

**LAW ENFORCEMENT**

**Cooperation**

**Agreement Between the  
UNITED STATES OF AMERICA  
and SWITZERLAND**

**with Annex**

Signed at Washington December 12, 2012

Entered into force June 16, 2023



NOTE BY THE DEPARTMENT OF STATE

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

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

**Agreement**

**between**

**the United States of America**

**and**

**the Swiss Confederation**

**On Enhancing Cooperation in Preventing and Combating Serious Crime**

The United States of America and the Swiss Confederation (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 sup-

plies 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 au-

tomated 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, paragraph 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 United States and the Swiss Confederation.

**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 ef-

fect 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

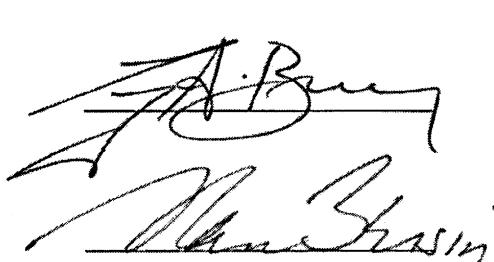
1. The Parties shall enter into consultations with respect to the amendment of this Agreement at the request of either Party.
2. The Parties may amend this Agreement at any time by written agreement.

**Article 29**  
Entry into force

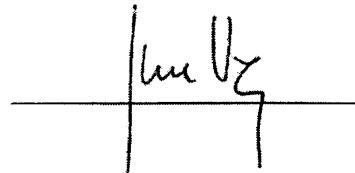
1. The Parties shall exchange diplomatic notes indicating that each has completed its internal approval procedures for entry into force. This Agreement shall enter into force thirty days after the date on which the second Party has sent its notification.
2. The automated querying and further supply of 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, D.C., this 12<sup>th</sup> December 2012, in duplicate, in the English and German languages, both texts being equally authentic.

FOR THE UNITED STATES  
OF AMERICA:



FOR THE SWISS CONFEDERATION:



## **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

**Abkommen**  
**zwischen**  
**den Vereinigten Staaten von Amerika**  
**und**  
**der Schweizerischen Eidgenossenschaft**  
**über**  
**die Vertiefung der Zusammenarbeit bei der Verhinderung und**  
**Bekämpfung schwerer Straftaten**

Die Vereinigten Staaten von Amerika und die Schweizerische Eidgenossenschaft (im Folgenden „die Vertragsparteien“),

geleitet von dem Wunsch, durch partnerschaftliche Zusammenarbeit schwere Straftaten, insbesondere die organisierte Kriminalität sowie den Terrorismus, wirksamer zu verhindern und zu bekämpfen,

in Anerkennung, dass der Austausch von Informationen ein wesentlicher Faktor bei der Bekämpfung schwerer Straftaten, insbesondere der organisierten Kriminalität sowie des Terrorismus, ist,

in Anerkennung der Bedeutung der Verhinderung und Bekämpfung schwerer Straftaten, insbesondere der organisierten Kriminalität sowie des Terrorismus, und unter gleichzeitiger Achtung der Grundrechte und Grundfreiheiten in den geltenden Gesetzen und internationalen Verpflichtungen der Vertragsparteien, einschliesslich derjenigen betreffend die Privatsphäre und den Schutz personenbezogener Daten,

in Anerkennung der Wichtigkeit, ein hohes Niveau beim Schutz personenbezogener Daten aufrechtzuerhalten, insbesondere der Wichtigkeit, zwischen den Vertragsparteien Verfahren zur Berichtigung, Sperrung und Löschung fehlerhafter personenbezogener Daten zu schaffen, die nach diesem Abkommen ausgetauscht werden,

unter Beachtung der Vereinbarung zwischen dem Eidgenössischen Justiz- und Polizeidepartement und dem Justizdepartement der Vereinigten Staaten von Amerika, handelnd für die zuständigen Strafverfolgungsbehörden der Schweizerischen Eidgenossenschaft und der Vereinigten Staaten von Amerika, über den Einsatz von gemeinsamen Ermittlungsgruppen zur Bekämpfung des Terrorismus und dessen Finanzierung, unterzeichnet am 12. Juli 2006,

angeregt durch den Vertrag vom 27. Mai 2005 über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration (Prümer Vertrag), und unter Kenntnisnahme der damit zusammenhängenden Beschlüsse 2008/615/JI und 2008/616/JI des Rates vom 23. Juni 2008 zur Integration des Prümer Vertrages in den Rahmen der Europäischen Union,

in Anerkennung der Verpflichtungen der Schweizerischen Eidgenossenschaft aus dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 und aus dem Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assozierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (Schengener Assoziierungsabkommen), und

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

sind wie folgt übereingekommen:

## Artikel 1

### Begriffsbestimmungen

Im Sinne dieses Abkommens bezeichnet der Ausdruck:

