

AGREEMENT
BETWEEN
THE PORTUGUESE REPUBLIC
AND
THE UNITED STATES OF AMERICA
ON ENHANCING COOPERATION IN PREVENTING AND
COMBATING CRIME

The Portuguese Republic and the United States of America, hereinafter referred to as “The Parties”,

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

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

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

Following the example of the Treaty of Prüm on enhancing cross-border cooperation, and seeking to enhance and encourage cooperation between the Parties in the spirit of partnership;

Bearing in mind the Instrument between the Portuguese Republic and the United States of America as contemplated by Article 3 (3) of the Agreement on Mutual Legal Assistance between the European Union and the United States of America signed 25 June 2003, signed at Washington, on 14 July 2005,

Agree as follows:

Article 1

Definitions

For the purposes of this Agreement:

- 1) “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;
- 2) “Reference data” shall mean a DNA profile and the related reference (DNA reference data) or fingerprinting data and the related reference (fingerprinting reference data), that cannot contain any data from which the data subject can be directly identified and must be recognizable as such when not traceable to any individual (untraceables);
- 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.

Article 2

Purpose and scope of this Agreement

1. The purpose of this Agreement is to enhance the cooperation between the Parties in preventing and combating crime.
2. The querying powers provided for under this Agreement shall be used only for the prevention, detection, repression, and investigation of crime.
3. The scope of this Agreement shall encompass crimes constituting an offence punishable under the domestic law of the Parties by a maximum deprivation of liberty of more than one year more serious penalty.

Article 3

Fingerprinting data

1. 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.
2. Reference data shall only include fingerprinting data and a reference.

Article 4

Automated querying of fingerprint data

1. For the prevention and investigation of 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.
2. Queries may be conducted only in individual cases and in compliance with the querying Party's national law.
3. Firm matching 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.

4. 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 the Portuguese Republic has a fully operational and automated fingerprint identification system that links to individual criminal records or is otherwise prepared to provide the United States of America with automated access to such a system, it shall provide an alternative means to conduct a query using other identifying data to determine a clear match linking the individual to additional data.
2. Query powers shall be exercised in the same manner as provided in Article 4 and a clear match will be treated the same as a firm match of fingerprinting data to allow for the supply of additional data as provided for in Article 6.
3. The querying powers provided for under this Agreement shall be used only as provided for under Article 2(2), 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 documents

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.

2. The powers of the contact points shall be governed by the national law applicable.
3. The technical and procedural details for the querying conducted pursuant to Articles 4 and 5 shall be set forth in one or more implementing documents.

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 comparing DNA profiles for the investigation of crime.
2. Queries may be made only in individual cases and in compliance with the querying Party's national law.
3. 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.
4. Should no match be found, automated notification of this shall be given as well.

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 documents

1. For the purposes of the supply of data as set forth in Article 8, each Party shall designate a national contact point.

2. The powers of the contact point shall be governed by the national law applicable.
3. The technical and procedural details for the queries conducted pursuant to Article 8 shall be set forth in one or more implementing documents.

Article 11

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

1. For the prevention of terrorist and criminal 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;
- b) Is undergoing or has undergone training to commit the offenses referred to in subparagraph a); or
- c) Will commit or has committed a criminal offence, or participates in an organized criminal group or association.

2. The personal data to be supplied shall include, if available, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, nationality, 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 made of such data by the receiving Party.

4. If the receiving Party accepts such data, it shall be bound by any such conditions.

5. Where additional conditions have been imposed in a particular case the requested Party may require the requesting Party to give information on the use made of the evidence or information.

6. Generic restrictions with respect to the legal standards of the receiving Party for processing personal data may not be imposed by the sending Party as a condition under the previous paragraphs to providing data.

7. 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.

8. 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.

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

3. This Agreement shall not give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data nor expand or limit rights otherwise available under domestic law.

Article 13

Limitation on processing to protect personal and other data

1. Without prejudice to Article 11, paragraphs 3, 4 and 5, the Parties may process data obtained under this Agreement:

- a) For the purpose of its criminal investigations;
- b) For preventing a 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 authorization 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, private entity or private person, without the prior authorization 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.

