

No. 44226

**Latvia
and
Georgia**

Agreement between the Government of the Republic of Latvia and the Government of Georgia on mutual protection of classified information (with annexes). Riga, 6 July 2005

Entry into force: *16 January 2006 by notification, in accordance with article 14*

Authentic texts: *English, Georgian and Latvian*

Registration with the Secretariat of the United Nations: *Latvia, 15 August 2007*

**Lettonie
et
Géorgie**

Accord entre le Gouvernement de la République de Lettonie et le Gouvernement de la Géorgie relatif à la protection mutuelle des informations classifiées (avec annexes). Riga, 6 juillet 2005

Entrée en vigueur : *16 janvier 2006 par notification, conformément à l'article 14*

Textes authentiques : *anglais, géorgien et letton*

Enregistrement auprès du Secrétariat des Nations Unies : *Lettonie, 15 août 2007*

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF LATVIA AND THE GOVERNMENT OF GEORGIA ON MUTUAL PRO- TECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Latvia and the Government of Georgia, hereinafter referred to as “Parties”, have – in order to safeguard the classified information exchanged directly or through other administrative entities or private legal entities that deal with classified information under jurisdiction of either Party – agreed upon the following:

Article 1. Applicability

(1) The purpose of this Agreement is to establish the legal framework of cooperation between the Parties, regarding the protection of classified information.

(2) This Agreement shall form an integral part of any contract or agreement involving exchange of classified information, that will be made or signed in the future between the Parties concerning the following subjects:

- a) Cooperation between governmental entities of the two Parties,
- b) Cooperation, exchange of information, joint ventures, contracts and any relations between governmental entities and/or private legal entities of the Parties,
- c) Sale of equipment and know-how by one Party to the other.

(3) This Agreement may not be invoked by either Party to obtain classified information that the other Party has received from a third party.

(4) Annexes A and B to this Agreement are integral parts of the Agreement.

Article 2. Definitions

The key terms used in this Agreement are defined in Annex A.

Article 3. Mutual Security Protection

(1) In accordance with their national laws, regulations and practice, both Parties shall take appropriate measures to protect classified information, which is transmitted, received, produced or developed as a result of any agreement or relation between the Parties. The Parties will afford to all of the transmitted, received, produced or developed classified information the same degree of security protection as is provided to their own classified information of equivalent level of classification, as defined in Article 6.

(2) Access to classified information and to locations and facilities where classified activities are performed or where classified information is stored, will be limited to those who have been cleared for access to RESTRICTED information or granted a security

clearance for access to information classified CONFIDENTIAL and above, and who, due to their functions or employment, have a “need to know”.

(3) Each Party shall supervise the observance of security laws, regulations and practice at the agencies, offices and facilities within their jurisdiction that possess, develop, produce and/or use classified information of the other Party, by means of, inter alia, review visits.

(4) Classified information shall be destroyed in such a manner that any reconstruction of classified information in whole or in part is effectively prevented.

Article 4. Disclosure of Information

(1) The Parties shall not disclose classified information under this Agreement to third parties without prior written consent of the originating Party. Received classified information from one Party to the other Party shall be used for the specified purpose only.

(2) In the event that either Party and/or its agencies or entities concerned with the subjects set out in Article 1, award a contract for performance within the territory of the other Party, and such contract involves classified information possessed by the contractor of the Party performing the work, then the Party of the country in which the performance under the Agreement is taking place, will assume responsibility for administering the other Party’s classified information in accordance with its own standards and requirements.

(3) Prior to release to either Party’s contractors or prospective contractors of any classified information received from the other Party, the receiving Party shall:

a) Ensure that such contractors or prospective contractors and their facilities have the capability to protect the classified information adequately,

b) Grant an appropriate facility security clearance to the relevant contractors,

c) Grant administrative access or an appropriate personnel security clearance for all personnel whose duties require access to the classified information,

d) Ensure that all persons having access to classified information, are informed of their responsibilities to protect the classified information in accordance with applicable laws,

e) Carry out periodic security inspections of relevant cleared facilities.

Article 5. Competent Security Authorities

(1) The receiving Party shall appoint and make known to the other Party a duly authorised security authority, hereafter called the Competent Security Authority, which shall supervise the implementation of any agreement, as defined in Article 1 of this Agreement, concerning all aspects of security.

(2) Each Party undertakes to ensure that its respective Competent Security Authority will duly observe the provisions of this Agreement.

(3) The Competent Security Authorities responsible for the implementation and supervision of all aspects of this Agreement are:

In Latvia:

Constitution Protection Bureau
Miera 85a, Riga, LV 1013
Latvia

In Georgia:
Ministry of Inner Affairs
Didi Kheivani str. 10
0114
Tbilisi, Georgia

(4) Each Competent Security Authority shall, upon request, furnish the other Competent Security Authority information concerning its security organisation and procedures and practices for safeguarding classified information, to make it possible to compare and maintain the same security standards and facilitate joint visits in both countries by certified officials. Both Parties must agree upon such visits.

Article 6. Security Classifications

(1) The security classifications of the Parties and their equivalents of are:

The Republic of Latvia	English language equivalent	Georgian
SEVIŠĶI SLEPENI	TOP SECRET	gansakutrebuli mnishvnelobis
SLEPENI	SECRET	Sruliad saidumlo
KONFIDENCIĀLI	CONFIDENTIAL	saidumlo
DIENESTA VAJADZĪBĀM	RESTRICTED	saidumlo

(2) The receiving Party and/or its entities shall neither use a lower security classification level for received classified information, nor declassify that information without the prior written consent of the originating Party. The originating Party shall inform the receiving Party of any changes in security classification of the exchanged information.

Article 7. Marking of Classified Information

(1) The receiving Party shall additionally mark the received classified information with its own equivalent security classification.

(2) Copies and translations of the received classified information shall be marked and placed under the same protection as the originals.

(3) Translations shall bear a note in the language into which they are translated stating that the translations contain classified information of the originating Party.

Article 8. Transmission of Classified Information

(1) Classified information shall normally be physically transmitted between the Parties through their respective diplomatic channels.

(2) Exchange of classified information can also take place through representatives officially appointed by the authorities in both countries. Such authorisation may be given to representatives of industrial undertakings engaged in specific projects.

(3) Delivery of large items or quantities of classified information shall be arranged on a case-by-case basis.

(4) Other approved means of transmission or exchange may be used if agreed upon by both Competent Security Authorities.

Article 9. Visits

(1) Visits aimed at exchanging classified information to premises where classified information is developed, handled or stored, or where classified projects are carried out, will only be granted by one Party to visitors from the country of the other Party if a prior written permission from the Competent Security Authority of the receiving Party has been obtained. Such permission will only be granted to persons who have been appropriately security cleared and have a “need to know”.

(2) The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the receiving Party of expected visitors at least three weeks prior to the planned visit, in accordance with the procedures defined in Annex B to this Agreement.

(3) Each Party shall guarantee the protection of personal data of the visitors according to the respective national laws and regulations.

Article 10. Industrial Security

(1) The Competent Security Authority of one Party, wishing to place a classified contract with a contractor in the country of the other Party, or wishing to authorise one of its own contractors to place a classified contract in the country of the other Party within a classified project, shall obtain a prior written assurance from the Competent Security Authority of the other Party that the proposed contractor holds a facility security clearance of the appropriate level and has the facilities to handle and store classified information of the same level.