1. *DNA-Profil*: einen Buchstaben- oder Zahlencode, der eine Reihe von Identifizierungsmerkmalen des nicht kodierenden Teils einer analysierten menschlichen DNA-Probe, das heisst der spezifischen chemischen Form an den verschiedenen DNA-Loci, abbildet;
2. *Fundstellendatensatz*: ein DNA-Profil und die damit verbundene Kennung (DNA-Fundstellendatensatz) oder daktyloskopische Daten und die damit verbundene Kennung (daktyloskopischer Fundstellendatensatz);  
Fundstellendatensätze dürfen keine die betroffene Person unmittelbar identifizierenden Daten enthalten. Fundstellendatensätze, die keiner Person zugeordnet werden können (offene Spuren), müssen als solche erkennbar sein;
3. *personenbezogene Daten*: Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person);
4. *Bearbeitung personenbezogener Daten*: jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten mit oder ohne Hilfe automatisierter Verfahren, wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, das Konsultieren, die Benutzung, die Weitergabe durch Übermittlung, die Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren oder Löschen durch Unkenntlichmachen oder Vernichten von personenbezogenen Daten;
5. *sperren*: die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Bearbeitung einzuschränken;
6. *schwere Straftaten*: die im Anhang dieses Abkommens aufgeführten strafbaren Handlungen sowie andere Handlungen, die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind.

## Artikel 2

### Zweck und Anwendungsbereich dieses Abkommens

1. Zweck dieses Abkommens ist die Vertiefung der Zusammenarbeit zwischen den Vertragsparteien bei der Verhinderung und Ermittlung schwerer Straftaten durch Polizei- und Justizbehörden.
2. Die unter diesem Abkommen eingeräumten Befugnisse zum Abruf von daktyloskopischen Daten und DNA-Profilen (Artikel 4 und 6) dürfen nur zum Zwecke der Verhinderung und Ermittlung einer schweren Straftat nach Artikel 1 Ziffer 6 genutzt werden und nur, wenn besondere und rechtlich gültige Umstände in Bezug auf eine bestimmte Person Anlass geben zu prüfen, ob diese Person eine solche schwere Straftat begangen hat.

3. Einem Ersuchen um Übermittlung weiterer personenbezogener Daten und sonstiger Informationen nach den Artikeln 5 und 7 wird nur Folge geleistet, wenn die in dem Ersuchen umschriebene Handlung eine schwere Straftat nach dem Recht der ersuchten Vertragspartei beinhaltet.

### **Artikel 3** **Daktyloskopische Daten**

Zur Umsetzung dieses Abkommens gewährleisten die Vertragsparteien die Verfügbarkeit der Fundstellendatensätze der nationalen automatisierten daktyloskopischen Identifizierungssysteme, die zur Verhinderung und Ermittlung von Straftaten eingerichtet wurden. Fundstellendatensätze enthalten ausschliesslich daktyloskopische Daten und eine Kennung.

### **Artikel 4** **Automatisierter Abruf von daktyloskopischen Daten**

1. Zur Verhinderung und Ermittlung von schweren Straftaten gestatten die Vertragsparteien den in Artikel 9 bezeichneten nationalen Kontaktstellen der anderen Vertragspartei den Zugang zu den Fundstellendatensätzen der zu diesem Zweck eingerichteten nationalen automatisierten daktyloskopischen Identifizierungssysteme mit der Berechtigung, automatisierte Abrufe mittels eines Abgleichs der daktyloskopischen Daten vorzunehmen. Ein Abruf darf nur im Einzelfall und im Einklang mit dem innerstaatlichen Recht der abrufenden Vertragspartei erfolgen.
2. Die endgültige Zuordnung eines daktyloskopischen Datums zu einem Fundstellendatensatz der für die Bewirtschaftung dieses Datensatzes zuständigen Vertragspartei erfolgt durch die abrufende nationale Kontaktstelle anhand der automatisiert übermittelten Fundstellendatensätze, die für die eindeutige Zuordnung erforderlich sind.

### **Artikel 5** **Übermittlung weiterer personenbezogener Daten und sonstiger Informationen**

Im Falle der Feststellung einer Übereinstimmung von daktyloskopischen Daten im Verfahren nach Artikel 4 erfolgt die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener Daten und sonstiger Informationen nach dem innerstaatlichen Recht der ersuchten Vertragspartei, einschliesslich deren Vorschriften über die Rechtshilfe. Die Übermittlung erfolgt in Übereinstimmung mit den Artikeln 9 und 11.

**Artikel 6**  
**Automatisierter Abruf von DNA-Profilen**

1. Falls der Zugriff nach dem innerstaatlichen Recht beider Vertragsparteien zulässig und in der Praxis für beide Vertragsparteien möglich ist und nachdem die Durchführungsvereinbarungen abgeschlossen wurden, können die Vertragsparteien der nationalen Kontaktstelle nach Artikel 9 der anderen Vertragspartei den Zugang zu den Fundstellendatensätzen ihrer DNA-Analyse-Dateien mit der Berechtigung gestatten, zum Zwecke der Verhinderung und Ermittlung schwerer Straftaten automatisierte Abrufe mittels eines Abgleichs der DNA-Profile vorzunehmen. Ein Abruf darf nur im Einzelfall und im Einklang mit dem innerstaatlichen Recht der abrufenden Vertragspartei erfolgen.
2. Wird im Zuge eines automatisierten Abrufs die Übereinstimmung eines übermittelten DNA-Profiles mit einem in der Datei der anderen Vertragspartei gespeicherten DNA-Profil festgestellt, so erhält die abrufende nationale Kontaktstelle automatisch die Fundstellendatensätze hinsichtlich derer eine Übereinstimmung festgestellt worden ist. Kann keine Übereinstimmung festgestellt werden, so wird dies automatisch mitgeteilt.

**Artikel 7**  
**Übermittlung weiterer personenbezogener Daten und sonstiger Informationen**

Im Falle der Feststellung einer Übereinstimmung von DNA-Profilen im Verfahren nach Artikel 6 erfolgt die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener Daten und sonstiger Informationen nach dem innerstaatlichen Recht der ersuchten Vertragspartei, einschliesslich deren Vorschriften über die Rechtshilfe. Die Übermittlung erfolgt in Übereinstimmung mit den Artikeln 9 und 11.

**Artikel 8**  
**Alternative Möglichkeiten zum Abruf von DNA-Dateien**

Bis die in Artikel 29 Ziffer 2 vorgesehene Notifikation erfolgt, kann jede Vertragspartei auf Ersuchen der anderen Vertragspartei eine Abfrage der eigenen DNA-Datenbank im Einklang mit ihrem innerstaatlichen Recht und ihren technischen Anforderungen durchführen.

**Artikel 9**  
**Nationale Kontaktstellen**

Zum Zwecke der Übermittlung von Daten und sonstigen Informationen nach den Artikeln 4 bis 8 bezeichnet jede Vertragspartei eine nationale Kontaktstelle für Datenübermittlungen nach den Artikeln 6 und 7 sowie eine oder mehrere nationale Kontaktstellen für

Datenübermittlungen nach den Artikeln 4 und 5. Jede nationale Kontaktstelle übermittelt die Daten in Übereinstimmung mit ihrem innerstaatlichen Recht.

**Artikel 10**  
**Kontingente**

Die Vertragsparteien konsultieren sich, um die Anzahl von Abrufen, die sie nach den Artikeln 4 bis 7 durchführen, angemessen zu beschränken, und nehmen diese Beschränkungen in die Durchführungsvereinbarungen auf.

**Artikel 11**  
**Durchführungsvereinbarungen**

Die technischen und prozeduralen Einzelheiten für die nach diesem Abkommen durchgeführten Datenabrufe und -übermittlungen werden in einer oder mehreren Durchführungsvereinbarungen geregelt.

**Artikel 12**  
**Übermittlung personenbezogener Daten und sonstiger Informationen zur Verhinderung schwerer Straftaten sowie Handlungen im Zusammenhang mit Terrorismus**

1. In Übereinstimmung mit ihrem innerstaatlichen Recht können die Vertragsparteien im Einzelfall auch ohne Ersuchen der in Ziffer 4 dieses Artikels benannten massgeblichen nationalen Kontaktstelle die in Ziffer 2 dieses Artikels genannten personenbezogenen Daten und sonstigen Informationen übermitteln, um strafbare Handlungen, die eine ernsthafte Bedrohung öffentlicher Interessen darstellen, zu verhindern, soweit dies erforderlich ist, weil besondere Umstände Grund zu der Annahme geben, dass die betroffene Person strafbare Handlungen im Zusammenhang mit Terrorismus, einer terroristischen Gruppierung oder Verschwörung sowie strafbare Handlungen im Zusammenhang mit schweren Straftaten, wie sie nach dem innerstaatlichen Recht der datenübermittelnden Vertragspartei bestimmt sind, begehen könnte.
2. Die nach Ziffer 1 zu übermittelnden Daten können Nachnamen, Vornamen, Geburtsdatum und Geburtsort sowie die Darstellung der Umstände, welche für den in Ziffer 1 erwähnten Verdacht Anlass gegeben haben, umfassen.
3. Die übermittelnde Vertragspartei kann in Anwendung ihres innerstaatlichen Rechts im Einzelfall Bedingungen für die Verwendung dieser Daten durch die empfangende Vertragspartei festlegen. Wenn die empfangende Vertragspartei die betreffenden Daten annimmt, muss sie sich an alle diese Bedingungen halten. Allgemeine Einschränkungen in Bezug auf die rechtlichen Standards der empfangenden Vertragspartei für die Bearbeitung personenbezogener Daten können von der übermittelnden Vertragspartei nicht als Bedingung im Sinne dieser Ziffer für die

Übermittlung von Daten auferlegt werden. Zusätzlich zu den personenbezogenen Daten nach Ziffer 2 dieses Artikels können die Vertragsparteien auch nicht personenbezogene Daten übermitteln, die im Zusammenhang mit den strafbaren Handlungen in Ziffer 1 dieses Artikels stehen.

4. Jede Vertragspartei bezeichnet eine oder mehrere nationale Kontaktstellen für den nach diesem Artikel erfolgenden Austausch personenbezogener Daten und sonstiger Informationen mit der oder den nationalen Kontaktstellen der anderen Vertragspartei. Die Befugnisse und Zuständigkeiten der nationalen Kontaktstellen werden nach innerstaatlichem Recht festgelegt.

### **Artikel 13**

#### Allgemeine Grundsätze des Datenschutzes

1. Die Vertragsparteien stellen ein hohes Datenschutzniveau in ihrem innerstaatlichen Recht sicher, um das Vertrauen in die Umsetzung dieses Abkommens zu bewahren.
2. Die Vertragsparteien verpflichten sich, personenbezogene Daten nach Treu und Glauben und nach ihren jeweiligen Rechtsvorschriften zu bearbeiten und insbesondere:
  - a. personenbezogene Daten nur sofern relevant, zweckmässig und nicht über den Zweck hinausgehend zu bearbeiten;
  - b. sicherzustellen, dass die bereitgestellten personenbezogenen Daten richtig, aktuell und angemessen sind;
  - c. die personenbezogenen Daten nur so lange aufzubewahren, wie dies für den spezifischen Zweck, zu dem die Daten in Übereinstimmung mit diesem Abkommen bereitgestellt oder weiterbearbeitet wurden, nötig ist.
3. Dieses Abkommen regelt die Rechte und Pflichten der Vertragsparteien in Bezug auf die Verwendung von nach diesem Abkommen bereitgestellten personenbezogenen Daten, einschliesslich der Berichtigung, Sperrung und Löschung von Daten nach Artikel 16. Privatpersonen erwachsen jedoch keine Rechte aus diesem Abkommen. Unabhängig von diesem Abkommen bestehende Rechte von Privatpersonen, einschliesslich des Rechts nach Artikel 21 auf Auskunft, Berichtigung, Sperrung und Löschung von Daten, bleiben unberührt.
4. Die Zuständigkeit und die Befugnisse für rechtliche Kontrollen der Übermittlung, des Empfangs, der Bearbeitung und der Speicherung von personenbezogenen Daten obliegen nach den Vorschriften ihres innerstaatlichen Rechts den unabhängigen Datenschutzbehörden oder, wo anwendbar, den Aufsichtsbehörden, den Datenschutzbeamten und den gerichtlichen Behörden der jeweiligen Vertragspartei. Die Vertragsparteien teilen sich gegenseitig die Behörden mit, die als Kontaktstellen für die Umsetzung der Datenschutzbestimmungen dieses Abkommens handeln.

## **Artikel 14**

### **Zusätzlicher Schutz bei der Übermittlung von personenbezogenen Daten besonderer Kategorien**

1. Personenbezogene Daten, aus denen die Rasse oder ethnische Herkunft, politische Anschauungen, religiöse oder sonstige Überzeugungen oder die Mitgliedschaft in Gewerkschaften hervorgeht oder die die Gesundheit und das Sexualleben betreffen, dürfen nur zur Verfügung gestellt werden, wenn sie für die Zwecke dieses Abkommens unter Abwägung der Interessen besonders relevant sind und nur nach den Artikeln 5, 7 oder 12 dieses Abkommens übermittelt werden.
2. In Anerkennung der besonderen Schutzbedürftigkeit der oben genannten Kategorien personenbezogener Daten treffen die Vertragsparteien angemessene Schutzvorkehrungen, insbesondere geeignete Sicherheitsmassnahmen, um solche Daten zu schützen.

