# LAW ENFORCEMENT

## Cooperation

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

Signed at Reykjavik May 14, 2012

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."

# ICELAND

## Law Enforcement: Cooperation

*Agreement signed at Reykjavik*
*May 14, 2012;*
*Entered into force February 24, 2014,*
*with the exception of Articles 8 through 10.*
*In accordance with Article 25, Articles 8*
*through 10 may enter into force in the*
*future under conditions specified in Article 25.*

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

The Government of the United States of America and the Government of Iceland (hereinafter "Parties"),

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

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

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

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

Have agreed as follows:

## Article 1
## Definitions

For the purposes of this Agreement,

1. Criminal justice purpose shall include activities defined as the administration of criminal justice, which means the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation activities of accused persons or criminal offenders. The administration of criminal justice also includes criminal identification activities.

2. DNA profiles (DNA identification patterns) shall mean a letter or numerical code representing a number of identifying features of the non-coding part of an analyzed human DNA sample, i.e. of the specific chemical form at the various DNA loci.

3. Personal data shall mean any information relating to an identified or identifiable natural person (the "data subject").

4. Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection,

recording, organization, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, combination or alignment, blocking, or deletion through erasure or destruction of personal data.

5. Reference data shall mean a DNA profile and the related reference (DNA reference data) or fingerprinting data and the related reference (fingerprinting reference data). Reference data must not contain any data from which the data subject can be directly identified. Reference data not traceable to any individual (untraceables) must be recognizable as such.

6. Serious crimes shall mean, for purposes of implementing this Agreement, conduct constituting an offense punishable by a maximum deprivation of liberty of more than one year or a more serious penalty. To ensure compliance with their national laws, the Parties may agree to specify particular serious crimes for which a Party shall not be obligated to supply personal data as described in Articles 6 and 9 of the Agreement.

**Article 2**
**Purpose of this Agreement**

1. The purpose of this Agreement is to enhance the cooperation between the United States and Iceland 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 shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offenses. Reference data shall only include fingerprinting data and a reference.

**Article 4**
**Automated querying of fingerprint data**

1. For the prevention and investigation of serious crime, each Party shall allow the other Party's national contact points, as referred to in Article 7, access to the reference data in the automated fingerprint identification system, which it has established for that purpose, with the power to conduct automated queries by comparing fingerprinting data. Queries may be conducted only in individual cases and in compliance with the querying Party's national law.

2. Comparison of fingerprinting data with reference data held by the Party in charge of the file shall be carried out by the querying national contact points by means of the automated supply of the reference data required for a clear match.

3. When needed, further analysis for the purpose of confirming a match of the fingerprinting data with reference data held by the Party in charge of the file may be carried out by the requested national contact points.

**Article 5**
**Alternative means to query using identifying data**

Until Iceland has a fully operational and automated fingerprint identification system that links to individual criminal records and is prepared to provide the United States with automated access to such a system, it shall provide an alternative means to conduct a query using other identifying data to determine a clear match linking the individual to additional data. Query powers shall be exercised in the same manner as provided in Article 4 and a clear match shall be treated the same as a firm match of fingerprinting data to allow for the supply of additional data as provided for in Article 6.

**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 national law, including the legal assistance rules, of the requested Party and shall be supplied in accordance with Article 7.

**Article 7**
**National contact points and implementing agreements**

1. For the purpose of the supply of data as referred to in Articles 4 and 5, and the subsequent supply of further personal data as referred to in Article 6, each Party shall designate one or more national contact points. The contact point shall supply such data in accordance with the national law of 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 of 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.

**Article 8**
**Automated querying of DNA profiles**

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

2. Should an automated query show that a DNA profile supplied matches a DNA profile entered in the other Party's file, the querying national contact point shall receive by

automated notification the reference data for which a match has been found. If no match can be found, automated notification of this shall be given.

## Article 9
## Supply of further personal and other data

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

## Article 10
## National 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 national contact point. The contact point shall supply such data in accordance with the national law of 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 of 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.

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

1. For the prevention of serious criminal and terrorist offenses, the Parties may, in compliance with their respective national law, in individual cases, even without being requested to do so, supply the other Party's relevant national contact point, as referred to in paragraph 6, with the personal data specified in paragraph 2, in so far as is necessary because particular circumstances give reason to believe that the data subject(s):

   a. will commit or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association, as those offenses are defined under the supplying Party's national law; or

   b. is undergoing or has undergone training to commit the offenses referred to in subparagraph a; or

   c. will commit or has committed a serious criminal offense, or participates in an organized criminal group or association.

2. The personal data to be supplied 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, in compliance with its national law, impose conditions on the use that may be made of such data by the receiving Party. If the receiving Party accepts such data, it shall be bound by any such conditions.

4. Generic restrictions with respect to the legal standards of the receiving Party for processing personal data may not be imposed by the transmitting Party as a condition under paragraph 3 to providing data.

