LAW ENFORCEMENT

Cooperation

Agreement Between the
UNITED STATES OF AMERICA
and LATVIA

Signed at Riga September 29, 2008

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."

LATVIA

Law Enforcement: Cooperation

Agreement signed at Riga
September 29, 2008;
Entered into force July 20, 2010,
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 the Republic of Latvia On Enhancing Cooperation in Preventing and Combating Serious Crime

The Government of the United States of America and the Government of the Republic of Latvia (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,

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, as well as the related June 18, 2007 European Council decision, and

Seeking to enhance and encourage cooperation between the Parties in the spirit of partnership, and seeking therefore to respect existing international obligations, including obligations of the Republic of Latvia arising from its membership in the European Union,

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 Articles 4 and 5 of this Agreement, conduct constituting an offense punishable by a maximum deprivation of liberty of more than one year or a more serious penalty.
   a. For the United States of America, serious crimes shall be deemed also to include any criminal offense that would render an individual inadmissible to or removable from the United States of America under U.S. federal law.
   b. For the Republic of Latvia serious crimes shall be deemed to also include any criminal offense that would render an individual inadmissible to or removable from the Republic of Latvia under the national law of the Republic of Latvia.

   To ensure compliance with their national laws, the Parties may agree to specify particular serious crimes for which a Party shall supply personal data as described in Articles 6 and 9 of the Agreement.

Article 2
Purpose of this Agreement

The purpose of this Agreement is to enhance the cooperation between the Republic of Latvia and the United States of America in preventing and combating serious 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 searching 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 searches by comparing fingerprinting data. Search powers may be exercised only in individual cases and in compliance with the searching Party's national law.
2. Firm matching of fingerprinting data with reference data held by the Party in charge of the file shall be carried out by the searching national contact points by means of the automated supply of the reference data required for a clear match.
3. The Parties agree that the search powers provided for in this Agreement may be exercised for border security reasons in situations when an individual for whom the additional data is sought has been identified for further inspection. The search powers provided for under this Agreement shall be used only for a criminal justice purpose.

Article 5
Alternative means to search using identifying data

1. With regard to the search powers in Article 4, until the Republic of Latvia has a fully operational and automated fingerprint identification system that links to individual criminal records and is prepared to provide the United States of America with automated access to such a system, it shall ensure an alternative means to determine by using other identifying data whether the person of concern has been convicted of committing a serious crime. If the person of concern is registered as convicted, any available data related to the person of concern shall be supplied in accordance with the national law, including the legal assistance rules, of the requested Party.
2. Such an alternative means shall be implemented in accordance with Article 4, paragraph 3.
3. The technical and procedural details for the use of an alternative means shall be set out in one or more implementing agreements or arrangements.

Article 6
Supply of further personal and other data

Should the procedure referred to in Article 4 show a match between fingerprinting data, the supply of any available further personal data and other data relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Party.

Article 7
National contact points and implementing agreements

1. For the purpose of the supply of data as referred to in Articles 4 and 5, each Party shall designate one or more national contact points. The powers of the contact points shall be governed by the national law applicable.
2. The technical and procedural details for the searching conducted pursuant to Articles 4 and 5 shall be set forth in one or more implementing agreements or arrangements.

Article 8
Automated searching 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 searches by comparing DNA profiles for the investigation of serious crime. Searches may be exercised only in individual cases and in compliance with the searching Party's national law.
2. Should an automated search show that a DNA profile supplied matches a DNA profile entered in the other Party's file, the searching 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.

Article 10
National contact point and implementing agreements

1. For the purposes of the supply of data as set forth in Article 8, each Party shall designate a national contact point. The powers of the contact point shall be governed by the national law applicable.
2. The technical and procedural details for the searching 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, a Party may, in compliance with its 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 shall 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 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 is adequate and relevant in relation to the specific purpose of the transfer;
   b. retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Agreement; and
   c. ensuring that possibly inaccurate personal data is timely brought to the attention of the receiving Party in order that appropriate corrective action is taken.
3. This Agreement shall not give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data. Rights existing independently of this Agreement, however, shall not be 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, the Parties 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 search of the other Party's fingerprint or DNA files under Articles 4 or 8, and process data received in response to such a search, 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.