(2) Every classified contract between entities of the Parties and/or private organisations (such as industries, research centres, assistance and/or service facilities etc.) shall contain an appropriate security section and a security classification list, based on the terms of this Agreement.

(3) The Competent Security Authority, in whose country the work is to be performed, shall assume responsibility for prescribing and administering security measures for the contract under the same standards and requirements that govern the protection of its own classified contracts.

(4) Sub-contractors interested in classified sub-contracts, shall be submitted in advance by the contractor to the Competent Security Authority for approval. If approved, the sub-contractor must fulfil the same security obligations as have been set for the contractor.

(5) Notification of any classified project, agreement, contract or sub-contract shall be forwarded in advance to the Competent Security Authority of the country where the project is to be performed.

(6) Two copies of the security section of any classified contract shall be forwarded to the Competent Security Authority in whose country the work is to be performed.

Article 11. Breach of Security

In case of a breach of security concerning classified information originated or received from the other Party, or if common interests are involved, the Competent Security Authority in whose country the security compromise has occurred shall inform the Competent Security Authority of the other Party as soon as possible and carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation. The other Party shall be informed in writing of the results of the investigation, the reasons and extent of the security compromise and the measures undertaken for their cessation.

Article 12. Expenses

Each Party shall cover its own expenses incurred in connection with the implementation of this Agreement.

Article 13. Dispute Settlement

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation between the Parties, without recourse to outside jurisdiction.

Article 14. Final Provisions

(1) This Agreement shall enter into force on the date of the receipt of the last written notification about accomplishments by the Parties of internal procedures necessary for its entry into force. It may be terminated at any time by either Party in the way of a written notification. In such case the Agreement expires six months from the date of the notification of the termination.

(2) Each Party shall promptly notify the other Party of any amendments of its national laws and regulations that would affect the protection of classified information under this Agreement.

(3) The review, changes and amendments of the Agreement may be done at any time on the basis of mutual written consent of both Parties.

(4) In the event of termination, classified information transmitted under the terms of this Agreement shall be returned to the other Party as soon as possible. Classified infor-

mation that is not returned to the other Party shall be protected in accordance with the provisions laid down in this Agreement.

Signed in Riga on July 6, 2005, in two original copies, for each of the following languages: Latvian, Georgian and English, all texts being equally authentic. In case of differences in interpretation, the English text shall prevail.

On behalf of the Government of the Republic of Latvia:

EDGARS RINKĒVIČS
State Secretary of the Ministry of Defence

On behalf of the Government of Georgia:

VASIL SIKHARULIDZE
Deputy Defence Minister

ANNEX A TO THE AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF LATVIA AND THE GOVERNMENT OF GEORGIA ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Definitions

For the purpose of this Agreement, the following terms are defined:

1. “Classified information” means –

- a. Any classified item, be it an oral communication of classified contents or the electrical or electronic transmission of a classified message, or a “material” as defined in (b) below,
- b. “Material” includes “document” as defined in (c) below, and any item of machinery, equipment, weapon or weapon-systems either manufactured or in the process of manufacture,
- c. “Document” means any form of recorded information regardless of type of recording media,

which in the interest of national security of the Party and in accordance with its applicable laws and regulations, requires protection against unauthorised disclosure and which has been classified in accordance with national legislation.

2. “Classified contract” means an agreement between two or more contractors, creating and defining enforceable rights and obligations between them, which contains or involves classified information.

3. “Contractor” means an individual or a legal entity possessing the legal capability to undertake classified contracts.

4. “Need to know” means the principle according to which a positive determination is made that a prospective recipient has a requirement for access to Classified Information in order to perform official tasks or services.

5. “Security clearance” means a positive determination following an investigative procedure to ascertain the capability of a person or entity to have access to and to handle classified information on a certain level in accordance with the respective national security regulations.

6. “Breach of security” means an act or an omission contrary to national security regulations, the result of which may endanger or compromise classified information.

ANNEX B TO THE AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF LATVIA AND THE GOVERNMENT OF GEORGIA ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Visits by personnel of one Party to the facilities, establishments etc. of the other Party

Access to classified information and to establishments and facilities etc. where classified activities are performed or where classified information is stored or handled, shall be allowed by one Party to visitors of the other Party only if they have been:

- (a) Checked by the Competent Security Authority or other competent government authority of the sending country and are authorised to receive classified information in accordance with the national regulations of the host country, and/or
- (b) Authorised by the Competent Security Authority or other competent government authority of the respective country to perform the required visit.

A visit request shall include the following information:

- (a) Visitor's name and surname, date and place of birth, nationality and passport or other identity document of the visitor,
- (b) Official (employment) status of the visitor, including the name of the establishment, company or organisation, which the visitor represents,
- (c) Certification of the visitor being administratively cleared or possessing a security clearance,
- (d) Object (name and address of the establishment/facility to be visited) and purpose of the visit,
- (e) Point of contact at the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit,
- (f) Expected dates and duration of the visit.

The visit request shall be submitted:

- (a) Through the Competent Security Authority for visit requests of the citizens of Georgia to the Republic of Latvia,
- (b) Through to the Competent Security Authority for visit requests of the citizens of the Republic of Latvia to Georgia,
- (c) Other procedures may be used if agreed upon by both Competent Security Authorities.

The validity of visit authorisations shall not exceed 12 months.

All visitors will comply with the national security regulations on protection of classified information of the host Party.

[GEORGIAN TEXT – TEXTE GÉORGIEN]

შეთანხმება ლატვიის რესპუბლიკის მთავრობასა და საქართველოს მთავრობას შორის საიდუმლო ინფორმაციის ერთობლივი დაცვის შესახებ

ლატვიის რესპუბლიკის მთავრობა და საქართველოს მთავრობა, შემდგომში “მხარეება წოდებულნი, იმ საიდუმლო ინფორმაციის დაცვის მიზნით, რომელიც გაიცელება პირდაპირ სხვა ადმინისტრაციული ორგანოების ან კერძო სამართლის იურიდიული პირების საშუალებით, რომლებიც თვითიური მხარის იურისდიქციის ფარგლებში მუშაობენ საიდუმლო ინფორმაციაზე, შეთანხმდნენ შემდეგზე:

**მუხლი 1
გამოყენების სფერო**

- (1) წინამდებარე შეთანხმების მიზანია მხარეებს შორის საიდუმლო ინფორმაციის დაცვას დაკავშირებული თანამშრომლობის სამართლებრივი სისტემის ჩამოყალიბება.
- (2) წინამდებარე შეთანხმება იქნება განუყოფელი ნაწილი შემდგომში დადებული ნებისმიერ ხელშეკრულებისა თუ შეთანხმების, რომელიც ჩამოყალიბდება ან ხელმოწერილ იქნება მომავალში მხარეებს შორის შემდგომ საკითხებზე:
 - a. ორი მხარის სამთავრობო უწყებათა შორის თანამშრომლობა,
 - b. თანამშრომლობა, ინფორმაციის გაცვლა, ერთობლივი პროექტები, კონტრაქტები ნებისმიერი ურთიერთობა სამთავრობო უწყებებს შორის და/ან მხარეთა კერძო სამართალ იურიდიულ პირებს შორის.
 - c. ერთი მხარის მიერ მეორე მხარისათვის აღჭურვილობის და “ნოუ-ჰაუ“-ს მიყიდვა.
- (3) წინამდებარე შეთანხმება არ შეიძლება გამოყენებულ იქნას რომელიმე მხარის მიერ მესამე მხარისაგან მიწოდებული საიდუმლო ინფორმაციის მისაღებად.
- (4) წინამდებარე შეთანხმების “ა“ და “ხ“ დანართები აღნიშნული შეთანხმების განუყოფელი ნაწილია.