5. In addition to the personal data referred to in paragraph 2, the Parties may provide each other with non-personal data related to the offenses set forth in paragraph 1.

6. Each Party shall designate one or more national contact points for the exchange of personal and other data under this Article with the other Party's contact points. The powers of the national contact points shall be governed by the national law applicable.

**Article 12**
**Privacy and Data Protection**

1. The Parties recognize that the handling and processing of personal data that they acquire from each other is of critical importance to preserving confidence in the implementation of this Agreement.

2. The Parties commit themselves to processing personal data fairly and in accord with their respective laws and:

   a. ensuring that the personal data provided are adequate and relevant in relation to the specific purpose of the transfer;

   b. retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Agreement; and

   c. ensuring that possibly inaccurate personal data are timely brought to the attention of the receiving Party in order that appropriate corrective action is taken.

3. This Agreement shall not give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data. Rights existing independently of this Agreement, however, are not affected.

**Article 13**
**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 particularly relevant to the purposes 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 14
## Limitation on processing to protect personal and other data

1. Without prejudice to Article 11, paragraph 3, each Party may process data obtained under this Agreement:

   a. for the purpose of its criminal investigations;

   b. for preventing a serious threat to its public security;

   c. in its non-criminal judicial or administrative proceedings directly related to investigations set forth in subparagraph (a); or

   d. for any other purpose, only with the prior consent of the Party which has transmitted the data.

2. The Parties shall not communicate data provided under this Agreement to any third State, international body or private entity without the consent of the Party that provided the data and without the appropriate safeguards.

3. A Party may conduct an automated query of the other Party's fingerprint or DNA files under Articles 4 or 8, and process data received in response to such a query, including the communication whether or not a hit exists, solely in order to:

   a. establish whether the compared DNA profiles or fingerprint data match;

   b. prepare and submit a follow-up request for assistance in compliance with national law, including the legal assistance rules, if those data match; or

   c. conduct record-keeping, as required or permitted by its national law.

4. The Party administering the file may process the data supplied to it by the querying Party during the course of an automated query in accordance with Articles 4 and 8 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Article 16. The data supplied for comparison shall be deleted immediately following data comparison or automated replies to queries unless further processing is necessary for the purposes mentioned under this Article, paragraph 3, subparagraphs (b) or (c).

## Article 15
## Correction, blockage and deletion of data

1. At the request of the supplying Party, the receiving Party shall be obliged to correct, block, or delete, consistent with its national law, data received under this Agreement that are incorrect or incomplete or if its collection or further processing contravenes this Agreement or the rules applicable to the supplying Party.

2. Where a Party becomes aware that data it has received from the other Party under this Agreement are not accurate, it shall take all appropriate measures to safeguard against

erroneous reliance on such data, which shall include in particular supplementation, deletion, or correction of such data.

3. Each Party shall notify the other if it becomes aware that material data it has transmitted to the other Party or received from the other Party under this Agreement are inaccurate or unreliable or are subject to significant doubt.

## Article 16
## Documentation

1. Each Party shall maintain a record of the transmission and receipt of data communicated to the other Party under this Agreement. This record shall serve to:

   a. ensure effective monitoring of data protection in accordance with the national law of the respective Party;

   b. enable the Parties to effectively make use of the rights granted to them according to Articles 14 and 18; and

   c. ensure data security.

2. The record shall include:

   a. information on the data supplied;

   b. the date of supply; and

   c. the recipient of the data in case the data are supplied to other entities.

3. The recorded data 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 recorded data shall be deleted immediately, unless this is inconsistent with national law, including applicable data protection and retention rules.

## Article 17
## Data Security

1. The Parties shall ensure that the necessary technical measures and organizational arrangements are utilized to protect personal data against accidental or unlawful destruction, accidental loss or unauthorized disclosure, alteration, access or any unauthorized form of processing. The Parties in particular shall reasonably take measures to ensure that only those authorized to access personal data can have access to such data.

2. The implementing agreements or arrangements that govern the procedures for automated querying of fingerprint and DNA files pursuant to Articles 4 and 8 shall provide:

   a. that appropriate use is made of modern technology to ensure data protection, security, confidentiality and integrity;

b. that encryption and authorization procedures recognized by the competent authorities are used when having recourse to generally accessible networks; and

c. for a mechanism to ensure that only permissible queries are conducted.

**Article 18**
**Transparency – Providing information to the data subjects**

1. Nothing in this Agreement shall be interpreted to interfere with the Parties' legal obligations, as set forth by their respective laws, to provide data subjects with information as to the purposes of the processing and the identity of the data controller, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him or her and any further information such as the legal basis of the processing operation for which the data are intended, the time limits for storing the data and the right of recourse, in so far as such further information is necessary, having regard for the purposes and the specific circumstances in which the data are processed, to guarantee fair processing with respect to data subjects.