## **Artikel 15**

### **Bearbeitungsbeschränkungen zum Schutz personenbezogener Daten und sonstiger Informationen**

1. Unbeschadet des Artikels 12 Ziffer 3 darf jede Vertragspartei Daten, die sie nach diesem Abkommen erlangt hat, nur bearbeiten:
  - a. für den Zweck ihrer strafrechtlichen Ermittlung;
  - b. zur Verhinderung einer ernsthaften Bedrohung ihrer öffentlichen Sicherheit;
  - c. in ihren nicht strafrechtlichen Gerichts- und Verwaltungsverfahren, die in direktem Zusammenhang mit den Ermittlungen nach Buchstabe a stehen; oder
  - d. für jeden anderen Zweck, jedoch nur mit vorheriger Zustimmung der Vertragspartei, die die Daten übermittelt hat, in Übereinstimmung mit dem innerstaatlichen Recht der übermittelnden Vertragspartei.
2. Die Vertragsparteien geben Drittstaaten und internationalen Organisationen Daten, die ihnen nach diesem Abkommen zur Verfügung gestellt wurden, nicht ohne vorherige ausdrückliche und in geeigneter Weise dokumentierte Zustimmung der Vertragspartei, die die Daten zur Verfügung gestellt hat, und ohne geeignete Schutzvorkehrungen weiter.
3. Eine Vertragspartei darf in den daktyloskopischen Dateien oder DNA-Dateien der anderen Vertragspartei einen automatisierten Abruf nach Artikel 4 oder 6 lediglich dazu durchführen und die als Ergebnis eines solchen Abrufs erhaltenen Daten, einschliesslich der Mitteilung über das Vorliegen oder Nichtvorliegen eines Treffers, ausschliesslich bearbeiten, um:
  - a. festzustellen, ob die verglichenen DNA-Profile oder daktyloskopischen Daten übereinstimmen;
  - b. im Fall einer Übereinstimmung der Daten ein Folgeersuchen um Unterstützung im Einklang mit dem innerstaatlichen Recht einschliesslich der Vorschriften über die Rechtshilfe vorzubereiten und zu übermitteln; oder

- c. die Protokollierung durchzuführen, wie diese nach innerstaatlichem Recht verlangt wird oder zulässig ist.
- 4. Die für die Bewirtschaftung der Datei zuständige Vertragspartei darf die ihr nach den Artikeln 4 und 6 von der abrufenden Vertragspartei im Zuge eines automatisierten Abrufs übermittelten Daten ausschliesslich bearbeiten, soweit dies für die Durchführung des Abgleichs, für die automatisierte Beantwortung des Abrufs oder für die Protokollierung nach Artikel 17 erforderlich ist. Nach Beendigung des Datenabgleichs oder nach der automatisierten Beantwortung des Abrufs müssen die zu Vergleichszwecken übermittelten Daten unverzüglich gelöscht werden, sofern nicht die Weiterbearbeitung für die in Ziffer 3 Buchstaben b oder c dieses Artikels genannten Zwecke erforderlich ist.

### **Artikel 16** **Berichtigung, Sperrung und Löschung von Daten**

- 1. Auf Verlangen der übermittelnden Vertragspartei ist die empfangende Vertragspartei verpflichtet, Daten, die sie nach diesem Abkommen erlangt hat, zu berichtigen, zu sperren oder zu löschen, wenn sie unrichtig oder unvollständig sind oder ihre Erhebung oder Weiterbearbeitung im Einzelfall im Widerspruch zu diesem Abkommen oder zu den für die übermittelnde Vertragspartei geltenden Vorschriften steht.
- 2. Stellt eine Vertragspartei fest, dass Daten, die sie von der anderen Vertragspartei nach diesem Abkommen erhalten hat, unrichtig sind, ergreift sie unverzüglich alle geeigneten Massnahmen zum Schutz vor fälschlichem Vertrauen in diese Daten; dies umfasst insbesondere die Ergänzung, Löschung oder Berichtigung oder, wenn zweckdienlich, als zusätzliche Massnahme die Kennzeichnung solcher Daten.
- 3. Stellt eine Vertragspartei fest, dass relevante Daten, die sie nach diesem Abkommen der anderen Vertragspartei übermittelt oder von ihr empfangen hat, unrichtig, nicht verlässlich oder Gegenstand erheblicher Zweifel sind, teilt sie dies der anderen Vertragspartei unverzüglich mit.
- 4. Wenn es Grund zur Annahme gibt, dass durch eine Löschung Interessen der direkt betroffenen Person oder anderer betroffener Personen beeinträchtigt werden, sind diese Daten in Übereinstimmung mit dem innerstaatlichen Recht zu sperren anstatt zu löschen.
- 5. Die Vertragsparteien gewährleisten die ordnungsgemäße Beseitigung personenbezogener Informationen nach Ablauf der spezifischen Aufbewahrungsfristen, die nach innerstaatlichem Recht vorgesehen sind. Diese Aufbewahrungsfristen sollen angemessene operationelle Erwägungen, das öffentliche Interesse, die Art der Daten, den Zweck der Bearbeitung oder Verwendung sowie die Interessen der betroffenen Person auf Schutz der Privatsphäre widerspiegeln.