The Party administering the file may process the data supplied to it by the searching Party during the course of an automated search in accordance with Articles 4 and 8 solely where this is necessary for the purposes of comparison, providing automated replies to the search or record-keeping pursuant to Article 16. The data supplied for comparison shall be deleted immediately following data comparison or automated replies to searches 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 is not accurate, it shall take all appropriate measures to safeguard against erroneous reliance on such data, which shall include in particular supplementation, deletion, or correction of such data.
3. Each Party shall notify the other if it becomes aware that material data it has transmitted to the other Party or received from the other Party under this Agreement 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 15 and 19; 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 is supplied to other entities.
3. The recorded data must be protected with suitable measures against inappropriate use and other forms of improper use and must be kept for two years. After the conservation period the recorded data must 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 searches 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 searches 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 Republic of Latvia or by the competent authorities in the United States of America; 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 Republic of Latvia and the United States of America.

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

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. 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..Riga..., this ..29th..day of September 2008, in duplicate in the Latvian and English languages, both texts being equally authentic.

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:

FOR THE GOVERNMENT OF THE REPUBLIC OF LATVIA:

Amerikas Savienoto Valstu valdības un Latvijas Republikas valdības līgums par sadarbības pastiprināšanu smago noziegumu novēršanā un apkarošanā

Amerikas Savienoto Valstu valdība un Latvijas Republikas valdība (turpmāk – Puses),

vadoties no apņēmības efektīvāk savstarpēji sadarboties smago noziegumu, it īpaši terorisma, novēršanā un apkarošanā;

apzinoties, ka informācijas apmaiņa ir viens no būtiskākajiem elementiem cīņā pret smagajiem noziegumiem, it īpaši terorismu;

apzinoties smago noziegumu, it īpaši terorisma, novēršanas un apkarošanas nozīmīgumu, tajā pašā laikā ievērojot pamattiesības un brīvības, īpaši personīgās dzīves neaizskaramību;

iedvesmojoties no Konvencijas par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu, pārrobežu noziedzību un nelegālu migrāciju, kura tika parakstīta 2005. gada 27. maijā Prīmē, kā arī attiecīgo 2007. gada 18. jūnija Eiropas Padomes lēmumu, un

cenšoties pastiprināt un veicināt sadarbību starp Pusēm partnerības garā un tāpēc cenšoties ievērot esošās starptautiskās saistības, ieskaitot Latvijas Republikas saistības, kuras izriet no dalības Eiropas Savienībā;

ir vienojušās par sekojošo:

1. pants
Definīcijas

Šī Līguma mērķiem:

1. Krimināljustīcijas mērķis iekļauj darbības, kas definētas kā krimināljustīcijas pielietošana, kas nozīme jebkuras no turpmāk minētajām darbībām veikšanu: atklāšana, aizturēšana, turēšana apcietinājumā, pirmstiesas atbrīvošana, atbrīvošana pēc tiesas, apsūdzība, sprieduma pieņemšana, uzraudzība soda izciešanas laikā vai apsūdzēto vai noziegumus izdarījušo personu rehabilitācija. Krimināljustīcijas pielietošana arī iekļauj kriminālas identificēšanas pasākumus.
2. Ar DNS profiliem (DNS identifikācijas paraugi) ir apzīmēti burtu vai ciparu kods, kas apzīmē analizētā cilvēka DNS parauga nekodētās daļas īpatnības, t.i., specifiska ķīmiskā formula dažādiem DNS lokusiem.
3. Ar personas datiem ir apzīmēta jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu („datu subjektu").
4. Ar personas datu apstrādi ir apzīmēta jebkura darbība vai darbību kopums, kas tiek veikta ar personas datiem vai nu ar automatizētiem līdzekļiem, vai bez