2. Such information may be denied in accordance with the respective laws of the Parties, including if providing this information may jeopardize:

   a. the purposes of the processing;

   b. investigations or prosecutions conducted by the competent authorities in the United States or by the competent authorities in Iceland; or

   c. the rights and freedoms of third parties.

**Article 19**
**Information**

Upon request, the receiving Party shall inform the supplying Party of the processing of supplied data and the result obtained. The receiving Party shall ensure that its answer is communicated to the supplying Party in a timely manner.

**Article 20**
**Relation to Other Agreements**

Nothing in this Agreement shall be construed to limit or prejudice the provisions of any treaty, other agreement, working law enforcement relationship, or domestic law allowing for information sharing between the United States and Iceland.

**Article 21**
**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 22**
**Expenses**

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

**Article 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 note completing an exchange of diplomatic notes between the Parties indicating that each has taken any steps necessary to bring the 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 their domestic law.

2. Articles 8 through 10 of this Agreement shall enter into force following the conclusion of the implementing agreement(s) or arrangement(s) referenced in Article 10 and on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each Party is able to implement those articles on a reciprocal basis. This exchange shall occur if the laws of both Parties permit the type of DNA screening contemplated by Articles 8 through 10.

Done at Reykjavik this 14th day of May 2012, in duplicate, in the English and Icelandic languages, both texts being equally authentic.

For the Government of

the United States of America:

Ambassador Luis E. Arreaga

For the Government of

Iceland:

Ambassador Jón Egill Egilsson

**Samningur milli**
**ríkisstjórnar Bandaríkja Ameríku og ríkisstjórnar Íslands**
**um að auka samstarf um að koma í veg fyrir og berjast gegn**
**alvarlegum glæpum**

Ríkisstjórn Bandaríkja Ameríku og ríkisstjórn Íslands (hér á eftir nefndar „samningsaðilar“),

sem vilja eiga samstarf um að koma í veg fyrir og berjast gegn alvarlegum glæpum, einkum hryðjuverkum, á skilvirkari hátt,

sem viðurkenna að upplýsingaskipti eru grundvallarþáttur í baráttunni gegn alvarlegum glæpum, einkum hryðjuverkum,

sem viðurkenna mikilvægi þess að koma í veg fyrir og berjast gegn alvarlegum glæpum, einkum hryðjuverkum, og virða um leið grundvallarréttindi og frelsi, einkum friðhelgi einkalífs, og

sem leitast við að auka og hvetja til samstarfs samningsaðilanna í anda samvinnu,

hafa orðið ásáttar um eftirfarandi:

**1. gr.**
**Skilgreiningar**

Í samningi þessum hafa eftirfarandi hugtök þá merkingu sem hér greinir:

1. Refsivörslumarkmið skulu taka til starfsemi sem lýtur að framkvæmd refsivörslu og athafna sem felast í eftirfarandi: að hafa upp á, handtöku, varðhaldi, lausn úr haldi fyrir réttarhald, lausn úr haldi eftir réttarhald, saksókn, dómsálagningu, betrunarvist eða endurhæfingu sakborninga eða brotamanna. Framkvæmd refsivörslu felur einnig í sér ráðstafanir til að ljóstra upp um glæpi.

2. DNA-snið (erfðagerð) skulu merkja upplýsingar um erfðaefni táknaðar með bókstaf eða talnakóða sem sýnir fjölda auðkennandi eiginleika í greindu DNA-sýni án táknraða, þ.e. sérstakt efnafræðilegt form á mismunandi stöðum á DNA-sameindinni.

3. Persónuupplýsingar skulu merkja hvers konar upplýsingar um persónugreindan eða persónugreinanlegan einstakling („skráður aðili“).

4. Vinnsla persónuupplýsinga skal merkja hverja þá aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort sem vinnsla þeirra er sjálfvirk eða ekki, svo sem þegar

þeim er safnað eða þær skráðar, þeim er raðað, þær geymdar eða aðlagaðar, þeim er breytt, þær flokkaðar, sóttar, þeim flett upp, þær notaðar, afhjúpaðar með afhendingu, þeim er miðlað, þær sendar eða á annan hátt gerðar aðgengilegar, þær settar saman eða tengdar, aðgangur að þeim hindraður eða þeim eytt með því að þurrka þær út eða eyðileggja.

5. Tilvísunargögn skal merkja DNA-snið og tengda tilvísun (DNA- tilvísunargögn) eða fingrafaraupplýsingar og tengda tilvísun (tilvísunargögn fingrafaraupplýsinga). Í tilvísunargögnum mega ekki vera upplýsingar af neinu tagi sem hægt er að nota til að auðkenna skráðan aðila. Tilvísunargögn sem ekki er hægt að rekja til einstaklings (órekjanleg) verða að vera greinanleg sem slík.

6. Alvarlegir glæpir skal merkja, í því skyni að hrinda ákvæðum samnings þessa í framkvæmd, háttsemi sem er brot er varðar frelsissviptingu í eitt ár eða lengur eða sem þyngri refsing liggur við. Til að tryggja samræmi við landslög sín geta samningsaðilar komið sér saman um að tilgreina að tilteknir alvarlegir glæpir skyldi samningsaðila ekki til að afhenda persónuupplýsingar, eins og lýst er í 6. gr. og 9. gr. samningsins.

**2. gr.**
**Markmið samningsins**

1. Markmiðið með samningi þessum er að bæta samvinnu milli Bandaríkja Ameríku og Íslands um að koma í veg fyrir og berjast gegn alvarlegum glæpum.

2. Heimildir til þess að gera fyrirspurnir, sem kveðið er á um í samningi þessum, skal einungis nota til þess að koma í veg fyrir, ljóstra upp um og rannsaka glæpi.

**3. gr.**
**Fingrafaraupplýsingar**

Samningsaðilarnir skulu, í því skyni að hrinda ákvæðum samnings þessa í framkvæmd, tryggja að tilvísunargögn úr skrá fyrir sjálfvirkt kerfi til fingrafaragreiningar, sem komið var á fót til að koma í veg fyrir og rannsaka refsilagabrot, séu tiltæk. Tilvísunargögn skulu eingöngu innihalda fingrafaraupplýsingar ásamt tilvísun.

**4. gr.**
**Sjálfvirk fyrirspurn um fingrafaraupplýsingar**

1. Hvor samningsaðili skal, til að koma í veg fyrir og rannsaka alvarlega glæpi, heimila innlendum tengiliðum hins samningsaðilans, sem um getur í 7. gr., aðgang að tilvísunargögnum í sjálfvirku kerfi til fingrafaragreiningar sem fyrrnefndi samningsaðilinn hefur komið á fót í því skyni, ásamt valdheimild til þess að senda sjálfvirka fyrirspurn með samanburði á fingrafaraupplýsingum. Einungis má gera slíkar fyrirspurnir í einstökum tilvikum og í samræmi við landslög samningsaðilans sem sendir fyrirspurnina.

2. Innlendir tengiliðir, sem gera fyrirspurnir, skulu bera saman fingrafaraupplýsingar við tilvísunargögn í vörslu þess samningsaðila sem hefur skrána undir höndum með því að

styðjast við sjálfvirka sendingu þeirra tilvísunargagna sem nauðsynleg eru til að fá skýra samsvörun.

3. Ef nauðsyn krefur, er heimilt að frekari greining til að staðfesta samsvörun fingrafaraupplýsinga við tilvísunargögn í vörslu samningsaðila, sem hefur skrána undir höndum, fari fram hjá innlendum tengilið sem fyrirspurn er beint til.

**5. gr.**
**Aðrar aðferðir við fyrirspurnir með auðkenningargögnum**

Þar til Ísland hefur tekið í fulla notkun sjálfvirkt kerfi til fingrafaragreiningar, sem tengt er við einstakar sakaskrár, og er reiðubúið til að veita Bandaríkjum Ameríku sjálfvirkan aðgang að slíku kerfi, skal það gera aðrar ráðstafanir til að hægt sé að senda fyrirspurnir með annars konar auðkenningargögnum til að finna skýra samsvörun sem tengir einstaklinginn við viðbótarupplýsingar. Heimildum til fyrirspurna skal beitt með sama hætti og kveðið er á um í 4. gr. og skal fara með skýra samsvörun á sama hátt og trausta samsvörun við fingrafaraupplýsingar svo unnt sé að láta af hendi viðbótarupplýsingar eins og kveðið er á um í 6. gr.

**6. gr.**
**Afhending frekari persónuupplýsingar eða annarra gagna**

Komi fram samsvörun milli fingrafaraupplýsinga þegar málsmeðferðinni sem um getur í 4. gr. er beitt, eða leiði málsmeðferðin sem beitt er skv. 5. gr. til samsvörunar, skulu landslög þess samningsaðila sem fyrirspurn er beint til, þ.m.t. reglur um réttaraðstoð, gilda um afhendingu frekari fyrirliggjandi persónuupplýsinga og annarra gagna er varða tilvísunargögnin, og skulu þessar upplýsingar og gögn afhent í samræmi við ákvæði 7. gr.

**7. gr.**
**Innlendir tengiliðir og samningar um framkvæmd**

1. Hvor samningsaðili skal tilnefna einn eða fleiri innlenda tengiliði vegna afhendingar gagna sbr. ákvæði 4. og 5. gr. og síðari sendingu frekari persónuupplýsinga sbr. ákvæði 6. gr. Tengiliðurinn skal afhenda slík gögn í samræmi við ákvæði landslaga samningsaðilans sem tilnefnir tengiliðinn. Ekki er nauðsynlegt að nýta aðra réttaraðstoð nema nauðsyn krefji, þ.m.t. til að staðfesta slík gögn í því skyni að gera þau nothæf við dómsmeðferð hjá þeim samningsaðila sem sendir fyrirspurn.