## **Artikel 17**

### Dokumentation

1. Jede Vertragspartei dokumentiert jede nicht automatisierte Übermittlung und jeden nicht automatisierten Empfang von personenbezogenen Daten durch die für die Bewirtschaftung der Datei zuständige Stelle und durch die abrufende Stelle zur Kontrolle der Zulässigkeit der Übermittlung nach diesem Abkommen. Die Dokumentation umfasst folgende Angaben:
  - a. den Anlass der Übermittlung,
  - b. Informationen über die übermittelten Daten,
  - c. das Datum der Übermittlung; und
  - d. die Bezeichnung oder Kennung der abrufenden und der für die Bewirtschaftung der Datei zuständigen Stelle.
2. Für den automatisierten Abruf von Daten auf Grund der Artikel 4 und 6 gilt Folgendes:
  - a. Der automatisierte Abruf darf nur durch eigens ermächtigte Beamte der nationalen Kontaktstellen erfolgen. Jede Vertragspartei führt Aufzeichnungen, die es ermöglichen, jene Person zu identifizieren, die den automatisierten Abruf veranlasst oder durchgeführt hat.
  - b. Jede Vertragspartei gewährleistet, dass jede Übermittlung und jeder Empfang von Daten von der für die Bewirtschaftung der Datei zuständigen Stelle und der abrufenden Stelle protokolliert werden, einschliesslich der Mitteilung des Vorliegens oder Nichtvorliegens eines Treffers. Die Protokollierung umfasst folgende Angaben:
    - (i) Informationen über die übermittelten Daten;
    - (ii) das Datum und den Zeitpunkt der Übermittlung;
    - (iii) die Bezeichnung oder Kennung der abrufenden und für die Bewirtschaftung der Datei zuständigen Stelle; und
    - (iv) den Grund für den Abruf.
3. Die Aufzeichnung jeder Übermittlung und jedes Empfangs von personenbezogenen Daten, die nach den Ziffern 1 und 2 protokolliert werden, sind durch geeignete Massnahmen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen und zwei Jahre aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unverzüglich zu löschen, sofern dies nicht dem innerstaatlichen Recht widerspricht.

## **Artikel 18**

### Datensicherheit

1. Die Vertragsparteien gewährleisten, dass die notwendigen technischen Massnahmen und organisatorischen Vorkehrungen getroffen werden, um personenbezogene Daten und sonstige Informationen gegen zufällige oder unrechtmässige Zerstörung, zufälligen Verlust oder unbefugte Bekanntgabe, Veränderung, unbefugten Zugang oder jede unbefugte Form der Bearbeitung zu schützen. Insbesondere gewährleisten

- die Vertragsparteien, dass nur eigens dazu befugte Personen Zugang zu diesen personenbezogenen Daten und sonstigen Informationen haben.
2. Die Durchführungsvereinbarungen nach Artikel 11, die das Verfahren für den automatisierten Abruf von daktyloskopischen Daten und DNA-Daten nach den Artikeln 4 und 6 regeln, sehen vor, dass:
- moderne Technologie in geeigneter Weise eingesetzt wird, um den Schutz, die Sicherheit, die Vertraulichkeit und die Integrität der Daten sicherzustellen;
  - bei der Nutzung allgemein zugänglicher Netze Verschlüsselungs- und Authentifizierungsverfahren angewendet werden, die von den dafür zuständigen Stellen anerkannt sind; und
  - ein Verfahren besteht um sicherzustellen, dass nur erlaubte Abrufe durchgeführt werden.

### **Artikel 19** Transparenz –Information der betroffenen Personen

- Die sich aus ihren jeweiligen Rechtsvorschriften ergebenden gesetzlichen Verpflichtungen der Vertragsparteien bleiben vorbehalten, wonach sie die betroffenen Personen über die Zwecke der Datenbearbeitung, die Identität der für die Datenbearbeitung verantwortlichen Person, die Empfänger oder Empfängerkategorien und über ihr Recht, die sie betreffenden Daten einzusehen und zu berichtigen, zu informieren und ihnen jede weitere Information zu geben haben, wie Informationen über die Rechtsgrundlage des Bearbeitungsvorgangs, für den die Daten vorgesehen sind, über die Fristen für die Datenspeicherung und über Entschädigungsansprüche, soweit solche weiteren Informationen notwendig sind, um unter Berücksichtigung der Zwecke und konkreten Umstände, unter denen die Daten bearbeitet werden, gegenüber der betroffenen Person eine Bearbeitung nach Treu und Glauben zu gewährleisten.
- Solche Informationen dürfen in Übereinstimmung mit den jeweiligen Rechtsvorschriften der Vertragsparteien verweigert werden, einschliesslich der Fälle, in denen
  - die Zwecke der Bearbeitung,
  - Ermittlungen oder strafrechtliche Verfolgungsmassnahmen der zuständigen Behörden der Vertragsparteien, oder
  - die Rechte und Freiheiten Dritterdurch die Bereitstellung dieser Informationen gefährdet würden.