tiem, piem., personas datu vākšana, reģistrēšana, organizēšana, glabāšana, pielāgošana vai grozīšana, šķirošana, atgūšana, konsultēšana, lietošana, atklāšana nosūtot, izplatīšana vai pieejamības nodrošināšana citā veidā, apkopošana vai grupēšana, bloķēšana vai svītrošana, tos izdzēšot vai iznīcinot.
5. Ar atsauces datiem ir apzīmēts DNS profils un ar to saistītā atsauce (DNS atsauces dati) vai pirkstu nospiedumu dati un ar tiem saistītā atsauce (pirkstu nospiedumu atsauces dati). Atsauces dati nedrīkst saturēt nekādus datus, kurus izmantojot var tieši identificēt datu subjektu. Par atsauces datiem, pēc kuriem nevar atrast nevienu personu (neizsekojami dati), jābūt attiecīgai norādei.
6. Šī Līguma 4. un 5. panta īstenošanas nolūkos ar terminu „smags noziegums" saprot noziedzīgu nodarījumu, par kura izdarīšanu paredzēta brīvības atņemšana, kuras maksimālā robeža nav mazāka par vienu gadu, vai smagāks sods.

a. Amerikas Savienotajās Valstīs smagie noziegumi iekļauj sevī arī jebkuru kriminālpārkāpumu, kas saskaņā ar ASV federālo likumu uzskatāms par pamatojumu personas neielaišanai Amerikas Savienotajās Valstīs vai izraidīšanai no tām.

b. Latvijas Republikā smagie noziegumi iekļauj sevī arī jebkuru kriminālpārkāpumu, kas saskaņā ar Latvijas Republikas nacionālajiem normatīvajiem aktiem uzskatāms par pamatojumu personas neielaišanai Latvijas Republikā vai izraidīšanai no tās.

Lai garantētu atbilstību nacionālajiem normatīvajiem aktiem, Puses var vienoties par konkrētiem smago noziegumu veidiem, par kuriem Puse sniegs personas datus saskaņā ar Līguma 6. un 9. pantu.

2. pants
Šī Līguma mērķis

Šī Līguma mērķis ir pastiprināt sadarbību starp Latvijas Republiku un Amerikas Savienotajām Valstīm smago noziegumu novēršanā un apkarošanā.

3. pants
Pirkstu nospiedumu dati

Lai īstenotu šo Līgumu, Puses nodrošina, ka valsts automātisko pirkstu nospiedumu identificēšanas sistēmām, kas izveidotas, lai novērstu un izmeklētu noziedzīgus nodarījumus, ir pieejami datnes atsauces dati. Atsauces dati ietver vienīgi pirkstu nospiedumu datus un atsauci.

4. pants
Automatizēta pirkstu nospiedumu datu meklēšana

1. Lai novērstu un izmeklētu smagos noziegumus, katra Puse dod iespēju otras Puses nacionālajiem kontaktpunktiem, kā tas ir noteikts 7. pantā, piekļūt atsauces datiem automatizētajā pirkstu nospiedumu identificēšanas sistēmā, kas

izveidota šim mērķim, ļaujot veikt automatizētu meklēšanu, salīdzinot pirkstu nospiedumu datus. Pilnvaras veikt meklēšanu var tikt realizētas tikai atsevišķos gadījumos un saskaņā ar tās Puses nacionālajiem normatīvajiem aktiem, kas veic meklēšanu.
2. Galīgo apstiprinājumu par pirkstu nospiedumu datu atbilstību atsauces datiem, ko sagatavojusi Puse, kas ir atbildīga par datni, veic nacionālie meklēšanas kontaktpunkti, automatizēti nosūtot atsauces datus, kas ir nepieciešami, lai noskaidrotu atbilstību.
3. Puses vienojas, ka meklēšanas pilnvaras, kas noteiktas saskaņā ar šo Līgumu, var tikt realizētas robežas drošības mērķiem situācijās, kad persona, par kuru tiek prasīti papildus dati, ir tikusi novirzīta tālākai pārbaudei. Meklēšanas pilnvaras, kas ir noteiktas saskaņā ar šo Līgumu, izmanto tikai krimināljustīcijas mērķiem.