2. Einstökum atriðum, sem lúta að tækni og verklagi og varða fyrirspurnir sem gerðar eru skv. 4. og 5. gr., skal lýst í einum eða fleiri samningum eða samkomulagi um framkvæmd.

**8. gr.**
**Sjálfvirk fyrirspurn um DNA-snið**

1. Samningsaðilar geta, svo fremi að landslög þeirra heimili það og á grundvelli gagnkvæmni, veitt innlendum tengiliði hvors annars, sem um getur í 10. gr., aðgang að

tilvísunargögnum í DNA-greiningarskrám og heimilað þeim að framkvæma sjálfvirkar fyrirspurnir með samanburði á DNA-sniðum í þágu rannsóknar á alvarlegum glæp. Einungis má framkvæma fyrirspurnir í einstaklingsbundnum tilvikum og í samræmi við landslög samningsaðilans sem framkvæmir fyrirspurn.

2. Leiði sjálfvirk fyrirspurn í ljós að DNA-snið sem var látið í té samsvari DNA-sniði í skrá hins samningsaðilans, skal innlendi tengiliðurinn sem framkvæmir fyrirspurn fá senda sjálfvirka tilkynningu um tilvísunargögn sem samsvörun hefur fundist við. Ef engin samsvörun finnst skal sjálfvirk tilkynning berast þess efnis.

**9. gr.**
**Afhending frekari persónuupplýsinga og annarra gagna**

Ef málsmeðferðin sem um getur í 8. gr. sýnir samsvörun milli DNA-sniða gilda landslög þess samningsaðila sem fyrirspurn er beint til, þ.m.t. reglur um réttaraðstoð, um afhendingu frekari fyrirliggjandi persónuupplýsinga eða annarra upplýsinga sem tengjast tilvísunargögnunum og skulu upplýsingarnar afhentar í samræmi við ákvæði 10. gr.

**10. gr.**
**Innlendur tengiliður og samningar um framkvæmd**

1. Hvor samningsaðili skal tilnefna einn eða fleiri innlenda tengiliði vegna afhendingar gagna sem fjallað er um í 8. gr. og síðari sendingu frekari persónuupplýsinga sbr. ákvæði 9. gr. Tengiliðurinn skal afhenda slík gögn í samræmi við ákvæði landslaga samningsaðilans sem tilnefnir tengiliðinn. Ekki er nauðsynlegt að nýta aðra réttaraðstoð nema nauðsyn krefji, þ.m.t. til að staðfesta slík gögn í því skyni að gera þau nothæf við dómsmeðferð hjá þeim samningsaðila sem sendir fyrirspurn.

2. Einstökum atriðum, sem lúta að tækni og verklagi og varða fyrirspurnir sem gerðar eru skv. 8. gr., skal lýst í einum eða fleiri samningum eða samkomulagi um framkvæmd.

**11. gr.**
**Afhending persónuupplýsinga og annarra gagna**
**til þess að koma í veg fyrir alvarlega glæpi og hryðjuverk**

1. Til að koma í veg fyrir alvarlega glæpi og hryðjuverk geta samningsaðilar, í samræmi ákvæði landslaga hvors um sig, í einstökum tilvikum, jafnvel án beiðni þar að lútandi, afhent innlendum tengilið hins samningsaðilans, eins og um getur í 6. mgr., persónuupplýsingar sem tilgreindar eru í 2. mgr., að því marki sem nauðsyn krefur, þar eð sérstakar aðstæður gefi tilefni til að ætla að skráður aðili:

   a. muni fremja eða hafi framið hryðjuverk eða brot sem tengist hryðjuverkum, eða brot sem tengjast hryðjuverkahópi eða -samtökum eins og þau brot eru skilgreind samkvæmt landslögum samningsaðilans sem afhendir upplýsingarnar, eða

   b. gangist undir eða hafi gengist undir þjálfun til að fremja þau brot sem um getur í a-lið, eða

c. muni fremja eða hafi framið alvarlegan glæp eða tekið þátt í skipulögðum glæpahópi eða -samtökum.

2. Persónuupplýsingarnar sem senda á geta falið í sér eftirfarandi upplýsingar, ef þær eru tiltækar, kenninafn, eiginnöfn, fyrri nöfn, önnur nöfn, tökuheiti, annan rithátt nafna, kynferði, fæðingardag og fæðingarstað, núverandi og fyrrverandi ríkisfang, vegabréfsnúmer, númer annarra persónuskilríkja og fingrafaraupplýsingar, auk lýsingar á sakfellingu eða kringumstæðum sem gefa tilefni til þeirra ályktana sem um getur í 1. mgr.

3. Samningsaðilinn sem lætur upplýsingar í té, getur samkvæmt landslögum sínum, sett skilyrði fyrir notkun samningsaðilans, sem er viðtakandi slíkra upplýsinga. Ef samningsaðilinn sem er viðtakandi tekur við slíkum upplýsingum skal hann bundinn af slíkum skilyrðum.