### **Artikel 20** Überprüfung

Zusätzlich zu ihren Rechten nach Artikel 16 kann eine Vertragspartei von der Datenschutzbehörde der anderen Vertragspartei oder einer anderen zuständigen Behörde nach

Artikel 13 Ziffer 4 verlangen, dass diese überprüft, ob die personenbezogenen Daten einer betroffenen Person, die aufgrund dieses Abkommens übermittelt wurden, in Übereinstimmung mit diesem Abkommen bearbeitet wurden. Die Behörde, die einen solchen Antrag erhält, hat der zuständigen Behörde der anderen Vertragspartei zügig zu antworten.

### **Artikel 21**

#### **Ersuchen von Personen auf Zugang zu Daten und auf Berichtigung, Sperrung und Löschung von Daten sowie Entschädigungsverfahren**

1. Auf Ersuchen einer betroffenen Person um Auskunft nach innerstaatlichem Recht über die sie betreffenden, im Rahmen des Anwendungsbereichs dieses Abkommens bearbeiteten Daten, hat die das Ersuchen empfangende Vertragspartei in Übereinstimmung mit ihrem innerstaatlichen Recht zu verfahren.
2. Jede Person, die Informationen über die Verwendung ihrer personenbezogenen Daten verlangt, die im Rahmen dieses Abkommens bearbeitet wurden, oder das ihr nach den innerstaatlichen Gesetzen zustehende Recht auf Berichtigung, Sperrung oder Löschung solcher Daten ausüben will, kann ein Ersuchen an ihre Datenschutzbehörde oder eine andere zuständige Behörde nach Artikel 13 Ziffer 4 richten. Diese Behörde hat in Übereinstimmung mit ihrem innerstaatlichen Recht und nach Artikel 16 oder Artikel 20 vorzugehen.
3. Die Vertragsparteien gewährleisten, dass den betroffenen Personen Verfahren zur Verfügung stehen, um eine angemessene Entschädigung für Verstöße gegen anwendbare Datenschutzrechte zu erlangen.
4. Die massgeblichen Verfahren betreffend den Zugang, die Berichtigung, Sperrung, Löschung und Entschädigung richten sich nach dem innerstaatlichen Recht derjenigen Vertragspartei, auf deren Gebiet die betroffene Person ihre Rechte geltend macht.

### **Artikel 22**

#### **Unterrichtung**

1. Die Vertragsparteien unterrichten einander über ihre innerstaatlichen Gesetze zum Schutz personenbezogener Daten und jede Änderung dieser Gesetze, die für die Umsetzung dieses Abkommens von Bedeutung sind.
2. Die empfangende Vertragspartei unterrichtet die übermittelnde Vertragspartei auf Ersuchen über die Bearbeitung der übermittelten Daten und das dadurch erzielte Ergebnis. Die empfangende Vertragspartei stellt sicher, dass ihre Antwort der übermittelnden Vertragspartei zügig mitgeteilt wird.
3. Die Vertragsparteien setzen alles daran, sich gegenseitig über die von betroffenen Personen erhaltenen Ersuchen nach Artikel 21 dieses Abkommens zu informieren.

**Artikel 23**  
**Verhältnis zu anderen Abkommen**

Durch dieses Abkommen werden die Rechte und Pflichten der Vertragsparteien aus internationalen Abkommen, deren Vertragspartei sie beide sind, sowie aus bilateralen Abkommen zwischen den Vereinigten Staaten von Amerika und der Schweizerischen Eidgenossenschaft nicht berührt.

**Artikel 24**  
**Konsultationen**

1. Die Vertragsparteien konsultieren sich regelmässig betreffend die Umsetzung der Bestimmungen dieses Abkommens.
2. Im Fall von Streitigkeiten über die Auslegung oder Anwendung dieses Abkommens konsultieren sich die Vertragsparteien, um deren Beilegung zu ermöglichen.

**Artikel 25**  
**Kosten**

Jede Vertragspartei trägt die Kosten, die ihren Behörden bei der Umsetzung dieses Abkommens entstehen.

**Artikel 26**  
**Kündigung**

Dieses Abkommen kann von jeder Vertragspartei unter Einhaltung einer sechsmonatigen Frist schriftlich gekündigt werden. Vorbehältlich einer anderslautenden Vereinbarung der Vertragsparteien wenden die Vertragsparteien im Falle einer Kündigung des Abkommens dessen Bestimmungen auf alle im Rahmen des Abkommens erhaltenen Daten weiterhin an.

