comparing fingerprinting data. Queries may be conducted only in individual cases and in compliance with the querying Party's national law.
2. Comparison of fingerprinting 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.
3. When needed, further analysis for the purpose of confirming a match of the fingerprinting data with reference data held by the Party in charge of the file shall be carried out by the requested national contact points.

Article 5
Alternative means to query using identifying data

1. Until Malta has a fully operational and automated fingerprint identification system that links to individual criminal records and is prepared to provide the United States with automated access to such a system, for a criminal justice purpose related to serious crime, it shall compare expeditiously fingerprinting reference data or other identifying data provided by the United States in order to establish clear matches and shall expeditiously communicate whether or not the comparison results in a clear match. Such requests shall be made by the United States only in individual cases and in compliance with its domestic law.
2. The querying powers provided for under this Agreement shall be used only for a criminal justice purpose, including when applied at the border where an individual for whom the additional data is sought has been identified for further inspection.

Article 6
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.

Article 7
National contact points and implementing agreements

1. For the purpose of the supply of data as referred to in Articles 4 and 5, each Party shall designate one or more national contact points. The powers of the contact points shall be governed by the national law of the Party designating the contact point.
2. The technical and procedural details for the queries conducted pursuant to Articles 4 and 5 shall be set forth in one or more implementing agreements or arrangements.

Article 8
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 10, 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 made 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 9
Supply of further personal and other data

Should the procedure referred to in Article 8 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 10
National contact point and implementing agreements

1. For the purposes of the supply of data as set forth in Article 8, each Party shall designate a national contact point. The powers of the contact point shall be governed by the national law of the Party designating the contact point.
2. The technical and procedural details for the queries conducted pursuant to Article 8 shall be set forth in one or more implementing agreements or arrangements.

Article 11
Supply of personal and other data in order to prevent serious criminal and terrorist offenses

1. For the prevention of serious criminal and 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 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, or participates in an organized criminal group or association.
2. The personal data to be supplied should 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 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 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 transmitting 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 12
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 are 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 are 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 existing independently of this Agreement, however, are not affected.

Article 13
Limitation on processing to protect personal and other data

1. Without prejudice to Article 11, paragraph 3, each 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 query of the other Party's fingerprint or DNA files under Articles 4 or 8, 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 fingerprint 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.

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 8 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 searches 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, consistent with its national law, data received under this Agreement that are 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 are 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 are inaccurate or unreliable or are 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. information on the data supplied;
   b. the date of supply; and

c. the recipient of the data in case the data are 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 reasonably take measures to ensure that only those authorized to access personal data can have access to such data.

2. The implementing agreements or arrangements that govern the procedures for automated querying of fingerprint and DNA files pursuant to Articles 4 and 8 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 or by the competent authorities in Malta; 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 treaty, other agreement, working law enforcement relationship, or domestic law allowing for information sharing between the United States and Malta.

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 may agree on different arrangements.

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

1. This Agreement shall enter into force, with the exception of Articles 8 through 10, 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 8 through 10 of this Agreement shall enter into force following the conclusion of the implementing agreement(s) or arrangement(s) referenced in Article

10 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 8 through 10.

Done at Washington, this 3rd day of October 2008, in duplicate, in the English language.

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:

Richard C. Barth
Department of Homeland Security

Department of State

FOR THE GOVERNMENT OF MALTA: