

**Agreement between
the American Institute in Taiwan and the Taipei Economic and
Cultural Representative Office in the United States
On Enhancing Cooperation in
Preventing and Combating Serious Crime**

The American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States (hereinafter respectively "AIT" and "TECRO" or, collectively, the "Parties"),

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

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

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

Seeking to enhance and encourage cooperation between the Parties in the spirit of partnership,

Have agreed as follows:

**Article 1
Definitions**

For the purposes of this Agreement,

1. Criminal justice purpose shall include activities defined as the administration of criminal justice, which means the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation activities of accused persons or criminal offenders. The administration of criminal justice also includes criminal identification activities.
2. DNA profiles (DNA identification patterns) shall mean a letter or numerical code representing a number of identifying features of the non-coding part of an analyzed human DNA sample, i.e. of the specific chemical form at the various DNA loci.
3. Personal data shall mean any information relating to an identified or identifiable natural person (the "data subject").
4. Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, combination or alignment, blocking, or deletion through erasure or destruction of personal data.
5. Reference data shall mean a DNA profile and the related reference (DNA reference data) or fingerprinting data and the related reference (fingerprinting reference data). Reference data must not contain any data from which the data subject can be directly

identified. Reference data not traceable to any individual (untraceables) must be recognizable as such.

6. Serious crimes shall mean, for purposes of implementing this Agreement, conduct constituting an offense punishable by a maximum deprivation of liberty of more than one year or a more serious penalty. The Parties may not be obligated to supply personal data as described in Articles 6 and 9 of the Agreement for specific identified offenses in accordance with the laws applicable in the territories of the authorities they represent.

Article 2

Purpose of this Agreement

1. The purpose of this Agreement is to enhance the cooperation between AIT and TECRO, through their designated representatives, in preventing and combating serious crime.
2. The querying powers provided for under this Agreement shall be used only for prevention, detection and investigation of crime.

Article 3

Fingerprinting data

For the purpose of implementing this Agreement, the Parties, through their designated representatives, shall ensure the availability of reference data from the file for the automated fingerprint identification systems established in the territories of the authorities represented by the Parties for the prevention and investigation of criminal offenses. Reference data shall only include fingerprinting data and a reference.

Article 4

Automated querying of fingerprint data

1. For the prevention and investigation of serious crime, each Party shall, if permitted under relevant law, allow the other Party's contact points, as referred to in Article 7, access to the reference data in the automated fingerprint identification system, which it has established for that purpose, with the power to conduct automated queries by comparing fingerprinting data. Queries may be conducted only in individual cases and in compliance with the law applicable in the territory of the authorities represented by the querying Party.
2. Comparison of fingerprinting data with reference data held by the designated representative of the Party in charge of the file shall be carried out by the querying contact points by means of the automated supply of the reference data required for a clear match.
3. When needed, further analysis for the purpose of confirming a match of the fingerprinting data with reference data held by the designated representative of the Party in charge of the file may be carried out by the requested contact points.

Article 5

Alternative means to query using identifying data

Until the designated representative of TECRO has a fully operational and automated fingerprint identification system that links to individual criminal records and is legally authorized by relevant law to provide AIT's designated representative with automated access to such a system, it shall provide an alternative means to conduct a query to determine a clear match linking the individual to additional data. Responses to queries through such alternative means shall be provided by a TECRO designated representative at the request of AIT's designated representative on as close to a real time basis as possible. Queries may be conducted only in individual cases and in compliance with the law applicable in the territory of the authorities represented by the querying Party.

Article 6

Supply of further personal and other data

Should the procedure referred to in Article 4 show a match between fingerprinting data, or should the procedure utilized pursuant to Article 5 show a match, the supply of any available further personal data and other data relating to the reference data shall be governed by the law, including the legal assistance rules, applicable in the territory of the authorities represented by the requested Party and shall be supplied in accordance with Article 7.