4. Samningsaðilanum sem lætur upplýsingar í té er óheimilt að setja almennar takmarkanir, að því er varðar lagareglur þess samningsaðila sem er viðtakandi og sem gilda um meðferð slíkra upplýsinga, sem skilyrði skv. 3. mgr. fyrir afhendingu persónuupplýsinga.

5. Til viðbótar þeim persónuupplýsingum sem um getur í 2. mgr., geta samningsaðilarnir sent hvor öðrum gögn sem ekki eru persónulegs eðlis og tengjast brotum sem um getur í 1. mgr.

6. Hvor samningsaðili skal tilnefna einn eða fleiri innlenda tengiliði sem annast skipti á persónuupplýsingum og öðrum gögnum samkvæmt þessari grein við tengiliði hins samningsaðilans. Heimildir innlendra tengiliða skulu ákvarðast af gildandi landslögum.

**12. gr.**
**Persónuvernd og gagnavernd**

1. Samningsaðilar viðurkenna að meðferð og vinnsla persónuupplýsinga, sem þeir fá hvor frá öðrum hefur grundvallarþýðingu fyrir traust á framkvæmd þessa samnings.

2. Samningsaðilar skuldbinda sig til að vinna með persónuupplýsingar af sanngirni og í samræmi við lög hvors um sig og til að:

   a. tryggja að veittar persónuupplýsingar séu fullnægjandi og í samræmi við sérstakt tilefni þess að þær eru sendar,

   b. varðveita persónuupplýsingar einungis svo lengi sem þörf krefur í þeim sérstaka tilgangi sem var tilefni sendingar upplýsinganna eða frekari vinnslu þeirra í samræmi við ákvæði samnings þessa, og

   c. tryggja að athygli samningsaðilans sem er viðtakandi sé vakin tímanlega á því ef persónuupplýsingar kunna að vera ónákvæmar svo hægt sé að gera viðeigandi leiðréttingu.

3. Samningur þessi skal ekki leiða til þess að einstaklingur öðlist rétt, m.a. til þess að fá, halda leyndum eða útiloka sönnunargögn eða koma í veg fyrir að persónuupplýsingum sé deilt. Réttur, sem er í gildi óháð þessum samningi, stendur óhaggaður.

## 13. gr.
## Frekari vernd sendingar sérstakra flokka persónuupplýsinga

1. Einungis má veita persónuupplýsingar sem leiða í ljós kynþátt eða þjóðerni, stjórnmálaskoðanir, trúarskoðanir, aðrar skoðanir eða aðild að verkalýðsfélögum, eða upplýsingar sem varða heilsu eða kynhegðun, ef þær hafa sérstaka þýðingu að því er samning þennan varðar.

2. Að teknu tilliti til þess hversu viðkvæmir ofangreindir flokkar persónuupplýsinga eru skulu samningsaðilar gera viðeigandi verndarráðstafanir, einkum viðeigandi öryggisráðstafanir, til þess að vernda slíkar upplýsingar.

## 14. gr.
## Takmörkun á vinnslu til að vernda persónuupplýsingar og önnur gögn

1. Hvorum samningsaðila er heimilt, samanber þó 3. mgr. 11. gr., að vinna gögn sem fengin eru samkvæmt samningi þessum:

   a. vegna rannsóknar sakamáls,

   b. til þess að koma í veg fyrir alvarlega ógn við almannaöryggi,

   c. í öðrum málum en sakamálum vegna málsmeðferðar fyrir dómi eða innan stjórnsýslunnar sem tengjast með beinum hætti rannsóknum sem um getur í a-lið, eða

   d. í einhverjum öðrum tilgangi svo fremi að samningsaðilinn sem sendi gögnin hafi veitt samþykki sitt fyrir fram.

2. Samningsaðilar skulu ekki senda gögn sem fengin eru samkvæmt samningi þessum til þriðja ríkis, alþjóðlegrar stofnunar eða einkakaaðila án samþykkis samningsaðilans sem lét gögnin í té og án viðeigandi verndarráðstafana.

3. Samningsaðili getur framkvæmt sjálfvirka fyrirspurn í fingrafara- og DNA-skrám hins samningsaðilans skv. 4. gr. og 8. gr. og unnið gögn sem berast sem svar við slíkri fyrirspurn, þ.m.t. upplýsingar um hvort samsvörun finnst eða ekki, í þeim eina tilgangi að:

   a. staðfesta hvort samsvörun finnist við samanburð DNA-sniða eða fingrafaraupplýsinga,

   b. undirbúa og senda beiðni um frekari aðstoð í samræmi við landslög, þ.m.t. reglur um réttaraðstoð, ef samsvörun finnst í gögnunum, eða

   c. sinna skráningu, eftir því sem innlend lög heimila eða krefjast.