5.pants
Alternatīvā meklēšana, izmantojot identifikācijas datus

1. Attiecībā uz 4. pantā minētajām meklēšanas pilnvarām, līdz brīdim, kad Latvijas Republikai ir pilnīga darboties spējīga un automatizēta pirkstu nospiedumu datu identificēšanas sistēma, kura ir sasaistīta ar sodāmības reģistra ierakstiem par personu un tā ir sagatavota, lai nodrošinātu Amerikas_Savienotās Valstis ar automātisko piekļuvi šādai sistēmai, tā nodrošina alternatīvos veidus, izmantojot citus identifikācijas datus, lai noteiktu, vai attiecīgā persona ir sodīta par smaga nozieguma izdarīšanu. Ja attiecīgā persona ir reģistrēta kā sodīta, jebkuri pieejamie dati par attiecīgo personu tiek sniegti saskaņā ar pieprasījumu saņemušās Puses nacionālajiem normatīvajiem aktiem, ieskaitot tiesiskās palīdzības noteikumus.
2. Šādi alternatīvie veidi tiek īstenoti saskaņā ar Līguma 4. panta 3. punktu.
3.Tehniskās un procesuālās detaļas par alternatīvu veidu izmantošanu nosaka vienā vai vairākos īstenošanas līgumos vai vienošanās.

6. pants
Personas papildus datu un citu datu nosūtīšana

Ja 4.pantā minētās procedūras izpildes rezultātā ir atklāta atbilstība starp pirkstu nospiedumu datiem, jebkuru pieejamo personas papildus datu un citu datu, kas attiecas uz atsauces datiem nosūtīšanu, nosaka pieprasījumu saņēmušās Puses nacionālie normatīvie akti, ieskaitot tiesiskās palīdzības noteikumus.

7. pants
Nacionālie kontaktpunkti un īstenošanas līgumi

1. Lai nosūtītu datus, kā tas ir noteikts 4. un 5. pantā, katra Puse nosaka vienu vai vairākus nacionālos kontaktpunktus. Kontaktpunktu pilnvaras nosaka piemērojamie nacionālie normatīvie akti.

2. Tehniskās un procesuālās detaļas meklēšanas veikšanai saskaņā ar 4. un 5. pantu nosaka vienā vai vairākos īstenošanas līgumos vai vienošanās.

8. pants
Automatizēta DNS profilu meklēšana

1. Ja to pieļauj abu Pušu nacionālie normatīvie akti un uz savstarpējās sadarbības principa pamata, Puses var atļaut viena otras nacionālajam kontaktpunktam, kā tas ir noteikts 10. pantā, piekļūt atsauces datiem to DNS analīzes datnēs ar pilnvarām veikt automatizētas meklēšanas, salīdzinot DNS profilus, smago noziegumu izmeklēšanai. Meklēšanas var realizēt tikai atsevišķos gadījumos un saskaņā ar tās Puses nacionālajiem normatīvajiem aktiem, kas veic meklēšanu.
2. Ja automatizētās meklēšanas rezultāti liecina, ka nosūtītais DNS profils atbilst DNS profilam, kas ir ievadīts otras Puses datnē, nacionālais kontaktpunkts, kas veic meklēšanu, saņem automātisku paziņojumu par atsauces datiem, attiecībā uz kuriem ir atklāta atbilstība. Ja atbilstība nav atklāta, par to nosūta automātisku paziņojumu.

9. pants
Personas papildus datu un citu datu nosūtīšana

Ja 8. pantā aprakstītās procedūras veikšanas laikā ir atrasta atbilstība starp DNS profiliem, jebkuru citu pieejamo papildus personas datu un citu datu, kas attiecas uz atsauces datiem, nosūtīšanu nosaka nacionālie normatīvie akti, ieskaitot pieprasījumu saņēmušās Puses tiesiskās palīdzības noteikumus.