Article 7

Contact points and implementing agreements

1. For the purpose of the supply of data as referred to in Articles 4 and 5, and the subsequent supply of further personal data as referred to in Article 6, each Party shall designate one or more contact points. The contact point shall supply such data in accordance with the law applicable in the territory of the authorities represented by the Party designating the contact point. Other available legal assistance channels need not be used unless necessary, for instance to authenticate such data for purposes of its admissibility in judicial proceedings in the territory of the authorities represented by the requesting Party.
2. The technical and procedural details for the queries conducted pursuant to Articles 4 and 5 shall be set forth in one or more implementing agreements or arrangements between the Parties.

Article 8

Automated querying of DNA profiles

1. If permissible under the law applicable in the territory of the authorities represented by both Parties and on the basis of reciprocity, the Parties may allow each other's contact point, as referred to in Article 10, access to the reference data in their DNA analysis files, with the power to conduct automated queries by comparing DNA profiles for the investigation of serious crime. Queries may be made only in individual cases and in compliance with the law applicable in the territory of the authorities represented by the querying Party.

2. Should an automated query show that a DNA profile supplied matches a DNA profile entered in the other Party's file, the querying contact point shall receive by automated notification the reference data for which a match has been found. If no match can be found, automated notification of this shall be given.

Article 9

Supply of further personal and other data

Should the procedure referred to in Article 8 show a match between DNA profiles, the supply of any available further personal data and other data relating to the reference data shall be governed by the law, including the legal assistance rules, applicable in the territory of the authorities represented by the requested Party and shall be supplied in accordance with Article 10.

Article 10

Contact point and implementing agreements

1. For the purposes of the supply of data as set forth in Article 8, and the subsequent supply of further personal data as referred to in Article 9, each Party shall designate a contact point. The contact point shall supply such data in accordance with the law applicable in the territory of the authorities represented by the Party designating the contact point. Other available legal assistance channels need not be used unless necessary, for instance to authenticate such data for purposes of its admissibility in judicial proceedings in the territory of the authorities represented by the requesting Party.
2. The technical and procedural details for the queries conducted pursuant to Article 8 shall be set forth in one or more implementing agreements or arrangements between the Parties.

Article 11

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

1. For the prevention of serious criminal and terrorist offenses, the Parties may, through their designated representatives, in compliance with the laws applicable in the territories of the authorities they respectively represent, in individual cases, even without being requested to do so, supply the other Party's relevant 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 law applicable in the territory of the authorities represented by the supplying Party; or
 - b. is undergoing or has undergone training to commit the offenses referred to in subparagraph a; or

- c. will commit or has committed a serious criminal offense, or participates in an organized criminal group or association.
2. The personal data to be supplied may include, if available, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, current and former nationalities, passport number, numbers from other identity documents, and 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, through its designated representative, in compliance with the law applicable in the territory of the authorities it represents, impose conditions on the use that may be made of such data by the receiving Party or its designated representative. If the receiving Party, or its designated representative, accepts such data, they shall be bound by any such conditions.
4. Generic restrictions with respect to the legal standards applicable in the territory of the authorities represented by the receiving Party for processing personal data may not be imposed by the supplying Party or its designated representative as a condition under paragraph 3 to providing data.
5. In addition to the personal data referred to in paragraph 2, the Parties may, through their designated representatives, provide each other with non-personal data related to the offenses set forth in paragraph 1.
6. Each Party shall designate one or more contact points for the exchange of personal and other data under this Article with the other Party's contact points. The powers of the contact points shall be governed by the law applicable in the territories of the authorities they respectively represent.

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 ensuring that their designated representatives process personal data fairly and in accord with the laws applicable in the territories of the authorities they respectively represent and:
 - a. ensuring that the personal data provided are adequate and relevant in relation to the specific purpose of the transfer;
 - b. retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Agreement; and
 - c. ensuring that possibly inaccurate personal data are timely brought to the attention of the designated representative of the receiving Party in order that appropriate corrective action is taken.
3. This Agreement shall not give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of

personal data. Rights existing independently of this Agreement, however, are not affected.

Article 13

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, genetic information or concerning health and sexual life may only be provided if they are particularly relevant to the purposes of this Agreement.
2. The Parties, through their designated representatives, 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 14

Limitation on processing to protect personal and other data

1. Without prejudice to Article 11, paragraph 3, each Party, through its designated representative, may process data obtained under this Agreement:
 - a. for the purpose of its criminal investigations;
 - b. for preventing a serious threat to its public security;
 - c. in its non-criminal judicial or administrative proceedings directly related to investigations set forth in subparagraph (a); or
 - d. for any other purpose, only with the prior consent of the Party which has transmitted the data.
2. The Parties and their designated representatives shall not communicate data provided under this Agreement to any foreign government, international body or private entity without the consent of the designated representative of the Party that provided the data and without the appropriate safeguards.
3. A Party, through its designated representative, may conduct a query of the other Party's fingerprint or DNA files under Articles 4, 5 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 the law, including the legal assistance rules, applicable in the territory of the authorities it represents, if those data match; or
 - c. conduct record-keeping, as required or permitted by the laws applicable in the territory of the authorities it represents.

The designated representative of the Party administering the file may process the data supplied to it by the designated representative of the querying Party during the course of a query in accordance with Articles 4, 5 or 8 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Article 16. The data supplied for comparison shall be deleted immediately

following data comparison or replies to queries unless further processing is necessary for the purposes mentioned under paragraph 3, subparagraphs (b) or (c) of this Article.

Article 15

Correction, blockage and deletion of data

1. At the request of the designated representative of the supplying Party, the designated representative of the receiving Party shall be obliged to correct, block, or delete, consistent with the laws applicable in the territory of the authorities represented by the receiving Party, data received under this Agreement that are incorrect or incomplete or if its collection or further processing contravenes this Agreement or the rules applicable in the territory of the authorities represented by the supplying Party.
2. Where the designated representative of a Party becomes aware that data it has received from the designated representative of the other Party under this Agreement are not accurate, the designated representative of the first Party 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. The designated representative of a Party shall notify the designated representative of the other Party if it becomes aware that material data it has transmitted to the designated representative of the other Party or received from the designated representative of the other Party under this Agreement are inaccurate or unreliable or are subject to significant doubt.

Article 16

Documentation

1. Each Party, through its designated representative, shall maintain a record of the transmission and receipt of data communicated to the designated representative of the other Party under this Agreement. This record shall serve to:
 - a. ensure effective monitoring of data protection in accordance with the laws applicable in the territory of the authorities represented by the respective Party;
 - b. enable the Parties and their designated representatives effectively to make use of the rights granted to them according to Articles 14 and 18; and
 - c. ensure data security.
2. The record shall include:
 - a. information on the data supplied;
 - b. the date of supply; and
 - c. the recipient of the data in case the data are supplied to other entities.
3. The record 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 the law, including applicable data protection and retention rules, applicable in the territory of the authorities represented by the receiving Party.

Article 17
Data Security

1. The Parties, through their designated representatives, 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. In particular, the Parties shall ensure that their designated representatives shall take reasonable measures to ensure that only those authorized to access personal data can have access to such data.
2. The implementing agreements or arrangements that govern the procedures for querying of fingerprint and DNA files pursuant to Articles 4, 5 and 8 shall provide:
 - a. that appropriate use is made of modern technology to ensure data protection, security, confidentiality and integrity;
 - b. that encryption and authorization procedures recognized by the competent authorities are used when having recourse to generally accessible networks; and
 - c. for a mechanism to ensure that only permissible queries are conducted.

Article 18
Transparency – Providing information to the data subjects

1. Nothing in this Agreement shall be interpreted to interfere with the legal obligations of the Parties and their designated representatives, as set forth by the laws applicable in the territories of the authorities represented respectively by the Parties, 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 laws applicable in the territories of the authorities represented by the Parties, including if providing this information may jeopardize:
 - a. the purposes of the processing;
 - b. investigations or prosecutions conducted by the competent authorities in the territories of the authorities represented by each of the Parties; or
 - c. the rights and freedoms of third parties.

Article 19
Information

Upon request, the receiving Party, through its designated representative, shall inform the supplying Party, through its designated representative, of the processing of supplied data and the result obtained. The receiving Party shall ensure that the answer of its designated

representative is communicated to the designated representative of the supplying Party in a timely manner.

Article 20

Relation to Other Agreements

Nothing in this Agreement shall be construed to limit or prejudice the provisions of any agreement, working law enforcement relationship, or other law allowing for information sharing between AIT and TECRO or their designated representatives.

Article 21

Consultations

1. The Parties, through their designated representatives, 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 22

Expenses

Each Party and its designated representatives shall bear their respective expenses incurred in implementing this Agreement. In special cases, the Parties and their designated representatives may agree on different arrangements.

Article 23

Termination of the Agreement

This Agreement may be terminated by either Party with three months' notice in writing to the other Party. The provisions of this Agreement shall continue to apply to data supplied prior to such termination.

Article 24

Amendments

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

Article 25
Entry into force

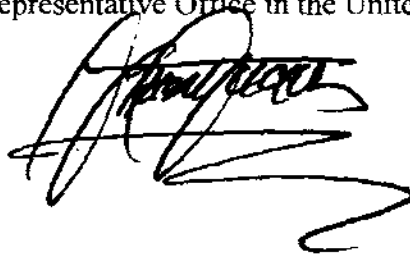
1. This Agreement shall enter into force, with the exception of Articles 8 through 10, on the date of the later letter completing an exchange of letters between the Parties indicating that each has taken any steps necessary to bring this Agreement into force. The Parties shall provisionally apply this Agreement, with the exception of Articles 8 through 10, from the date of signature to the extent consistent with the law applicable in the territories of the authorities they represent.
2. Articles 8 through 10 of this Agreement shall enter into force following the conclusion of the implementing agreement(s) or arrangement(s) referenced in Article 10 and on the date of the later letter completing an exchange of letters between the Parties indicating that each Party is able to implement those articles on a reciprocal basis. This exchange shall occur if the laws applicable in the territories of the authorities represented by both Parties permit the type of DNA screening contemplated by Articles 8 through 10.

Done at *Washington, DC*, this *20th* day of *December, 2011* in duplicate, in the English and Mandarin Chinese languages, both texts being equally authentic.

For the American Institute in Taiwan:

Barton J. Schuyler

For the Taipei Economic and Cultural
Representative Office in the United States:



美國在台協會與駐美國台北經濟文化代表處間 強化預防及打擊重大犯罪合作協定

美國在台協會 (AIT) 與駐美國台北經濟文化代表處 (TECRO) (以下合稱「雙方」),

因盼以夥伴身分合作, 以更有效預防及打擊重大犯罪, 尤其是恐怖主義;

認定資訊分享對打擊重大犯罪, 尤其是恐怖主義, 乃一項關鍵要素;
認定預防與打擊重大犯罪尤其是恐怖主義之重要性, 同時尊重基本權利與自由, 特別是隱私權,

並尋求促進並鼓勵雙方以夥伴精神合作,

爰經協議如下:

第 1 條

定義

基於此協定之目的:

1. 刑事司法目的, 應包括實施刑事司法之各項活動, 亦即任何下列活動之實行: 被告或刑事犯之偵查、逮捕、留置、審前釋放、審後釋放、起訴、裁判、矯正監護, 或感化教育活動。刑事司法之實施亦包括罪犯身分辨識。
2. DNA 資料 (即 DNA 個化鑑定型別) 係指代表人類 DNA 分析樣本中非密碼區之各種身分鑑定特徵 (即各個 DNA 基因座之特異化學物質) 的一個字母或數字代碼。
3. 個人資料應指任何與已辨識或可辨識之自然人 (簡稱為資料當事人) 有關之資料。

4. 個人資料之處理，係指將個人資料以自動或非自動之單一或一系列作業，例如蒐集、記錄、組織、儲存、改編或變更、分類、檢索、參閱、使用、通過提供或傳播及其他讓他人得以取得的方式公布、組合或校正、封鎖，或以清除或銷毀方式刪除個人資料。
5. 參考資料係指 DNA 檔及其相關參考資料 (DNA 參考資料)，或指紋資料及其相關參考資料 (指紋參考資料)。參考資料不得包括任何可直接辨識資料當事人身分之資料，此類「無法追蹤到任何個人之參考資料」(簡稱「無法追蹤資料」) 必須如此標識。
6. 本協定所稱重大犯罪應指最重本刑在一年以上或更重刑責之罪行。雙方得同意就特定案例可不必提供本協定第 6 條及第 9 條所定之個人資料，以配合各自所代表之當局所轄領土內適用之法律。

第 2 條

協定目的

1. 本協定之目的為促進美國在台協會與駐美國台北經濟文化代表處經各自指定之代表在預防與打擊重大犯罪方面之合作。
2. 此協定賦予之查詢權，僅供預防、偵查及調查犯罪之用。

第 3 條

指紋資料

為履行本協定，雙方應透過指定代表確保藉由各自所代表之當局所轄領土內建置之「自動指紋析鑑系統」所含參考資料可提供各方用於預防及偵查重大犯罪。參考資料應僅包括指紋資料及相關說明。

第 4 條

指紋資料之自動化查詢

1. 為預防與調查重大犯罪之目的，在相關法律許可下一方得允許另一方之聯絡窗口（如第 7 條所指）獲取其為防範與調查重大犯罪所建立之自動化指紋辨識系統之參考資料，該聯絡窗口亦有權透過比對指紋辨識資料進行自動化查詢。查詢得僅針對個案，且須依據查詢方所代表之當局所轄領土內適用之法律進行。
2. 指紋辨識資料與檔案負責方指定代表所持有參考資料之比對，應由查詢方之聯絡窗口透過自動化供應之參考資料進行（該參考資料係為明顯吻合之所需）。
3. 必要時，被要求方之聯絡窗口得再進行進一步分析，以確認指紋資料與檔案負責方指定代表所持有之參考資料吻合。

第 5 條

使用可辨識身分資料之替代查詢方法

在駐美國台北經濟文化代表處指定代表之一方未擁有可完整運作且與個人犯罪紀錄連線之自動化指紋辨識系統，並經法律授權供美國在台協會指定代表自動化進入該系統之前，駐美國台北經濟文化代表處應提供一個替代方法進行查詢，以確定個人與額外資料明顯吻合。利用此替代方式的查詢回復必須由駐美國台北經濟文化代表處之指定代表對於美國在台協會指定代表之查詢需求作盡可能即時性的回復。查詢得僅針對個案，且須依據查詢方所代表之當局所轄領土內適用之法律進行。

第 6 條

提供進一步個人與其他資料

倘依第 4 條所指之程序，顯示指紋資料吻合，或倘依第 5 條之程序顯示吻合，任何進一步個人資料與其他相關參考資料之提供，則應依被要求方所代表之當局所轄領土內適用之法律辦理，包括其司法互助協定，且應依第 7 條方式提供。

第 7 條

聯絡窗口及履行協定

1. 為第 4 條及第 5 條所指之資料提供，以及第 6 條所指之進一步個人資料之後續提供，雙方皆應指定一個或一個以上之聯絡窗口。聯絡窗口應根據指定該聯絡窗口者所代表之當局所轄領土內適用之法律提供該資料。除非必要，如驗證該資料之真偽以利要求方所代表之當局所轄領土內之司法程序採納該資料，否則無需使用其他可得之司法互助管道。
2. 第 4 條及第 5 條所訂查詢之技術與程序細節，應在雙方訂定之實施協定或協議中明定。

第 8 條

DNA 檔之自動化查詢

1. 若符合在雙方所代表之當局所轄領土內適用之法律，且基於互惠原則，各方得允許彼此的聯絡窗口（參照第 10 條）獲取其 DNA 分析檔案中之參考資料；該聯絡窗口亦有權透過比對 DNA 檔進行自動化查詢，以調查重大犯罪。惟僅能針對個案且在符合被查詢方所代表之當局所轄領土內適用之法律的條件下進行

查詢。

2. 倘自動化查詢顯示某個所提供之 DNA 檔，與另一方檔案中所輸入之 DNA 檔吻合，則查詢方之聯絡窗口應獲自動通知該吻合之相關資料。倘未發現吻合情形，亦應接獲如是自動通知。

第 9 條

提供進一步個人資料與其他資料

倘依第 8 條規定所指之程序，顯示 DNA 檔案吻合，則任何有關之進一步個人資料與其他資料之提供均應受被要求方所代表之當局所轄領土內適用之法律約束，包括其司法互助規定，且應依第 10 條方式提供。

第 10 條

聯絡窗口與履行協定

1. 為執行第 8 條所列之資料提供，以及第 9 條所指之進一步個人資料之後續提供，雙方皆應指定一個聯絡窗口。聯絡窗口應根據指定該聯絡窗口者所代表之當局所轄領土內適用之法律提供該等資料。除非必要，如驗證該資料之真偽，以利要求方所代表之當局所轄領土內之司法程序採納該資料，否則無須使用其他可得之司法互助管道。
2. 第 8 條所訂之查詢之技術與程序細節，應在雙方訂定之實施協定或協議中明定。

第 11 條

提供個人及其他資料，以預防重大犯罪與恐怖份子罪行

1. 為預防重大犯罪與恐怖份子罪行，當特殊情況使雙方有理由相信資料當事人將從事下列行為時，得透過各自的指定代表依個案考量，按照其各自所代表之當局所轄領土內適用之法律，提供第 2 項所指之個人資料予第 6 項所指之另一方相關聯絡窗口，甚至無須另一方提出要求：
 - a. 資料當事人將犯下或已犯下根據供應方所代表之當局所轄領土內適用之法律定義為恐怖份子或恐怖主義相關罪行，或者與恐怖集團、團體或相關組織有關之罪行；或
 - b. 正在或曾經接受足以犯下如前述 a 款所述罪行之訓練；
或
 - c. 將犯下或已犯下重大罪行，或參與有組織之犯罪團體或集團。
2. 欲提供之個人資料，得包括姓氏、名字、舊名、別名、化名、名字的另外拼法、性別、出生時地、目前及先前的國籍、護照號碼、其他身分文件號碼、指紋辨識資料、以及任何定罪內容，或者任何足以讓人相信會發生第 1 項所指內容之情況。
3. 提供方得依其所代表之當局所轄領土內適用之法律，透過指定代表，向接受方或其指定代表就該資料之可能用途提出附加條件。接受方或其指定代表倘接受該資料，即受該等條件之約束。
4. 提供方不得以第 3 項之規定為由，將接受方所代表之當局所轄領土內處理個人資料之適用法律標準的普遍限制加諸於接受方，作為提供資料的一個條件。
5. 除第 2 項所指之個人資料外，雙方得透過其指定代表提供彼此與第 1 段所列罪行有關之非個人資料。
6. 雙方均得指定一個或一個以上之聯絡窗口，以依此條規定與另一方之聯絡窗口交換個人及其他資料。聯絡窗口之權力應由各

自代表之當局所轄領土內適用之法律所管轄。

第 12 條

隱私權與資料保護

1. 雙方承認，自另一方所取得之個人資料之交付及處理過程，對雙方在履約過程中保密極具重要性。
2. 雙方承諾，其指定代表將以公正方式並依各自所代表之當局所轄領土內適用之法律處理個人資料，同時：
 - a. 確保所提供之個人資料為適當，且與轉移資料之特定目的有關；
 - b. 僅於為依此協定提供或進一步處理資料所需之時間內，保留個人資料；及
 - c. 確保及時告知接受方之指定窗口不正確之個人資料，以便接受方進行適當的更正。
3. 此協定不造成任何私人因而擁有任何權利，包括取得、隱瞞、或排除任何證據之權利，或阻礙分享個人資料之權利。惟獨立於此約之外之權利則不受影響。

第 13 條

特殊類個人資料傳輸之額外保護

1. 凡顯示種族、政治理念、宗教或其他信念、工會會員身分、遺傳訊息，或有關健康與性生活之個人資料，僅得於其與此協定之目的特別有關時方能提供。
2. 雙方透過其指定代表承認因上述類別之個人資料具特別敏感性，應採取適當之安全防護，尤其是適當之安全性措施，以保護該等資料。

第 14 條

限制處理程序，以保護個人及其他資料

1. 在不損及第 11 條第 3 項之規定下，雙方透過其指定代表均得為下列目的，處理依此協定所取得之資料：
 - a. 為其犯罪調查之目的；
 - b. 為預防對其公共安全之嚴重威脅；
 - c. 應與第 a 款所列調查直接有關之非刑事司法或行政程序所需；
或
 - d. 為任何其他目的，惟須經傳輸資料方之同意。
2. 未經資料提供方之指定代表同意，且在沒有適當之安全防護措施下，雙方與其指定代表不得將據此協定所提供之資料，告知任何外國當局、國際機構或者私人團體。
3. 一方透過其指定代表得依第 4 條、第 5 條或第 8 條規定，對另一方之指紋或 DNA 檔案進行查詢，並處理該查詢所得之資料，包括告知查詢是否獲得結果，惟其目的僅限於：
 - a. 確定比對後之 DNA 檔案或指紋資料是否吻合；
 - b. 在資料吻合之前提下，依其所代表之當局所轄領土內適用之法律（包括司法互助規定）準備及提出後續協助要求；或
 - c. 依其所代表之當局所轄領土內適用之法律要求或許可作成紀錄。

於第 4 條、第 5 條或第 8 條所定之查詢過程中，檔案提供方指定代表得處理查詢方指定代表所提供之資料，惟其目的僅限於比對、對查詢提供自動回應、或依第 16 條規定作成紀錄。除非為本條第 3

項第 b 款或第 c 款所提之目的，而有必要做進一步處理外，否則提供比對之資料，在資料比對或回應查詢之後應立刻刪除。

第 15 條

資料之更正、封鎖及刪除

1. 倘接受方依此協定所接獲之資料不正確或不完整，或倘該資料之蒐集或進一步處理抵觸此協定或提供方所代表之當局所轄領土內之相關規定，在提供方指定代表之要求下，接受方指定代表有責任依接收方所代表之當局所轄領土內適用之法律更正、封鎖或刪除該資料。
2. 倘一方之指定代表得知其依此協定從另一方之指定代表得到之資料不正確，第一方之指定代表應採取所有適當措施以避免錯信該資料，其方式包括補充、刪除或更正該資料。
3. 一方之指定代表倘得知其依此協定傳輸予另外一方之指定代表之資料，或從另一方之指定代表所得到之資料為不正確或不可靠，或有值重大懷疑處，則應通知另一方之指定代表。

第 16 條

文件紀錄

1. 雙方應透過其指定代表記錄依此協定所完成之資料傳輸與接收，該紀錄應用作下列用途：
 - a. 根據雙方各自所代表之當局所轄領土內適用之法律，確保有效監控資料之保護；
 - b. 使雙方之指定代表能有效運用依第 14 條與第 18 條所授予之權利；及

- c. 確保資料安全。
2. 該紀錄應包括：
 - a. 所提供資料之資訊；
 - b. 提供日期；及
 - c. 倘將資料提供予其他實體，則應記錄資料之接收人。
3. 紀錄應以適當措施保護，以防遭不適當之使用，以及其他形式之不當使用，並應保留兩年。除非與接收方所代表之當局所轄領土內適用之法律抵觸，包括相關之資料保護與留存法規，否則於保存期過後，紀錄應立刻刪除。

第 17 條

資料安全

1. 雙方應透過其指定代表確保運用必要之技術措施與組織化之安排保護個人資料，以防意外或者非法破壞、意外遺失或未經授權之揭露、更改、存取或任何未經授權之處理形式。雙方尤應確保其指定代表採取合理措施，以確保進入個人資料者皆獲授權。
2. 依第 4 條、第 5 條與第 8 條規定，管理指紋與 DNA 檔案查詢程序之實施協定或辦法應明列下列相關條文：
 - a. 該資料之適當使用皆透過現代科技為之，以確保資料之保護、安全、機密與完整；
 - b. 運用一般可存取之網路時，採取主管當局認可之加密與授權程序；及
 - c. 提供機制，以確保僅進行獲許可之查詢。

第 18 條

透明化—提供資訊予資料當事人

1. 此協定內容均不得解釋為干涉雙方及其指定代表依其各自所代表之當局所轄領土內適用之法律，提供資料當事人下列資訊之法律義務：處理之目的、資料控制者之身分、接收人或接收人之類型、獲取及更正當事人本身相關資料及任何進一步資料之權利，其中進一步資料包括該資料處理作業目的之法律依據、儲存資料與追索權之時間限制以及追索權，惟僅限於必要，並考量處理該資料之目的與特殊情況，以確保資料處理流程對資料當事人之公平。
2. 倘上述資訊之提供有危及以下項目之虞，則雙方得依其所代表之當局所轄領土內適用之法律拒絕提供：
 - a. 處理之目的；
 - b. 雙方各自所代表之當局所轄領土內法定官方機構所進行之調查或起訴；或
 - c. 第三方之權利與自由。

第 19 條

資料內容

在要求下，接收方應透過指定代表告知提供方指定代表所提供資料之處理與所得結果。接收方之指定代表應確保其結果及時回覆提供方之指定代表。

第 20 條

與其他協定之關係

此協定不得構成對允許美國在台協會與駐美國台北經濟文化代表處或其指定代表分享資訊之任何協定、有效執法關係或其他法律之限制或損害。

第 21 條

諮商

1. 雙方得透過其指定代表就此協定中條文之履行定期進行諮商。
2. 有關此協定之解釋或履行倘有任何爭議，雙方應彼此諮商以利解決。

第 22 條

費用

雙方及其指定代表應負擔其各自執行此協定之費用。惟如遇特案，雙方得同意進行不同之安排。

第 23 條

終止協定

任一方得於提出書面通知三個月後終止此協定。協定終止前所提供之資料應持續適用此協定之條文。

第 24 條

修訂

1. 在任何一方要求下，雙方應就此協定之修訂進行諮商。
2. 此協定得由雙方隨時以書面協議之方式修訂之。

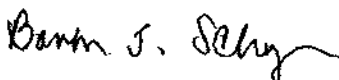
第 25 條

生效

1. 除第 8 條至第 10 條外，此協定應於雙方完成換函後生效（以較晚之換函日期為準），該換函述明雙方已採必要之步驟使協定生效。除第 8 條至第 10 條外，自簽署日起，雙方得於遵守他們所代表之當局所轄領土內適用法律之前提下，暫時適用此約。
2. 本協定第 8 條至第 10 條規定，應於第 10 條所指之實施協定或協議議定後，並於雙方完成換函之日生效（以較晚之換函日期為準），該換函中應述明雙方將能夠基於互惠原則履行該等條款。該換函之前提為雙方所代表之當局所轄領土內適用之法律規定允許第 8 條至第 10 條所稱之 DNA 檢測。

本協定以英文及中文各繕製兩份，於華盛頓哥倫比亞特區，二〇一一年十二月二十日簽署，兩種版本約文同一作準。

美國在台協會：



駐美國台北經濟文化代表處：