4. Samningsaðili, sem hefur umsjón með viðkomandi skrá, má vinna gögn látin í té af samningsaðila sem framkvæmir fyrirspurn á meðan á vinnslu sjálfvirkrar fyrirspurnar stendur, skv. ákvæðum 4. gr. og 8. gr., aðeins í þeim tilfellum þegar það er nauðsynlegt vegna samanburðar, sjálfvirkrar svörunar við fyrirspurninni eða skýrsluhalds skv. 16. gr. Gögnum, sem aflað er til samanburðar, skal eytt án tafar að loknum samanburði eða sjálfvirkri svörun við fyrirspurnum, nema frekari vinnsla sé nauðsynleg af ástæðum sem um getur í b- eða c-lið 3. mgr. þessarar greinar.

## 15. gr.
## Leiðrétting, aðgangshindrun og eyðing gagna

1. Að beiðni samningsaðila, sem afhendir gögn, skal samningsaðila, sem er viðtakandi, skylt að leiðrétta, hindra aðgang að eða eyða, í samræmi við landslög sín, þeim gögnum sem veitt er viðtaka samkvæmt samningi þessum og eru röng eða ófullnægjandi, eða ef söfnun þeirra eða frekari vinnsla stríðir gegn samningi þessum eða þeim reglum sem gilda um samningsaðilann sem sendir gögn.

2. Verði samningsaðili var við að gögn, sem hann veitir viðtöku frá hinum samningsaðilanum samkvæmt samningi þessum, séu ónákvæm skal hann gera allar viðeigandi ráðstafanir til þess að varna því að slíkum gögnum sé ranglega treyst, og skal það einkum felast í því að viðbætur hafi verið gerðar, að gögnunum hafi verið eytt eða að þau hafi verið leiðrétt.

3. Verði annar samningsaðilanna var við að efnisleg gögn, sem hann hefur sent hinum samningsaðilanum eða veitt viðtöku frá hinum samningsaðilanum samkvæmt samningi þessum, séu ónákvæm eða óáreiðanleg, eða að umtalsverðar efasemdir séu uppi um þau, skal hann tilkynna hinum samningsaðilanum um það.

## 16. gr.
## Skjalfesting

1. Hvor samningsaðili skal, samkvæmt samningi þessum, halda skrá yfir gögn send og móttekin í samskiptum við hinn samningsaðilann. Slík skrá skal þjóna þeim tilgangi:

   a. að tryggja skilvirkt eftirlit með gagnavernd í samræmi við landslög hlutaðeigandi samningsaðila,

   b. að gera samningsaðilunum kleift að nýta sér rétt sinn skv. 14. gr. og 18. gr. til hlítar, og

   c. tryggja gagnaöryggi.

2. Skráin skal innihalda:

   a. upplýsingar um send gögn,

   b. dagsetningu sendingar, og

   c. viðtakanda gagnanna, séu þau afhent öðrum aðilum.

3. Vernda skal skráð gögn á viðeigandi hátt gegn óviðeigandi notkun og annars konar rangri notkun og skulu þau varðveitt í tvö ár. Að geymslutíma loknum skal skráðum gögnum eytt án tafar, nema það brjóti í bága við landslög, þ.m.t. gildandi reglur um gagnavernd og varðveislu gagna.

## 17. gr.
## Gagnaöryggi

1. Samningsaðilar skulu tryggja að nauðsynlegar tæknilegar ráðstafanir og skipulagsráðstafanir séu gerðar til þess að vernda persónuupplýsingar gegn óviljandi eða ólöglegri eyðileggingu, eða gegn því að þær glatist fyrir slysni eða vegna ólöglegrar upplýsingagjafar eða breytingar, ólöglegs aðgangs eða annars konar ólöglegrar vinnslu. Samningsaðilar skulu gera hæfilegar ráðstafanir til tryggja að einungis þeir, sem er heimilaður aðgangur að persónuupplýsingum, hafi aðgang að þeim.

2. Samningar eða samkomulag til framkvæmdar samningnum, sem gildir um tilhögun sjálfvirkra fyrirspurna í fingrafaraupplýsingum og DNA-sniðum samkvæmt 4. gr. og 8. gr., skal kveða á um:

   a. að nútímatækni sé notuð á viðeigandi hátt til að tryggja gagnavernd, öryggi, að þagnarskyldu sé gætt og ráðvendni,

   b. að notuð sé dulkóðun og málsmeðferð við leyfisveitingu sem viðurkennd er af lögbærum stjórnvöldum þegar þarf að nota net sem almennt eru aðgengileg, og

   c. fyrirkomulag til að tryggja að einungis leyfilegar fyrirspurnir séu framkvæmdar.