10. pants
Nacionālais kontaktpunkts un īstenošanas līgumi

1. Lai varētu veikt datu nosūtīšanu, kā tas ir noteikts 8. pantā, katra Puse nosaka nacionālo kontaktpunktu. Kontaktpunkta pilnvaras nosaka piemērojamie nacionālie normatīvie akti.
2. Tehniskās un procesuālās detaļas meklēšanas veikšanai saskaņā ar 8. pantu nosaka turpmākajā vienā vai vairākos īstenošanas līgumos vai vienošanās.

11. pants
Personas datu un citu datu nosūtīšana, lai novērstu smagus noziegumus un teroristiskus nodarījumus

1. Lai novērstu smagus noziegumus un teroristiskus nodarījumus, Puse saskaņā ar tās attiecīgajiem nacionālajiem normatīvajiem aktiem, atsevišķos gadījumos pat bez pieprasījuma saņemšanas, saskaņā ar 6. pantu var nosūtīt attiecīgajam otras Puses nacionālajam kontaktpunktam personas datus, kas ir minēti 2. punktā, ciktāl tas ir nepieciešams, ja īpaši apstākļi dod iemeslu uzskatīt, ka datu

subjekts (-i):

a. izdarīs vai ir izdarījis teroristiskus vai ar terorismu saistītus noziegumus vai noziegumus, kas ir saistīti ar teroristu grupu vai organizāciju, atbilstoši tam, kā šie noziegumi ir definēti pieprasījumu nosūtošās Puses nacionālajos normatīvajos aktos; vai
b. piedalās vai ir piedalījies mācībās a) apakšpunktā norādīto noziegumu izdarīšanai; vai
c. izdarīs vai ir izdarījis smago noziegumu vai piedalās organizētajā noziedzīgajā grupā vai apvienībā.

2. Nosūtāmie personas dati ietver, ja ir pieejams, uzvārdu, vārdus, iepriekšējos vārdus, citus vārdus, pieņemtos vārdus, vārdu alternatīvo rakstību, dzimumu, dzimšanas datumu un vietu, pašreizējo un iepriekšējo tautību, pases numuru, citu personu apliecinošo dokumentu numurus un pirkstu nospiedumu datus, kā arī jebkuras sodāmības vai tādu apstākļu aprakstu, kas liecina par 1. punktā norādīto.

3. Nosūtošā Puse atbilstoši nacionālajiem normatīvajiem aktiem var noteikt nosacījumus par šādu datu lietošanu saņemošajā Pusē. Ja saņemošā Puse akceptē šos datus, tai ir jāievēro šie nosacījumi.

4. Nosūtošā Puse nevar izmantot vispārīgos ierobežojumus kā nosacījumu datu nosūtīšanai saskaņā ar 3. punktu, attiecībā uz saņemošās Puses personas datu apstrādes tiesiskajiem standartiem.

5. Papildus personas datiem, kas ir norādīti 2. punktā, Puses var sniegt viena otrai ar personu nesaistītus datus, kas ir saistīti ar 1. punktā minētajiem noziegumiem.

6. Katra Puse nosaka vienu vai vairākus nacionālos kontaktpunktus personas un citu datu apmaiņai šī panta ietvaros ar otras Puses kontaktpunktiem. Nacionālo kontaktpunktu pilnvaras ir noteiktas piemērojamajos nacionālajos normatīvajos aktos.

12. pants
Privātums un datu aizsardzība

1. Puses atzīst, ka rīcība ar tiem personas datiem, ko tās iegūst viena no otras, un šo datu apstrāde ir būtiski svarīga, lai saglabātu konfidencialitāti īstenojot šo Līgumu.

2. Puses uzņemas saistības apstrādāt personas datus godīgi un saskaņā ar to nacionālajiem normatīvajiem aktiem un:

a. nodrošina, ka nosūtītie personas dati ir atbilstoši un saistīti ar specifisko nosūtīšanas mērķi;
b. saglabā personas datus tik ilgi, cik tas ir nepieciešams specifiskajam mērķim, kādam šie dati ir nosūtīti vai apstrādāti saskaņā ar šo Līgumu; un
c. nodrošina, ka informācija par personas datu iespējamo neprecizitāti tiek laikus paziņota saņemošajai Pusei, lai tiktu veiktas atbilstošas korektīvās darbības.

3. Šis Līgums nepiešķir privātajām personām nekādas tiesības, ieskaitot iegūt,

noklusēt vai padarīt par neesošu kādu pierādījumu vai kavēt personas datu sniegšanu. Tiesības, kas tiek nodrošinātas neatkarīgi no šī Līguma, netiek ietekmētas.

13. pants

Papildus aizsardzība speciālo kategoriju personas datu nosūtīšanai

1. Personas datus, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģiju vai citas ticības, dalību arodbiedrībā vai attiecas uz veselību un seksuālo dzīvi, var sniegt tikai tajā gadījumā, ja tie ir īpaši svarīgi šī Līguma mērķu īstenošanai.
2. Puses, apzinoties īpašo iepriekš minēto personas datu kategoriju sensitīvo dabu, nodrošina šo datu atbilstošu aizsardzību īpaši piemērotu drošības līdzekļu veidā.

14. pants

Apstrādes ierobežojumi personas un citu datu aizsardzības nodrošināšanai

1. Neietekmējot 11. panta 3. punktā norādīto, Puses var apstrādāt datus, kas iegūti saskaņā ar šo Līgumu:
a. savas kriminālizmeklēšanas mērķim;
b. lai novērstu nopietnus draudus sabiedriskajai drošībai;
c. savā civilajā tiesvedībā vai administratīvi procesuālajās darbībās, kas ir tieši saistītas ar izmeklēšanu, kas ir norādīta a) apakšpunktā; vai
d. jebkuriem citiem mērķiem tikai ar iepriekšēju datus nosūtījušās Puses piekrišanu.
2. Puses nedrīkst šī Līguma darbības ietvaros saņemtos datus nodot nevienai trešajai valstij, starptautiskajai institūcijai vai privātajam subjektam bez datus nosūtījušās Puses piekrišanas un bez atbilstošu drošības līdzekļu izmantošanas.
3. Puse var veikt automatizētu meklēšanu otras Puses pirkstu nospiedumu un DNS datnēs saskaņā ar 4. un 8. pantu un apstrādāt datus, kas iegūti šīs meklēšanas rezultātā, ieskaitot saziņu par to, vai atbilstība ir vai tās nav vienīgi, lai:
a. konstatētu, vai salīdzinātie DNS profili vai pirkstu nospiedumu dati sakrīt;
b. sagatavotu un iesniegtu papildus palīdzības pieprasījumu saskaņā ar nacionālajiem normatīvajiem aktiem, ieskaitot tiesiskās palīdzības noteikumus, ja šie dati sakrīt; vai
c. vadītu lietvedību, kā tas ir noteikts vai atļauts nacionālajos normatīvajos aktos.

Puse, kas veic datnes administrēšanu, var automatizētās meklēšanas veikšanas gaitā apstrādāt datus, ko tai ir nosūtījusi meklējošā Puse saskaņā ar 4. un 8. pantu vienīgi tajā gadījumā, ja tas ir nepieciešams salīdzināšanai, nodrošinot automātiskas atbildes uz meklēšanu vai lietvedībai saskaņā ar 16. pantu. Salīdzināšanai nosūtītie dati pēc salīdzināšanas vai automātiskas atbildes uz meklēšanu ir nekavējoties jāiznīcina, ja vien nav nepieciešama turpmāka apstrāde mērķiem, kas minēti šī panta 3. punkta b) vai c) apakšpunktā.