**მუხლი 2
განსაზღვრებები**

ბირითადი ცნებები განსაზღვრულია შეთანხმების დანართში - “ა“.

**მუხლი 3
საიდუმლო ინფორმაციის ერთობლივი დაცვა**

- (1) შიდა კანონმდებლობის, დადგენილებების და არსებული პრაქტიკის შესაბამისად, ორი მხარე იღებს შესაბამის ზომებს იმ საიდუმლო ინფორმაციის დასაცავად, რომელსაც გააღაცემულია, მიღებულია ან წარმოქმნილია მხარეთა შორის ნებისმიერი შეთანხმების შედეგად. მხარეები გაავრცელებენ გადაცემულ, მიღებულ ან წარმოქმნილ ინფორმაციაზე დაცვის იმ დონეს, რაც ვრცელდება შესაბამისი ხარისხის მქონე მათ საკუთარ საიდუმლო ინფორმაციაზე, როგორც ეს განსაზღვრულია მე-6 მუხლში.
- (2) დაშვება საიდუმლო ინფორმაციაზე და იმ ადგილებსა თუ შენობებში სადაც საიდუმლო ინფორმაციასთან დაკავშირებული მოქმედებები მიმდინარეობს ან სადაც საიდუმლო ინფორმაცია ინახება, შესაძლებელი იქნება მხოლოდ მათთვის ვისაც დაშვება აქვთ “ინფორმაცია შეზღუდული სარეგლობისათვის“ ან მიღებული აქვთ დაშვება საიდუმლო (კონფიდენციალურ confidential) ინფორმაციაზე და უფრო მაღალ კატეგორიაზე, და ვისაც, ფუნქციებიდან საქმიანობიდან გამომდინარე აქვთ “ცოდნის აუცილებლობის“ საჭიროება.

(3) თითოეული მხარე კონტროლს გაუწევს საიდუმლო ინფორმაციის შესახებ არსებულ კანონების, დადგენილებებისა და არსებული პრაქტიკის შესრულებას მათი იურისდიქციის ქვეშ მყოფ ორგანიზაციებში, ოფისებსა და ნაგებობებში, რომლებიც ფლობენ, ავითარებენ, ქმნიან და/ან იყენებენ მეორე მხარის საიდუმლო ინფორმაციას სამუშაო ვიზიტების საშუალებით.

(4) საიდუმლო ინფორმაცია უნდა განადგურდეს ისე, რომ მისი მთლიანად ან ნაწილობრივ აღდგენა თავიდან იქნას აცილებული.

მუხლი 4
ინფორმაციის გამჟღავნება

(1) წინამდებარე შეთანხმების შესაბამისად, მხარეებმა არ უნდა გაუმჟღავნონ საიდუმლო ინფორმაცია მესამე მხარეს ამგვარი ინფორმაციის პირველწყაროს წინასწარი წერილობითი თანხმობის გარეშე. ერთი მხარის მიერ მეორისგან მიღებული საიდუმლო ინფორმაცია გამოყენებულ უნდა იქნას მხოლოდ განსაზღვრული მიზნისათვის.

(2) იმ შემთხვევაში როდესაც რომელიმე მხარე და/ან მისი ორგანიზაციები ან უწყებები, რომელთაც ესებათ 1 მუხლში აღნიშნული საკითხები, გააფორმებენ კონტრაქტს მეორე მხარის ტერიტორიაზე მოქმედებისათვის და ამგვარი კონტრაქტი შეიცავს საიდუმლო ინფორმაციას, რომელსაც ფლობს სამუშაოს განმახორციელებელი კონტრაქტორი მხარე, შემდეგ მხარე რომელშიდაც მიმდინარეობს მოქმედებანი წინამდებარე შეთანხმების შესაბამისად, აიღებს მეორე მხარის საიდუმლო ინფორმაციის აღმინსტრირების პასუხისმგებლობას მისი სტანდარტებისა და მოთხოვნების მიხედვით.

(3) რომელიმე მხარის კონტრაქტორებისათვის ან პოტენციური კონტრაქტორებისათვის ნებისმიერი საიდუმლო ინფორმაციის გამჟღავნებამდე რომელიც მიღებულია მეორე მხარის მიერ, მიმღებმა მხარემ უნდა:

- a) უზრუნველყოს, რომ ასეთ კონტრაქტორებს ან პოტენციურ კონტრაქტორებს და მათ მოწყობილობებს შეუძლიათ ადექვატურად დაიცვან საიდუმლო ინფორმაცია.
- b) მიანიჭოს შესაბამისი დაშვების შესაძლებლობა შესაბამის კონტრაქტორებს.
- c) მიანიჭოს აღმინსტრაციული დაშვება ან პერსონალის დაშვების უფლება იმ პერსონალს, რომელთა სამსახურებრივი მოვალეობები მოითხოვს საიდუმლო ინფორმაციაზე დაშვებას.
- d) უზრუნველყოს, რომ ის პერსონალი რომლებსაც აქვთ დაშვება საიდუმლო ინფორმაციაზე, ინფორმირებულნი არიან მათი ვალდებულებების შესახებ რათა დაიცვან საიდუმლო ინფორმაცია შესაბამისი კანონების გათვალისწინებით.
- e) პერიოდულად იმ ნაგებობების ინსპექტირების განხორციელება, რომლებშიდაც ინახება საიდუმლო ინფორმაცია.

მუხლი 5
უშიშროების კომპეტენტური ორგანოები

(1) მიმღებმა მხარემ უნდა განსაზღვროს და შეატყობინოს მეორე მხარეს შესაბამისი წესით უფლებამოსილი, შემდგომში კომპეტენტურ უშიშროების ორგანოდ წოდებული - უწყების შესახებ, რომელიც ზედამხედველობას გაუწევს უსაფრთხოების საკითხებთან დაკავშირებული ნებისმიერი შეთანხმების იმპლემენტაციას, როგორც ეს განსაზღვრულია შეთანხმების I მუხლში.

2. თითოეული მხარე კისრულობს ვალდებულებას, რომ მათი კომპეტენტური უშიშროების ორგანოები სათანადო დონეზე დაიცავენ აღნიშნული შეთანხმების დებულებებს.

3. კომპეტენტური უშიშროების ორგანოები პასუხისმგებლები არიან აღნიშნული შეთანხმების ყველა საკითხზე მეთვალყურეობასა და იმპლემენტაციაზე.

ლატვიაში:
კონსტიტუციის დაცვის ბიურო
მიერა 85ა, რიგა, ლვ 1013
ლატვია

საქართველოში:
შინაგან საქმეთა სამინისტრო
ლიდი ხეივანის ქუჩა 10,
0114
თბილისი, საქართველო

4. თითოეული კომპეტენტური უშიშროების ორგანო ვალდებულია მეორე მხარის კომპეტენტურ უშიშროების ორგანოს მოთხოვნისთანავე წარუდგინოს ინფორმაცია მისი საიდუმლო ინფორმაციის დაცვასთან დაკავშირებული საკითხების ორგანიზებაზე და პროცედურებზე (საიდუმლო ინფორმაციის დაცვის არსებულ პრაქტიკაზე, რათა შესაძლებელი გახდეს საიდუმლო ინფორმაციის დაცვის სტანდარტების შედარება და მსგავსი სტანდარტებზე შენარჩუნება და ოფიციალურ პირთა ერთობლივი ვიზიტების ხელშეწყობა ორივე ქვეყანაში ორივე მხარე უნდა შეთანხმდეს ამგვარ ვიზიტებზე.

მუხლი 6
საიდუმლო ინფორმაციის კატეგორიები

1. მხარეთა საიდუმლო ინფორმაციის ხარისხები და მათი ექვივალენტებია

ლატვიის რესპუბლიკა	ექვივალენტური ტერმინები ინგლისურ ენაზე	საქართველო
Seviski slepeni	TOP SECRET სრულიად საიდუმლო	განსაკუთრებული მნიშვნელობის
Slepeni	SECRET საიდუმლო	სრულიად საიდუმლო
Konfidenciali	CONFIDENTIAL კონფიდენციალური	საიდუმლო
Dienesta Vajadzibam	RESTRICTED შეზღუდული სარგებლობისათვის	საიდუმლო

2. მიმღები მხარე და/ან მისი ხელისუფლების ორგანოები არ შეუფარდებენ საიდუმლოებად დაბალ ხარისხს მიღებულ საიდუმლო ინფორმაციას, და არ მოახდენენ ამ ინფორმაციის დეკლასიფიკაციას წინასწარი წერილობითი თანხმობის გარეშე. ინფორმაციის მიმწოდებელ მხარე შეატყობინებს მიმღებ მხარეს ნებისმიერი ცვლილების შესახებ გაცვლილი ინფორმაციის კლასიფიკაციასთან დაკავშირებით.

მუხლი 7
საიდუმლო ინფორმაციის მარკირება

- (1) მიმღები მხარე დამატებით მარკირებას უკეთებს მიღებულ საიდუმლო ინფორმაციას მ ქვეყანაში არსებული საიდუმლოების ექვივალენტური ხარისხით.
- (2) უნდა მოხდეს მიღებული საიდუმლო ინფორმაციის ასლებისა და თარგმანების მარკირება და დაცვა ორიგინალების მსგავსად.
- (3) თარგმანს უნდა ჰქონდეს აღნიშვნა იმ ენაზე რა ენაზედაც ის იქნა თარგმნილი, იმ შესახებ რომ თარგმანი შეიცავს მომწოდებელი მხარის საიდუმლო ინფორმაციას.

მუხლი 8
საიდუმლო ინფორმაციის მიწოდება

- (1) ჩვეულებრივ საიდუმლო ინფორმაციის გაცვლა მხარეებს შორის უნდა მოხდეს მათი დიპლომატიური გზების მეშვეობით.
- (2) საიდუმლო ინფორმაციის გაცვლა შეიძლება აგრეთვე შედგეს ორივე ქვეყნის ხელისუფლების მიერ ოფიციალურად დანიშნულ წარმომადგენლებს შორის. ამგვარ უფლებამოსილება შეიძლება მიენიჭოს საწარმოს წარმომადგენლებს, რომლებიც მონაწილეობენ ოდებენ კონკრეტულ პროექტებში.

- (3) დიდი მოცულობით საიღუმლო ინფორმაციის მიწოდება ყოველ კონკრეტულ შემთხვევასთან დაკავშირებით ინდივიდუალურად უნდა განხორციელდეს.
- (4) მიწოდების ან გაცვლის სხვა მიღებული მეთოდები შეიძლება გამოყენებულ იქნას ორ მხარის უშიშროების კომპეტენტურ ორგანოებს შორის შეთანხმების არსებობის შემთხვევაში

**მუხლი 9
ვიზიტები**

- (1) ვიზიტები რომლებიც მიმართულია საიღუმლო ინფორმაციის გაცვლისაკენ იქნება საიღუმლო ინფორმაცია იქმნება, მუშავდება ან ინახება, ან სადაც საიღუმლო პროექტ ხორციელდება, ერთი მხარის მიერ მეორე ქვეყნის ვიზიტორებისათვის შესაძლებელი იქნება შემთხვევაში თუ მოპოვებულია მასპინძელი სახელმწიფოს კომპეტენტური უშიშრო ორგანოს წინასწარი წერილობითი ნებართვა. ამგვარი ნებართვა მიენიჭება მხოლოდ იმ პირ რომლებსაც აქვთ საიღუმლო ინფორმაციაზე დაშვება ან „ცოდნის აუცილებლობის“ საჭირო.
- (2) გამგზავნი მხარის უშიშროების კომპეტენტურმა ორგანომ უნდა აცნობონ მიმ მხარის უშიშროების კომპეტენტურ ორგანოებს ვიზიტორთა შესაძლო კანდიდატურ, შესახებ, დაგეგმილ ვიზიტამდე სამი კვირით ადრე მაინც, იმ პროცედურ გათვალისწინებით რომლებიც განხილულია დანართში - (b).
- (3) თითოეულმა მხარემ უნდა უზრუნველყოს ვიზიტში მონაწილე პირების პერსონალ ინფორმაციის დაცვა სახელმწიფოს შიდა კანონმდებლობის მიხედვით.

**მუხლი 10
სამეწარმეო უსაფრთხოება**

- (1) ერთი მხარის უშიშროების კომპეტენტურმა ორგანომ, რომელსაც სურვილი გააფორმოს საიღუმლო კონტრაქტი მეორე მხარის ქვეყანაში კონტრაქტორთან, ან ს მიაჩნლოს უფლებამოსილება ერთ-ერთს საკუთარი კონტრაქტორებიდან, რათა საიდუმლო პროექტის ფარგლებში გააფორმოს საიღუმლო კონტრაქტი მეორე მხარის ქვეყანაში, წინას უნდა მოიპოვოს მეორე მხარის უშიშროების კომპეტენტური ორგანოსაგან წერილობ გარანტია, რომ წარმოდგენილ კონტრაქტორს აქვს შესაბამისი დონის დაშვება და აგრ ფლობს აპარატურასა თუ შენობას იგივე ხარისხის საიღუმლო ინფორმაციაზე სამუშაო მის შესაძლებლობას.
- (2) ყოველი საიღუმლო კონტრაქტი მხარეების წარმომადგენელ ორგანოებსა და/ან კე ორგანიზაციებს შორის (როგორებიცაა სამრეწველო, კვლევითი ცენტრები, დამხმარე დ მომსახურე დაწესებულებები და ა.შ.) უნდა შეიცავდეს შესაბამის საიღუმლო განყოფილებას საიღუმლოებათა კატეგორიების ნუსხას, რომლებიც ეფუძნება აღნიშნული შეთანხმ დებულებებს.
- (3) უშიშროების კომპეტენტურმა ორგანომ, იმ ქვეყანაში სადაც სამუშაო განხორციელდ უნდა აიღოს პასუხისმგებლობა კონტრაქტის დაცვის ზომების განსაზღვრისა ადმინისტრირების თაობაზე, იმავე სტანდარტებისა და მოთხოვნების შესაბამისად, რომლები რეგულირდება საიღუმლო კონტრაქტების დაცვა.
- (4) ქვე-კონტრაქტორებმა, რომლებიც დაინტერესებულნი არიან საიღუმლო კონტრაქტებით, წინასწარ უნდა წარუდგინონ ქვე-კონტრაქტები უშიშროების კომპეტენტ ორგანოებს დასამტკიცებლად. ქვე-კონტრაქტის დამტკიცების შემთხვევაში ქვე-კონტრაქტ უნდა შეასრულოს საიღუმლოებასთან დაკავშირებული უსაფრთხოების ვალდებულებები ი როგორც ეს გათვალისწინებულია კონტრაქტორისათვის.
- (5) შეტყობინება ნებისმიერ საიღუმლო პროექტზე, შეთანხმებაზე, კონტრაქტზე ან კონტრაქტზე წინასწარ უნდა გადაეცეს იმ ქვეყნის უშიშროების კომპეტენტურ ორგან სადაც პროექტი უნდა განხორციელდეს.
- (6) ორი ასლი ნებისმიერი საიღუმლო კონტრაქტის საიღუმლო ნაწილის უნდა გადაეცე ქვეყნის უშიშროების კომპეტენტურ ორგანოს, სადაც სამუშაო განხორციელდება.