## 18. gr.
## Gagnsæi – upplýsingar veittar skráðum aðilum

1. Ekkert í samningi þessum skal túlkað þannig að það hafi áhrif á lagalegar skyldur samningsaðilanna, sem settar eru fram í viðkomandi lögum hvors fyrir sig, til að veita skráðum aðilum upplýsingar um tilganginn með vinnslu gagnanna og um það hver ábyrgðaraðili gagnanna sé, um viðtakendur eða flokka viðtakenda, þann rétt sem gildir um aðgang að gögnum og rétt til að lagfæra gögn um þá aðila og allar frekari upplýsingar, svo sem lagalegan grundvöll ráðgerðrar vinnslu á gögnunum, um það hversu lengi sé heimilt að geyma gögnin og um endurkröfurétt, að svo miklu leyti sem slíkar frekari upplýsingar eru nauðsynlegar, með hliðsjón af tilganginum og þeim sérstöku aðstæðum sem eru tilefni vinnslu gagnanna, í því skyni að tryggja réttláta vinnslu gagnvart þeim skráðu aðilum sem um ræðir.

2. Heimilt er að hafna því að veita slíkar upplýsingar í samræmi við við lög hvors samningsaðila fyrir sig, meðal annars af þeirri ástæðu að slíkar upplýsingar gætu stofnað í hættu:

   a. tilgangi vinnslunnar,

   b. rannsókn eða saksókn af hálfu lögbærra stjórnvalda í Bandaríkjum Ameríku eða lögbærra stjórnvalda á Íslandi, eða

c. rétti og frelsi þriðju aðila.

**19. gr.**
**Upplýsingar**

Sá samningsaðili sem er viðtakandi upplýsinga skal, að fram kominni beiðni þar um, upplýsa samningsaðilann sem lét gögnin af hendi um vinnslu þeirra og þær niðurstöður sem hún skilaði. Samningsaðili sem er viðtakandi skal sjá til þess að svarið berist þeim samningsaðila sem afhenti gögnin tímanlega.

**20. gr.**
**Tengsl við aðra samninga**

Ekkert í samningi þessum skal túlkað þannig að það takmarki eða rýri ákvæði annarra samninga eða samkomulags, samvinnu sem lýtur að því að framfylgja lögum eða innlendra laga sem heimila skipti á upplýsingum milli Bandaríkja Ameríku og Íslands.

**21. gr.**
**Samráð**

1. Samningsaðilar skulu hafa með sér reglulegt samráð um framkvæmd samnings þessa.

2. Komi upp ágreiningur varðandi túlkun eða beitingu ákvæða samnings þessa skulu samningsaðilar hafa samráð sín á milli í því skyni að finna lausn á honum.

**22. gr.**
**Útgjöld**

Hvor samningsaðili skal bera þann kostnað sem yfirvöld hans hafa af því að hrinda ákvæðum samnings þessa í framkvæmd. Í sérstökum tilvikum geta samningsaðilar komið sér saman um annars konar tilhögun.

**23. gr.**
**Uppsögn samningsins**

Hvor samningsaðili sem er getur sagt upp samningi þessum með því að tilkynna hinum samningsaðilanum um það skriflega með þriggja mánaða fyrirvara. Ákvæði samnings þessa skulu gilda áfram um gögn sem eru afhent áður en til slíkrar uppsagnar kemur.

**24. gr.**
**Breytingar**

1. Samningsaðilar skulu efna til samráðs um breytingar á samningi þessum að beiðni hvors samningsaðila sem er.

2. Samningi þessum má breyta með skriflegu samþykki samningsaðila hvenær sem er.

## 25. gr.
## Gildistaka

1. Samningur þessi öðlast gildi, að undanskildum 8. til 10. gr., þann dag sem seinni orðsendingin er dagsett að afloknum diplómatískum orðsendingaskiptum milli samningsaðilanna sem gefa til kynna að hvor um sig hafi gert nauðsynlegar ráðstafanir til þess að samningurinn megi öðlast gildi. Áskilið er að samningsaðilar beiti ákvæðum samnings þessa, að undanskildum 8. til 10. gr., frá undirritunardegi að því marki að það samræmist innlendum lögum hvors fyrir sig.

2. Greinar 8 til 10 í samningi þessum öðlast gildi að lokinni gerð samnings eða samninga eða samkomulags um framkvæmd er um getur í 10. gr. og þann dag sem seinni orðsendingin er dagsett að afloknum diplómatískum orðsendingaskiptum milli samningsaðilanna sem gefa til kynna að hvor um sig geti beitt ákvæðum fyrrnefndra greina með gagnkvæmum hætti. Orðsendingaskipti þessi skulu fara fram heimili löggjöf beggja samningsaðila þá gerð DNA-skimunar sem er fyrirséð samkvæmt 8. til 10. gr.

Gjört í Reykjavík hinn 14. dag Maí mánaðar 2012, í tvíriti, á ensku og íslensku og eru báðir textar jafngildir.

Fyrir hönd ríkisstjórnar

Bandaríkja Ameríku:

Ambassador Luis E. Arreaga

Fyrir hönd ríkisstjórnar

Íslands:

Ambassdor Jón Egill Egilsson