15. pants
Datu korekcija, bloķēšana un dzēšana

1. Pēc nosūtošās Puses pieprasījuma saņemošā Puse atbilstoši nacionālajiem normatīvajiem aktiem labo, bloķē vai dzēš saskaņā ar šo Līgumu saņemtos datus, kas ir nepareizi vai nepilnīgi vai arī, ja to vākšana vai turpmākā apstrāde ir pretrunā ar šo Līgumu vai attiecīgi piemērojamajām nosūtošās Puses prasībām.
2. Ja Puse pārliecinās, ka dati, ko tā ir saņēmusi no otras Puses saskaņā ar šo Līgumu, nav precīzi, tai ir jāveic atbilstoši pasākumi, lai aizsargātu no kļūdainas paļaušanās uz šiem datiem, un šiem pasākumiem ir jāietver it īpaši šo datu papildināšana, dzēšana vai labošana.
3. Katra Puse nosūta paziņojumu otrai Pusei, ja tā pārliecinās, ka materiālie dati, ko tā ir nosūtījusi otrai Pusei vai ir saņēmusi no otras Puses saskaņā ar šo Līgumu, ir neprecīzi vai nedroši vai ir iemesls par tiem nopietni šaubīties.

16. pants
Dokumentācija

1. Katra Puse uztur dokumentāciju par datiem, kas ir nosūtīti otrai Pusei saskaņā ar šo Līgumu un saņemti no tās. Šie pieraksti kalpo šādiem mērķiem:
a. nodrošina efektīvu datu aizsardzības monitoringu atbilstoši attiecīgās Puses nacionālajiem normatīvajiem aktiem;
b. dod iespēju Pusēm efektīvi īstenot tiesības, kas tām tiek piešķirtas atbilstoši šī Līguma 15. un 19. pantam; un
c. nodrošina datu aizsardzību.
2. Pieraksti ietver:
a. informāciju par nosūtītajiem datiem;
b. datu nosūtīšanas datumu; un
c. datu saņēmēju gadījumā, ja dati tiek nosūtīti citām organizācijām.
3. Reģistrētajiem datiem ir jābūt aizsargātiem ar piemērotiem aizsardzības līdzekļiem pret neatbilstošu izmantošanu un citiem nepareizas lietošanas veidiem un tie ir jāglabā divus gadus. Pēc glabāšanas perioda beigām reģistrētie dati ir nekavējoties jāiznīcina, ja vien tas nav pretrunā ar nacionālajiem normatīvajiem aktiem, ieskaitot piemērojamos datu aizsardzības un glabāšanas noteikumus.

17. pants
Datu drošība

1. Puses nodrošina, ka tiek izmantoti visi nepieciešamie tehniskie līdzekļi un veikti organizatoriskie pasākumi, lai aizsargātu personas datus no nejaušas vai nelikumīgas iznīcināšanas, nejaušas pazaudēšanas vai neatļautas izpaušanas,

izmainīšanas, piekļūšanas vai jebkāda veida neatļautas apstrādes. Puses it īpaši veic pasākumus, lai nodrošinātu, ka pieeja personas datiem ir iespējama tikai personām, kurām ir piešķirta pilnvara piekļūšanai šiem datiem.
2. Īstenošanas līgumi vai vienošanās, kas nosaka automatizētās pirkstu nospiedumu un DNS datņu meklēšanas procedūras saskaņā ar 4. un 8. pantu, nodrošina:
a. ka tiek izmantota atbilstoša mūsdienīga tehnoloģija, lai nodrošinātu datu aizsardzību, drošību, konfidencialitāti un integritāti;
b. ka tiek izmantotas šifrēšanas un pilnvarošanas procedūras, ko atzīst atbildīgās institūcijas, kad tiek lūgta palīdzība vispārējās pieejamības tīklos; un
c. mehānismu, kas garantē, ka tiek veiktas tikai atļautas meklēšanas.