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 8 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Article 15.

5. 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, consistent with its national law, data received under this Agreement that is incorrect or incomplete or if its collection or further processing contravenes this Agreement or the rules applicable to the supplying Party.
2. Where a Party becomes aware that data it has received from the other Party under this Agreement is not accurate, it shall take all appropriate measures to safeguard against erroneous reliance on such data, which shall include in particular supplementation, deletion, or correction of such data.
3. Each Party shall notify the other if it becomes aware that material data it has transmitted to the other Party or received from the other Party under this Agreement is inaccurate or unreliable or is subject to significant doubt.

Article 15

Record keeping

1. Each party shall maintain a record of the transmission and receipt of data communicated to the other Party under this Agreement.
2. The record of the transmission and receipt of data 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.
3. The record shall include namely:
 - a) Information on the data supplied;
 - b) The date of supply; and

- c) The recipient of the data in case the data is supplied to other entities.
- 4. The recorded data must be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years.
- 5. 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.
- 6. According to their national law, responsibility for legal checks on the supply, receipt, processing, and recording of personal data lies with the independent data protection authorities or, where applicable, oversight bodies, privacy officers, or judicial authorities of the respective Parties.

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.
- 2. The Parties in particular shall reasonably take measures to ensure that only those authorized to access personal data can have access to such data.
- 3. The implementing documents that govern the procedures for automated queries 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;
 - c) For a mechanism to ensure that only permissible queries are conducted.

Article17

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 consistent with national law, 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 of the Parties; or
- c) The rights and freedoms of third parties.

Article 18

Information

1. Upon request, the receiving Party shall inform the supplying Party of the processing of supplied data and the result obtained.

2. The receiving Party shall ensure that its answer is communicated to the supplying Party in a timely manner.

Article 19

Expenses

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

Article 20

Relation to Other Agreements

Nothing in this Agreement shall be construed to limit or prejudice the provisions of any existing treaty or agreement applicable to the Parties.

Article 21

Consultations

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

Article 22

Settlement of disputes

Any dispute concerning the interpretation or application of the present Agreement shall be resolved by consultations between the Parties and shall not be referred to any third party for settlement.

Article 23

Amendments

1. This Agreement may be amended by written agreement of the Parties.
2. Any such amendments shall enter into force in accordance with the terms specified in Article 25(1).

Article 24

Duration and Termination

1. The present Agreement shall remain in force for an indefinite period of time.
2. Either Party may, at any time, terminate this Agreement by notification in writing through the diplomatic channels.
3. This Agreement shall terminate three months after the date of such notification.
4. The provisions of this Agreement shall continue to apply to data supplied prior to such termination.

Article 25

Entry into force

1. This Agreement shall enter into force, with the exception of Articles 8 through 10, on the date of the later of the written notifications between the Parties, through the diplomatic channels, conveying the completion of the internal procedures of each Party required for that purpose.
2. Articles 8 through 10 of this Agreement shall enter into force following the conclusion of the implementing documents referenced in Article 10 and on the date of the later of the written notifications, between the Parties through the diplomatic channels, conveying that each Party is able to implement those articles on a reciprocal basis.
3. The exchange referenced in paragraph 2 shall occur only if the laws of both parties permit the type of DNA screening contemplated by Articles 8 to 10.

Article 26

Registration

This Agreement shall be registered with the United Nations in accordance with Article 102 of the Charter of the United Nations.

Done in Lisbon, on the 30th of June of 2009, in duplicate in the Portuguese and English languages, both texts being equally authentic.

FOR THE PORTUGUESE REPUBLIC

FOR THE UNITED STATES OF
AMERICA

RUI PEREIRA
MINISTRY OF INTERIOR

JANET NAPOLITANO
STATE SECRETARY FOR
HOMELAND SECURITY

ALBERTO COSTA
MINISTRY OF JUSTICE