

Agreement

between

the Swiss Confederation

and

the United States of America

On Enhancing Cooperation in Preventing and Combating Serious Crime

The Swiss Confederation and the United States of America (hereinafter the “Parties”),

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

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

Recognizing the importance of preventing and combating serious crime, particularly organized crime and terrorism, while respecting fundamental rights and freedoms under the applicable laws and international obligations of the respective parties, including those concerning privacy and the protection of personal data,

Recognizing the importance of maintaining a high standard of protection of personal data, particularly the importance of establishing procedures between the Parties for correction, blocking and deleting inaccurate personal data exchanged pursuant to this Agreement,

Taking into account the Arrangement between the Federal Department of Justice and Police and the Department of Justice of the United States of America, acting on behalf of the competent law enforcement authorities of the Swiss Confederation and the United States of America on the employment of joint investigation teams in the fight against terrorism and its financing, signed on July 12, 2006,

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 (Treaty of Prüm), and noting the related Council decisions 2008/615/JHA and 2008/616/JHA of June 23, 2008, on the integration of the Treaty of Prüm in the framework of the European Union,

Recognizing the obligations of the Swiss Confederation under the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and under the Agreement of October 26, 2004, between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation’s association with the implementation, application and development of the Schengen Acquis (Schengen association agreement), 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. Serious crimes shall mean offenses set forth in the Annex to this Agreement, and other acts punishable by a period of deprivation of liberty of more than three years.

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 investigating serious crime by police and justice authorities.
2. The powers for queries of dactyloscopic data and DNA profiles provided for under this Agreement (Articles 4 and 6) shall be used only for the prevention and investigation of a serious crime as defined in Article 1 paragraph 6 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.

3. A request for supply of further personal data and other information in accordance with Articles 5 and 7 will be granted only if the act described in the request involves a serious crime under the law of the requested Party.

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. 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 9, 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 data and other information

Should the procedure referred to in Article 4 show a match between dactyloscopic data, the supply of any available further personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Party. The supply shall be carried out in accordance with Articles 9 and 11.

Article 6

Automated querying of DNA profiles

1. If permissible under the national law of both Parties and if in practice possible for both Parties and only after the implementing arrangements have been finalized, 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 prevention and 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 shall be given.

Article 7

Supply of further personal data and other information

Should the procedure referred to in Article 6 show a match between DNA profiles, the supply of any available further personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Party. The supply shall be carried out in accordance with Articles 9 and 11.

Article 8

Alternative means to query DNA files

Until the notification contemplated by Article 29, paragraph 2, is made, each Party may conduct, at the request of the other Party, a search of its own DNA databases in accordance with its own law and technical requirements.

Article 9

National contact points

For the purpose of the supply of data and other information as referred to in Articles 4 to 8, each Party shall designate one national contact point for supplies of data as referred to in Articles 6 and 7 as well as one or more national contact points for supplies of data referred to in Articles 4 and 5. Each contact point shall supply such data in accordance with its national law.

Article 10

Quotas

The Parties shall consult for the purpose of establishing appropriate limits on the number of queries they will make in accordance with Articles 4 to 7 and include these limits in the implementing arrangements.

Article 11

Implementing arrangements

The technical and procedural details for queries and the supply of data conducted pursuant to this Agreement shall be set forth in one or more implementing arrangements.

Article 12

Supply of personal data and other information in order to prevent serious criminal offenses and activities related to terrorism

1. The Parties may, in accordance with their national law, case by case, even without being requested to do so, transmit to the relevant national contact point of the other Party, as referred to in paragraph 4 of the present Article, the personal data and other information mentioned in paragraph 2 of the present Article, in order to prevent offenses that represent a serious threat to the public interest and in so far as it is necessary because special circumstances give reason to believe that the person concerned is likely to commit offenses linked to terrorism, or offenses linked to a terrorist group or conspiracy, or offenses linked to serious crime as defined by the national law of the Party transmitting the data.
2. The data that may be transmitted pursuant to paragraph 1 may comprise last names, first names, date and place of birth and also a description of the circumstances that gave rise to the suspicion mentioned in paragraph 1 of this Article.
3. The transmitting Party may, in pursuance of its national law, stipulate conditions on a case by case basis as to the use of this data by the receiving Party. If the receiving Party accepts the said data, that Party shall abide by all the conditions. Generic restrictions with respect to the legal standards of the receiving Party for processing personal data and other information may not be imposed by the transmitting Party as a condition under this paragraph to providing data. In addition to the personal data mentioned in paragraph 2 of the present Article, the Parties may transmit to each other non-personal data in connection with the offenses mentioned in paragraph 1 of the present Article.

4. Each Party shall designate one or more national contact point(s) for the purpose of exchanging personal data and other information with the other Party's contact point(s) under the terms of this Article. The powers and responsibilities of the national contact points shall be defined by their respective national laws.

Article 13

General principles on the protection of personal data

1. The Parties provide in their respective national law a high standard of data protection in order to preserve confidence in the implementation of this Agreement.
2. The Parties commit themselves to processing personal data fairly and in accordance with their respective laws, and in particular:
 - a. Processing personal data only if relevant, appropriate and not excessive in relation to its purpose;
 - b. ensuring that the personal data provided are accurate, up to date, and adequate; 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 16. 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 as referenced in Article 21, 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 contact points for the implementation of the data protection provisions of this Agreement.