**Artikel 27**  
**Suspendierung**

1. Ist eine der Vertragsparteien der Ansicht, dass die andere Vertragspartei in grundlegender Weise gegen dieses Abkommen verstösst oder dass Entwicklungen im innerstaatlichen Recht einer der Vertragsparteien den Zweck und den Anwendungsbereich dieses Abkommens, insbesondere in Bezug auf den Schutz personenbezogener Daten, untergraben, kann sie die Anwendung des Abkommens oder von Teilen desselben suspendieren. Die Suspendierung ist der anderen Vertragspartei auf diplomatischem Wege mitzuteilen und wird sofort mit Erhalt der

- Notifikation wirksam. Dasselbe Verfahren gilt für eine allfällige Aufhebung einer Suspendierung.
2. Während der Dauer der Suspendierung dieses Abkommens konsultieren sich die Vertragsparteien, um ihre Differenzen zu bereinigen.

**Artikel 28**  
Änderungen

1. Auf Ersuchen einer Vertragspartei nehmen die Vertragsparteien Konsultationen betreffend die Änderung dieses Abkommens auf.
2. Die Vertragsparteien können dieses Abkommen jederzeit durch schriftliche Übereinkunft ändern.

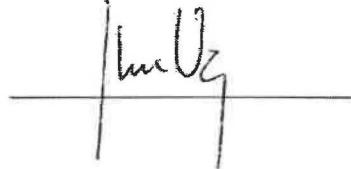
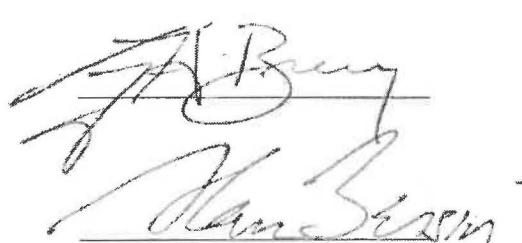
**Artikel 29**  
Inkrafttreten

1. Die Vertragsparteien teilen sich mittels diplomatischen Notenwechsels den Abschluss ihrer internen Genehmigungsverfahren für das Inkrafttreten mit. Dieses Abkommen tritt dreissig Tage nach dem Datum in Kraft, an dem die zweite Vertragspartei die Notifikation versandt hat.
2. Der automatisierte Abruf und die Übermittlung weiterer personenbezogener Daten und sonstiger Informationen nach den Artikeln 6 und 7 kommen erst zur Anwendung, wenn die Vereinigten Staaten von Amerika der Schweizerischen Eidgenossenschaft durch diplomatische Note mitgeteilt haben, dass das Recht der Vereinigten Staaten von Amerika die Umsetzung dieser Artikel auf der Grundlage der Gegenseitigkeit zulässt.

Geschehen zu Washington D.C.... am 12<sup>th</sup> Dec. 2013 in zwei Urschriften in englischer und deutscher Sprache, wobei beide Texte gleichermassen authentisch sind.

Für die Vereinigten Staaten von  
Amerika

Für die Schweizerische  
Eidgenossenschaft



## **Anhang**

Straftaten im Rahmen des Anwendungsbereichs dieses Abkommens umfassen die in diesem Anhang aufgelisteten Straftaten sowie die strafbaren Vorbereitungshandlungen zur Begehung solcher Straftaten, die Beteiligung an einer kriminellen Organisation oder der Versuch zur Begehung solcher strafbaren Handlungen, sofern unter Strafe:

1. Terrorismus und Terrorismus-bezogene Straftaten
2. Völkermord
3. Verbrechen gegen die Menschlichkeit
4. Kriegsverbrechen
5. Vorsätzliche Tötung, schwere Körperverletzung, zu schweren Verletzungen führende strafbare Handlungen
6. Vergewaltigung und andere schwere sexuelle Übergriffe
7. Schwerer Diebstahl
8. Einbruchdiebstahl
9. Menschenhandel- und schmuggel
10. Sexuelle Ausbeutung von Kindern und Kinderpornographie
11. Illegaler Handel mit Drogen und psychotropen Stoffen
12. Illegaler Handel mit Waffen, Munition und Sprengstoffen
13. Korruption
14. Betrug
15. Steuerbetrug
16. Geldwäsche
17. Geldfälschung
18. Fälschung von Zahlungsmitteln
19. Cyberkriminalität
20. Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt
21. Entführung, Freiheitsberaubung und Geiselnahme
22. Raub in organisierter Form oder mit Waffen
23. Erpressung und Schutzgelderpressung
24. Fälschung von amtlichen Dokumenten und Handel damit
25. Illegaler Handel mit nuklearen und radioaktiven Substanzen
26. Handel mit gestohlenen Kraftfahrzeugen
27. Brandstiftung
28. Flugzeug- und Schiffsentführung
29. Sabotage
30. Illegaler Handel mit Organen und menschlichem Gewebe
31. Illegaler Handel mit Kulturgütern, einschliesslich Antiquitäten und Kunstgegenstände
32. Nachahmung und Produktpiraterie
33. Umweltkriminalität, einschliesslich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten
34. Falschaussage als Zeuge oder unter sonstiger Verletzung innerstaatlichen Rechts