**მუხლი 11
დაცვის წესების დარღვევა**

იმ საიღუმლო ინფორმაციასთან დაკავშირებული დაცვის წესების დარღვე შემთხვევაში, რომლის პირველწყარო ან მომწოდებელია მეორე მხარე, ან თუ ის მოი საერთო ინტერესებს, იმ ქვეყნის უშიშროების კომპეტენტურმა ორგანომ, სადაც საიღუმლო ინფორმაციას საფრთხე შეექმნა უნდა შეატყობინოს მეორე მხარის უშიშროების კომპეტენტ

ორგანოს დაუყოვნებლივ და დაიწყოს შესაბამისი გამოძიების პროცესი. აუცილებლად შემთხვევაში მეორე მხარემ უნდა ითანამშრომლოს გამოძიებასთან. მეორე მხარეს წერილად უნდა მიეწოდოს გამოძიების შედეგები, მიზეზები და ინფორმაცია იმის შესახებ თუ რამდენად იყო საფრთხე და თუ რა ღონისძიებები იქნა გამოყენებული მათი შეჩერებისათვის.

**მუხლი 12
ხარჯები**

თითოეულმა მხარემ უნდა დაფაროს შეთანხმების განხორციელებასთან დაკავშირებული საკუთარი ხარჯები.

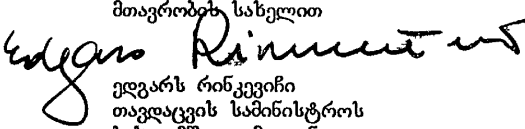
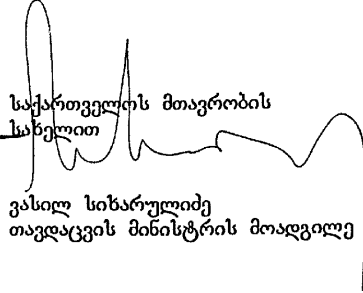
**მუხლი 13
დავების დარეგულირება**

აღნიშნული შეთანხმების ინტერპრეტაციასთან ან გამოყენებასთან დაკავშირებული ნებისმიერი დავა მოგვარდება მხარეთა შორის კონსულტაციების გზით მესამე მხარის ჩაურევლად.

**მუხლი 14
დასკვნითი დებულებები**

- (1) წინამდებარე შეთანხმება ძალაში შედის უკანასკნელი წერილობითი შეტყობის დღიდან, რომლითაც მხარეები ერთმანეთს აუწყებენ შეთანხმების ძალაში შესვლის აუცილებელი შიდა პროცედურების დასრულების შესახებ. შეთანხმების მოქმედება შეიძლება შეწყდეს ნებისმიერი მხარის მიერ მეორე მხარისათვის წერილობითი შეტყობინების გზით. შემთხვევაში შეთანხმება მოქმედებას წყვეტს მისი შეწყვეტის შესახებ შეტყობინების მიღების თვის გასვლის შემდგომ.
- (2) თითოეულმა მხარემ იმავდროულად უნდა შეატყობინოს მეორე მხარეს, მის კანონმდებლობაში ისეთი ცვლილებების შესახებ, რომლებიც გავლენას იქონიებენ წინამდებარე შეთანხმების ფარგლებში საიდუმლო ინფორმაციის დაცვაზე.
- (3) შეთანხმების განხილვა, ცვლილებებისა და შესწორებების შეტანა შეიძლება განხორციელდეს ნებისმიერ დროს ორმხრივი წერილობითი შეთანხმების საფუძველზე.
- (4) შეწყვეტის შემთხვევაში, საიდუმლო ინფორმაცია რომელიც გადაცემულია აღნიშნული შეთანხმების დებულებების შესაბამისად, დაუბრუნდება მეორე მხარეს დაუყოვნებლივ საიდუმლო ინფორმაცია რომელიც არ დაუბრუნდა მეორე მხარეს დაცულ იქნება შეთანხმების დებულებების შესაბამისად.

ხელმოწერილია .წ. . . , ივლისი ორ ეგზემპლარად, თითოეული ლატვიურ, ქართულ, ინგლისურ ენაზე, ამასთან ყველა ტექსტი თანაბრად აუთენტიურია. გაუგებრობის შემთხვევაში უპირატესობა მიენიჭება ტექსტს ინგლისურ ენაზე.

<p>ლატვიის რესპუბლიკის მთავრობის სახელით</p>  <p>ედგარს რინკევიჩი თავდაცვის სამინისტროს სახელმწიფო მდივანი</p>	<p>საქართველოს მთავრობის სახელით</p>  <p>ვასილ სიმარულიძე თავდაცვის მინისტრის მოადგილე</p>
---	--

დანართი ა.

შეთანხმებაზე ლატვიის რესპუბლიკის მთავრობასა და საქართველოს მთავრობას შორის საიდუმლო ინფორმაციის ერთობლივად დაცვის შესახებ

განსაზღვრებები

შეთანხმების მიზნებისათვის განსაზღვრულია შემდეგი ცნებები:

1. “საიდუმლო ინფორმაცია” ნიშნავს –

- a) ნებისმიერ საიდუმლო ინფორმაციას, გადაცემულს სიტყვიერი კომუნიკაციის გზით, თუ ელექტრონული საშუალებით გადაცემულ საიდუმლო შეტყობინებას თუ “მასალას” როგორც ეს განსაზღვრულია “გ” პუნქტში,
- b) “მასალა” შეიცავს “დოკუმენტს”, როგორც ეს განსაზღვრულია “გ” პუნქტში და ნებისმიერ განვითარებულ ან განვითარების პროცესში მყოფ ყველა მექანიზმ ალკუორვილობას, იარაღს ან შეიარაღების სისტემას;
- c) “დოკუმენტი” ნიშნავს ნებისმიერ სახის ჩაწერილ ინფორმაციას ჩაწერის საშუალებების მიუხედავად.

რომელიც ხელშეკრულების მხარის სახელმწიფო უშიშროების ინტერესებიდან გამომდინარე და შესაბამისი კანონებისა და დადგენილებების გათვალისწინებით, მოითხოვს დაცვას, რათა ნებართვის გარეშე არ იქნას გამოამჟღავნებული და რომელიც დასაიდუმლოებულ იქნა სახელმწიფო კანონმდებლობის შესაბამისად.

2. “საიდუმლო კონტრაქტი” ნიშნავს შეთანხმებას ორ ან მეტ კონტრაქტორს შორის რომელიც ქმნის და განსაზღვრავს მათ შორის საიდუმლო ინფორმაციის შემცველ შესაძლო უფლებებსა და ვალდებულებებს.

3. “კონტრაქტორი” ნიშნავს ფიზიკურ ან იურიდიულ პირს, რომელიც ფლობს იურიდიულ უფლებამოსილებას, რათა პასუხისმგებლობა დააკისროს საიდუმლო ხელშეკრულებებთან დაკავშირებით.

4. “ცოდნის აუცილებლობა” (“need to know”) ნიშნავს პრინციპს, რომლის თანახმად დადებითად განისაზღვრება მიმღების მოთხოვნა საიდუმლო ინფორმაციასთან დაშვებაზე როდესაც მას ამგვარი ინფორმაცია ესაჭიროება სამსახურებრივი მოვალეობები განხორციელებისათვის.

5. “საიდუმლო ინფორმაციაზე დაშვება” ნიშნავს შემოწმების პროცესის დადებითად დასრულებას, იმის დასადაგენად უნდა მიენიჭოს თუ არა პიროვნებას ან უწყებას საიდუმლო ინფორმაციაზე დაშვების უფლება გარკვეულ დონეზე ეროვნული უსაფრთხოების წესები შესაბამისად.

6. “საიდუმლო ინფორმაციის დაცვის წესების დარღვევა” ნიშნავს ეროვნული უსაფრთხოების წესების საწინააღმდეგო მოქმედებას ან უმოქმედობას, რომლის შედეგადაც შეიძლება საფრთხე შეუქმნას ან რისკის ქვეშ დააყენოს საიდუმლო ინფორმაცია.

დანართი b.

შეთანხმებაზე ლატვიის რესპუბლიკის მთავრობასა და საქართველოს მთავრობას შორის საიდუმლო ინფორმაციის ერთობლივად დაცვის შესახებ

ერთი მხარის წარმომადგენელთა ვიზიტები მეორე მხარის შენობა-ნაგებობებსა და დაწესებულებებში

საიდუმლო ინფორმაციასთან, დაწესებულებებსა და შენობა-ნაგებობებში, სადაც ხორციელდება საიდუმლო მოქმედებები ან სადაც ინახება ამგვარი ინფორმაცია, ერთი მხარის წარმომადგენლები დაიშვებიან იმ შემთხვევაში თუ ისინი არიან:

(a) შემოწმებული გამგზავნი ქვეყნის კომპეტენტური უშიშროების ორგანოების ან სხვა კომპეტენტური სამთავრობო უწყებათა მიერ და აქვთ მინიჭებული უფლება მიიღონ საიდუმლო ინფორმაცია მიმღები ქვეყნის ეროვნული კანონმდებლობის ფარგლებში, და/ან

(b) უფლებამოსილი არიან შესაბამისი ქვეყნის კომპეტენტური უშიშროების ორგანოების ან სხვა კომპეტენტური სამთავრობო ორგანოებისაგან, განახორციელონ საჭირო ვიზიტი.

ვიზიტის მოთხოვნები უნდა შეიცავდეს შემდეგ ინფორმაციას:

a) ვიზიტორის სახელი და გვარი, დაბადების ადგილი და თარიღი, ეროვნება და პირადობის დამადასტურებელი მოწმობა ან პასპორტი;

b) ვიზიტორის ოფიციალური (სამსახურეობრივი) სტატუსი, ორგანიზაციის ან კომპანიის სახელის ჩათვლით, რომელსაც ვიზიტორი წარმოადგენს;

c) დამადასტურებელი სერტიფიკატი იმისა, რომ ვიზიტორს ადმინისტრაციული დაშვება აქვს ან ფლობს საიდუმლო ინფორმაციაზე დაშვების უფლებას.

d) ვიზიტის ადგილი (დაწესებულების სახელი და მისამართი) და მიზანი;

e) საკონტაქტო პირი იმ დაწესებულებაში, რომელსაც უნდა ეწვიონ, ადრე არსებული კონტაქტები და სხვა ნებისმიერი საჭირო ინფორმაცია იმის გადასაწყვეტად თუ რამდენად მიზანშეწონილია ვიზიტი.

f) ვიზიტის მოსალოდნელი თარიღი და ხანგრძლივობა;

ვიზიტის მოთხოვნები წარდენილ უნდა იქნეს:

a) ლატვიის რესპუბლიკაში საქართველოს მოქალაქეთა ვიზიტის მოთხოვნებისათვის უშიშროების კომპეტენტურ ორგანოებში

b) საქართველოში ლატვიის რესპუბლიკის მოქალაქეთა ვიზიტის მოთხოვნებისათვის უშიშროების კომპეტენტურ ორგანოებში

c) შესაძლოა გამოყენებულ იქნას სხვა პროცედურები ორივე კომპეტენტურ უშიშროების უწყებას შორის შეთანხმების შემთხვევაში;

ვიზიტის მიზანშეწონილობაზე უფლებამოსილების ხანგრძლივობა არ უნდა აღემატებოდეს 12 თვეს.

ყველა ვიზიტორმა უნდა იმოქმედოს მასპინძელ ქვეყანაში საიდუმლო ინფორმაციის დაცვის სფეროში არსებული ეროვნული კანონმდებლობის შესაბამისად.

[LATVIAN TEXT – TEXTE LETTON]

LATVIJAS REPUBLIKAS VALDĪBAS

UN

GRUZIJAS VALDĪBAS

LĪGUMS

PAR

**SAVSTARPĒJU KLASIFICĒTĀS INFORMĀCIJAS
AIZSARDZĪBU**

Latvijas Republikas valdība un Gruzijas valdība, turpmāk sauktas par Pusēm, lai aizsargātu klasificēto informāciju, ar kuru Puses apmainījušās tieši vai caur citām administratīvām institūcijām vai privātām juridiskām personām, kuru darbs saistīts ar klasificēto informāciju attiecīgās Puses jurisdikcijā, ir vienojušās par sekojošo:

1. pants **Piemērošana**

(1) Šī Līguma mērķis ir definēt abu Pušu sadarbības juridisko pamatojumu klasificētās informācijas aizsardzības jomā.

(2) Šis Līgums ir neatņemama sastāvdaļa jebkuram turpmāk starp Pusēm sastādītam vai parakstītam līgumam, kas paredz klasificētās informācijas apmaiņu sekojošu jautājumu ietvaros:

a) Abu Pušu valdību institūciju sadarbība,

b) Pušu valdību institūciju un/vai privāto juridisko personu sadarbība, informācijas apmaiņa, kopējas komercsabiedrības, līgumi vai citas attiecības,

c) Vienas Puses iekārtu un nepatentēto praktisko zināšanu pārdošana otrai Pusei.

(3) Neviena Puse nevar atsaukties uz šo Līgumu, lai iegūtu klasificēto informāciju, kuru otra Puse ir saņēmusi no trešās puses.

(4) Šī Līguma Pielikumi A un B ir Līguma neatņemamas sastāvdaļas.

2. pants **Definīcijas**

Galvenie šai Līgumā lietotie termini ir definēti Pielikumā A.

3. pants **Savstarpēja drošības aizsardzība**

(1) Saskaņā ar nacionālajiem normatīvajiem aktiem un praksi abas Puses veic atbilstošus pasākumus, lai aizsargātu klasificēto informāciju, kas tiek nodota,

saņemta, radīta vai izstrādāta jebkāda starp Pusēm noslēgta līguma vai pastāvošo attiecību rezultātā. Puses nodrošina visai nodotai, saņemtai, radītai vai izstrādātai klasificētai informācijai tādu pašu aizsardzības pakāpi, kādu tā nodrošina savai informācijai ar līdzvērtīgu klasifikācijas pakāpi, kā noteikts 6. pantā.

(2) Pieeja klasificētai informācijai un vietām un objektiem, kur tiek veiktas darbības ar klasificēto informāciju vai kur tā tiek glabāta, tiek dota tikai tām personām, kuras ir atbildīgas par informācijas dienesta vajadzībām neizpaušanu vai kurām ir izsniegta speciālā atļauja darbam ar konfidenciālu un augstākas klasifikācijas pakāpes informāciju un kurām saistībā ar darba pienākumiem ir “nepieciešamība zināt”.

(3) Katra Puse pārrauga ar drošību saistīto nacionālo normatīvo aktu un prakses ievērošanu tās jurisdikcijā esošās institūcijās, birojos un objektos, kuru rīcībā ir, vai kas izstrādā, rada un/vai izmanto otras Puses klasificēto informāciju, veicot, cita starpā, pārbaudes apmeklējumus.

(4) Klasificētā informācija tiek iznīcināta tā, lai novērstu tās pilnīgu vai daļēju atjaunošanu.

4. pants **Informācijas atklāšana**

(1) Puses neatklāj saskaņā ar šo Līgumu saņemto klasificēto informāciju trešajām pusēm bez iepriekšējas rakstiskas nosūtītājas Puses piekrišanas. Klasificētā informācija, ko viena Puse saņēmusi no otras Puses, tiek izmantota tikai norādītajam mērķim.

(2) Ja kāda no Pusēm un/vai tās institūcijas vai organizācijas, kas ir saistītas ar 1. punktā minētajiem jautājumiem, slēdz līgumu par darbu izpildi otras Puses teritorijā, un šāds līgums ir saistīts ar klasificēto informāciju, kas pieder tās Puses līgumslēdzējam, kas veic darbu, tad tās valsts Puse, kurā tiek veikta darbu izpilde, uzņemas atbildību par šīs klasificētās informācijas pārraudzību saskaņā ar savas valsts standartiem un prasībām.

(3) Pirms jebkuras no vienas Puses saņemtas klasificētās informācijas nodošanas otras Puses līgumslēdzējiem vai iespējamiem līgumslēdzējiem, saņēmēja Puse:

a) Nodrošina, lai līgumslēdzēji vai iespējamie līgumslēdzēji un to objekti spēj atbilstoši aizsargāt klasificēto informāciju,

- b) Izsniedz atbilstošu industriālās drošības sertifikātu attiecīgajiem līgumslēdzējiem,
- c) Sniedz pieeju vai speciālo atļauju personām, kuru pienākumu izpildei nepieciešama pieeja klasificētai informācijai,
- d) Nodrošina, lai visas personas, kurām ir pieeja klasificētai informācijai, ir informētas par saviem pienākumiem aizsargāt klasificēto informāciju saskaņā ar spēkā esošiem normatīviem aktiem,
- e) Veic periodiskas drošības noteikumu ievērošanas pārbaudes attiecīgajos sertificētajos objektos.

5. pants

Atbildīgās drošības iestādes

(1) Saņēmeja Puse nozīmē un informē otru Pusi par pilnvarotu drošības iestādi, turpmāk sauktu par Atbildīgo drošības iestādi, kas pārbauda jebkura šī Līguma 1. pantā minētā līguma izpildi visu drošības aspektu ietvaros.

(2) Katra Puse apņemas nodrošināt, lai tās Atbildīgā drošības iestāde ievēro šī Līguma noteikumus.

(3) Atbildīgās drošības iestādes par visu šī Līguma aspektu izpildi un pārraudzību ir:

Latvijā:

Satversmes aizsardzības birojs

Miera 85a, Rīga, LV-1013,

LATVIJA

Gruzijā:

Iekšlietu ministrija

Didi Kheivani iela 10

0114

Tbilisi, Gruzija

(4) Vienas Puses Atbildīgā drošības iestāde pēc pieprasījuma iesniedz otras Puses Atbildīgajai drošības iestādei informāciju par drošības pasākumu organizāciju un procedūrām, un praksi, lai salīdzinātu un ievērotu tādus pašus drošības noteikumus, un veicina pilnvarotu amatpersonu kopīgas vizītes abās valstīs. Abām Pusēm ir jāsaņemas šādas vizītes.

6. pants
Klasifikācijas pakāpes

(1) Pušu klasifikācijas pakāpes un to ekvivalenti ir sekojoši:

Latvijas Republika	Angļu valodas ekvivalents	Gruzija
SEVIŠĶI SLEPENI	TOP SECRET	GANSAKUTREBULI MNISHVNELOBIS
SLEPENI	SECRET	SRULIAD SAIDUMLO
KONFIDENCIĀLI	CONFIDENTIAL	SAIDUMLO
DIENESTA VAJADZĪBĀM	RESTRICTED	SAIDUMLO

(2) Saņēmēja Puse un/vai tās institūcijas nedrīkst pazemināt saņemtās klasificētās informācijas klasifikācijas pakāpi vai deklasificēt šo informāciju bez iepriekšējas rakstiskas nosūtītājas Puses piekrišanas. Nosūtītāja Puse informē saņēmēju Pusi par jebkurām izmaiņām nodotās informācijas klasifikācijas pakāpē.

7. pants
Klasificētās informācijas apzīmējumi

(1) Saņēmēja Puse papildus piešķir saņemtajai klasificētai informācijai savu atbilstošo klasifikācijas pakāpi.

(2) saņemtās klasificētās informācijas kopijām un tulkojumiem tiek piešķirta tāda pati klasifikācijas un aizsardzības pakāpe kā oriģinālam.

(3) Uz tulkojumiem saņēmējas Puses nacionālajā valodā tiek norādīts, ka tie satur nosūtītājas Puses klasificēto informāciju.

8. pants
Klasificētās informācijas pārsūtīšana

(1) Klasificētā informācija starp Pusēm tiek nosūtīta caur to attiecīgajiem diplomātiskajiem kanāliem.

(2) Klasificētās informācijas apmaiņa var notikt, izmantojot pārstāvjus, kurus oficiāli pilnvarojušas abu valstu kompetentas institūcijas. Šāda atļauja, ja

nepieciešams, var tikt piešķirta attiecīgajos projektos iesaistītajiem uzņēmumu pārstāvjiem.