18. pants
Pārskatāmība – informācijas sniegšana datu subjektiem

1. Nekas šajā Līgumā netiek interpretēts tā, lai traucētu Pušu tiesiskās saistības, kā tas ir noteikts to attiecīgajos normatīvajos aktos, lai nodrošinātu datu subjektam informāciju attiecībā uz apstrādi un datu pārraugu, saņēmējiem vai saņēmēju kategorijām, piekļuves tiesību esamību un tiesībām labot datus, kas uz viņu attiecas, un jebkuru papildus informāciju, tādu kā likumīgo pamatojumu apstrādes operācijām, kam dati ir paredzēti, datu glabāšanas laika ierobežojumiem un palīdzības pieprasījuma iesniegšanas tiesībām tiktāl, ciktāl šāda papildu informācija ir nepieciešama mērķiem un īpašajiem apstākļiem, kuros šie dati tiek apstrādāti, lai garantētu godīgu datu apstrādi attiecībā uz datu subjektiem.
2. Šādas informācijas sniegšanu var atteikt saskaņā ar attiecīgajiem Pušu normatīvajiem aktiem, ieskaitot gadījumu, ja šī informācijas sniegšana var apdraudēt:
a. datu apstrādes mērķus;
b. izmeklēšanu vai kriminālvajāšanu, ko veic Latvijas Republikas kompetentās institūcijas vai Amerikas Savienotu Valstu kompetentās institūcijas; vai
c. trešo pušu tiesības un brīvības.

19. pants
Informācija

Pēc pieprasījuma, saņemošajai Pusei ir jāinformē nosūtošā Puse par nosūtīto datu apstrādi un iegūto rezultātu. Saņemošajai Pusei jānodrošina, ka tās atbilde tiek laikus paziņota nosūtošajai Pusei.

20. pants
Saistība ar citiem līgumiem

Nekas šajā Līgumā nav iztulkojams kā ierobežojums vai kaitējums jebkuru līgumu, citu vienošanos noteikumiem, tiesībsargājošo iestāžu sadarbībai vai nacionālo normatīvo aktu noteikumiem, kas dod iespēju apmainīties ar informāciju starp Latvijas Republiku un Amerikas Savienotajām Valstīm.

21. pants
Konsultācijas

1. Puses regulāri konsultējas par šī Līguma nosacījumu īstenošanas gaitu.
2. Ja par šī Līguma interpretāciju vai piemērošanu rodas domstarpības, Puses konsultē viena ar otru, lai atvieglotu to atrisināšanu.

22. pants
Izmaksas

Katra Puse sedz izdevumus, kas ir radušies tās institūcijām Līguma īstenošanas gaitā. Īpašos gadījumos Puses var vienoties par atšķirīgu kārtību.

23. pants
Līguma izbeigšana

Katra Puse var izbeigt šo Līgumu, rakstiski paziņojot par to otrai Pusei trīs mēnešus iepriekš. Līguma noteikumus turpina piemērot attiecībā uz datiem, kas tika nosūtīti pirms šādas izbeigšanas.

24. pants
Grozījumi

1. Pēc jebkuras Puses pieprasījuma Puses uzsāk konsultācijas par šī Līguma grozīšanu.
2. Šajā Līgumā jebkurā laikā var izdarīt grozījumus, Pusēm par to rakstiski vienojoties.

25. pants
Stāšanās spēkā

Šis Līgums, izņemot 8. - 10. pantu, stājas spēkā pēdējās notas datumā, kas noslēdz diplomātisko notu apmaiņas procesu starp Pusēm, norādot, ka katra no tām ir veikušas jebkurus pasākumus, kas ir nepieciešami, lai Līgums stātos spēkā. Šī Līguma 8. - 10. pants stājas spēkā pēc īstenošanas līguma (-u) vai vienošanās noslēgšanas, saskaņā ar 10. pantu, un pēdējās notas datumā, kas

noslēdz diplomātisko notu apmaiņas procesu starp Pusēm, norādot, ka katra no Pusēm ir spējīga uz savstarpējās sadarbības principa pamata īstenot šajos pantos norādīto. Tas notiek, ja abu Pušu nacionālie normatīvie akti atļauj DNS caurlūkošanas veidu, kas ir minēts 8. - 10. pantā.

Sagatavots Riga 29th Septembris, 2008 (vieta), . (laiks), divos eksemplāros latviešu un angļu valodā, abiem tekstiem esot vienlīdz autentiskiem.

Amerikas Savienoto Valstu valdības vārdā	Latvijas Republikas valdības vārdā