Article 14

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, on the balance of interests, particularly relevant for the purposes of this Agreement and are only transmitted pursuant to Articles 5, 7, or 12 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 15

Limitation on processing to protect personal data and other information

1. Without prejudice to Article 12, paragraph 3, each Party shall 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 and international organizations without the prior explicit and appropriately documented 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 dactyloscopic or DNA files under Articles 4 or 6 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 6 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Article 17. The data supplied for comparison must 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 16

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, supply, 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 immediately take 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 immediately if it becomes aware that relevant 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.
5. The Parties shall provide for the orderly disposal of personal information at specific retention periods set forth under their respective domestic laws. These retention periods shall reflect appropriate operational considerations, the public interest, the type of data, the purpose of the processing or use, and privacy interests of affected persons

Article 17

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 6:
 - 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 record of every supply and receipt of personal data 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 record shall be deleted immediately, unless this is inconsistent with national law.

Article 18

Data security

1. The Parties shall ensure that the necessary technical measures and organizational arrangements are utilized to protect personal data and other information 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 and other information can have access to such data.
2. The implementing arrangements according to Article 11 that govern the procedures for automated querying of dactyloscopic and DNA files pursuant to Articles 4 and 6 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 19

Transparency – providing information to the data subjects

1. This Agreement is without prejudice to 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 of the Parties or
 - c. the rights and freedoms of third parties.

Article 20

Verification

In addition to its rights under Article 16, a Party may request that the other Party's data protection or other competent authority referenced in Article 13, paragraph 4, 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 21

Requests of persons concerning access to and correction, blockage and deletion of data, and redress procedures

1. At the request of the data subject under national law for information on data processed within the scope of this Agreement in respect to his person, the Party receiving the request shall respond in accordance with its national law.
2. Any person seeking information on the use of his or her personal data processed within the scope of 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 referenced in Article 13, para-

graph 4. Such authority shall proceed according to Article 16 or Article 20 and in accordance with its national law.

3. The Parties shall ensure that procedures are in place for any data subjects concerned to have appropriate redress for infringement of applicable data protection rights.
4. The relevant procedures for access, correction, blockage, deletion and redress shall be governed by the national law of the Party where the data subject asserts its rights.

Article 22

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.
3. The Parties shall make best efforts to inform each other about requests received from data subjects according to Article 21 of this Agreement.

Article 23

Relation to other agreements

This Agreement is without prejudice to the rights and obligations of the Parties under international agreements to which both are party, including bilateral agreements between the Swiss Confederation and the United States.

Article 24

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 25

Expenses

Each Party shall bear the expenses incurred by its authorities in implementing this Agreement.

Article 26

Termination

This Agreement may be terminated by either Party with six months' notice in writing to the other Party. If the Agreement is terminated, the Parties shall apply the provisions of this Agreement with respect to any data obtained under this Agreement, unless the Parties agree otherwise.

Article 27

Suspension

1. If either Party considers that the other Party is in material breach of 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.
2. For the period of suspension of this Agreement, the Parties to the Agreement shall consult with each other to reconcile their differences.

Article 28

Amendments

1. The Parties shall enter into consultations with respect to the amendment of this Agreement at the request of either Party.
2. The Parties may amend this Agreement at any time by written agreement.

Article 29

Entry into force

1. The Parties shall exchange diplomatic notes indicating that each has completed its internal approval procedures for entry into force. This Agreement

shall enter into force thirty days after the date on which the second Party has sent its notification.

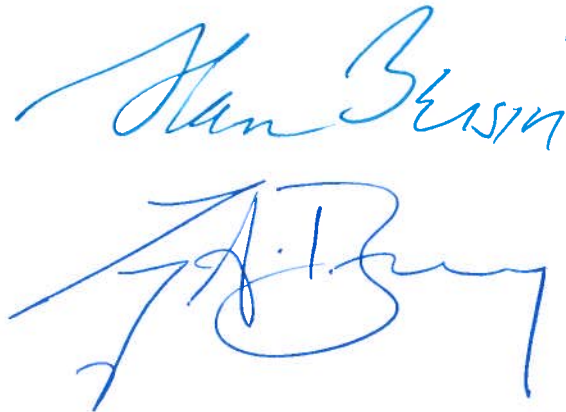
2. The automated querying and further supply of personal data and other information pursuant to Articles 6 and 7 shall be effective only if the United States has informed the Swiss Confederation by diplomatic note that the law of the United States permits the United States to implement those Articles on a reciprocal basis.

Done at Washington, this 12.12.2012, in duplicate, in the German and English languages, both texts being equally authentic.

FOR THE SWISS CONFEDERATION:



FOR THE UNITED STATES OF AMERICA:



ANNEX

Crimes within the scope of this Agreement include the crimes listed in this Annex, as well as the offenses of conspiracy to commit such offenses, participation in an organized criminal group, or attempt to commit such offenses, when criminalized:

1. Terrorism and terrorism-related offenses
2. Genocide
3. Crimes against humanity
4. War crimes
5. Murder, grievous bodily harm, offenses causing serious injury
6. Rape and other serious sexual assaults
7. Grand Theft
8. Burglary
9. Trafficking in and smuggling of human beings
10. Sexual exploitation of children and child pornography
11. Illicit trafficking in narcotic drugs and psychotropic substances
12. Illicit trafficking in weapons, munitions and explosives
13. Corruption
14. Fraud
15. Tax fraud
16. Laundering of the proceeds of crime
17. Counterfeiting currency
18. Forgery of means of payment
19. Computer-related crime
20. Facilitation of unauthorized entry and residence
21. Kidnapping, illegal restraint and hostage-taking
22. Organized or armed robbery
23. Racketeering and Extortion
24. Forgery of administrative documents and trafficking therein
25. Illicit trafficking in nuclear or radioactive materials
26. Trafficking in stolen vehicles
27. Arson
28. Unlawful seizure of aircrafts or ships
29. Sabotage
30. Illicit trade in human organs and tissue
31. Illicit trafficking in cultural goods, including antiques and works of art
32. Counterfeiting and piracy of products
33. Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties
34. False statement by a witness or otherwise in violation of domestic law