(3) Klasificētās informācijas lielu objektu vai lielu daudzumu nosūtīšana tiek saskaņota katrā gadījumā atsevišķi.

(4) Citi apstiprināti informācijas nosūtīšanas vai apmaiņas līdzekļi var tikt izmantoti, ja par to vienojas Pušu Atbildīgās drošības iestādes.

9. pants

Vizītes

(1) Vizītes, kuru mērķis ir klasificētās informācijas apmaiņa telpās, kurās klasificētā informācija tiek izstrādāta, apstrādāta vai glabāta, vai kurās tiek īstenoti projekti, kas saistīti ar klasificēto informāciju, viena Puse atļauj veikt apmeklētājiem no otras Puses valsts tikai tad, ja iepriekš ir saņemta rakstiska atļauja no uzņēmējas Puses Atbildīgās drošības iestādes. Šāda atļauja tiek piešķirta tikai personām, kuras ir saņēmušas speciālo atļauju un kurām ir “nepieciešamība zināt”.

(2) Nosūtītājas Puses Atbildīgā drošības iestāde paziņo saņēmējas Puses Atbildīgajai drošības iestādei par gaidāmajiem apmeklētājiem vismaz trīs nedēļas pirms plānotās vizītes, ievērojot šī Līguma Pielikumā B noteikto kārtību.

(3) Katra Puse nodrošina apmeklētāju personas datu aizsardzību saskaņā ar nacionāliem normatīviem aktiem.

10. pants

Industriālā drošība

(1) Vienas Puses Atbildīgā drošības iestāde, kas vēlas slēgt klasificētu līgumu ar otras Puses līgumslēdzēju vai kas vēlas atļaut kādam no savas valsts līgumslēdzējiem pildīt klasificētu līgumu otras Puses valstī klasificēta projekta ietvaros, saņem no otras Puses Atbildīgās drošības iestādes iepriekšēju rakstisku apstiprinājumu, ka attiecīgais līgumslēdzējs ir saņēmis atbilstošas kategorijas industriālās drošības sertifikātu un spēj nodrošināt tādas pašas pakāpes klasificētās informācijas apstrādi un glabāšanu.

(2) Katram klasificētam līgumam, kas noslēgts starp Pušu institūcijām un/vai privātām organizācijām (tādām kā rūpniecības uzņēmumi, pētījumu centri, palīdzības un/vai servisa centri u.c.) ir jāsaturs atbilstoša drošības sadaļa un klasifikācijas pakāpju saraksts, kas pamatojas uz šī Līguma noteikumiem.

(3) Atbildīgā drošības iestāde, kuras valstī ir paredzēts veikt darbu, uzņemas atbildību par drošības pasākumu noteikšanu un pārraudzīšanu attiecīgā līguma ietvaros saskaņā ar standartiem un prasībām, kas attiecas uz šīs valsts klasificēto līgumu aizsardzību.

(4) Informāciju par līgumslēdzēju, kas ir ieinteresēts pildīt klasificēto apakšlīgumu, līgumslēdzējs iepriekš iesniedz apstiprināšanai Atbildīgajai drošības iestādei. Ja līgumslēdzējs, kas pildīs apakšlīgumu, tiek apstiprināts, tam jāievēro tādi paši drošības noteikumi, kā līgumslēdzējam, ar kuru tiek slēgts klasificētais līgums.

(5) Paziņojums par jebkuru klasificētu projektu, vienošanos, līgumu vai apakšlīgumu ir iepriekš iesniedzams tās valsts Atbildīgajai drošības iestādei, kurā ir paredzēts izpildīt projektu.

(6) Jebkura klasificētā līguma drošības sadaļas divas kopijas tiek iesniegtas tās valsts Atbildīgajai drošības iestādei, kurā paredzēts veikt darbu.

11. pants

Drošības prasību pārkāpums

Drošības prasību pārkāpuma gadījumā saistībā ar klasificēto informāciju, kas radīta vai saņemta no otras Puses, vai arī gadījumā, ja ir iesaistītas kopējās intereses, tās Puses Atbildīgā drošības iestāde, kurā nesankcionētā izpaušana notikusi, nekavējoties informē otras Puses Atbildīgo drošības iestādi un veic nepieciešamo izmeklēšanu. Ja nepieciešams, šī otra Puse piedalās izmeklēšanā. Otra Puse tiek informēta par izmeklēšanas rezultātiem, un tai tiek nosūtīts nobeiguma ziņojums par drošības prasību pārkāpuma rezultātiem, iemesliem un apmēru, kā arī veiktajiem pasākumiem to novēršanā.

12. pants

Izdevumi

Katra Puse sedz savus izdevumus, kas radušies saistībā ar šī Līguma piemērošanu.

13. pants

Strīdu izšķiršana

Jebkurš strīds par šī Līguma interpretāciju vai piemērošanu tiek atrisināts konsultāciju ceļā starp Pusēm un netiek nodots risināšanai nevienai ārējai jurisdikcijai.

14. pants
Nobeiguma noteikumi

(1) Šis Līgums stājas spēkā datumā, kad tiek saņemts pēdējais rakstiskais abu Pušu paziņojums par visu procedūru ieviešanu, lai Līgums stātos spēkā. Jebkura Puse to var izbeigt jebkurā laikā, par to paziņojot rakstiski. Tādā gadījumā Līgums zaudē spēku pēc sešiem mēnešiem, skaitot no datuma, kurā otra Puse ir saņēmusi paziņojumu par izbeigšanu.

(2) Katra Puse nekavējoties informē otru Pusi par jebkurām izmaiņām tās nacionālajos normatīvajos aktos, kas ietekmē klasificētās informācijas aizsardzību šī Līguma ietvaros.

(3) Šī Līguma pārskatīšana, izmaiņas un grozījumi var tikt veikti jebkurā laikā, ja tam rakstiski piekrīt abas Puses.

(4) Līguma izbeigšanas gadījumā klasificētie objekti un/vai informācija, kas nodoti saskaņā ar šī Līguma noteikumiem, pēc iespējas ātrāk tiek nodoti atpakaļ otrai Pusei. Klasificētā informācija un/vai objekti, kas netiek nodoti atpakaļ, tiek aizsargāti saskaņā ar šī Līguma noteikumiem.

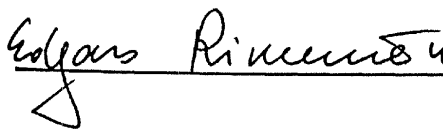
Līgums noslēgts *Rīgā*..... (kur) *2005.g. 6. jūlijā* (kad) divos oriģinālos eksemplāros latviešu, gruzīnu un angļu valodās, un visi teksti ir vienlīdz autentiski. Dažādu Līguma noteikumu interpretāciju gadījumā noteicošais ir teksts angļu valodā.

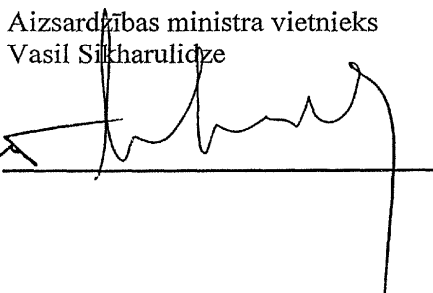
Latvijas Republikas valdības
vārdā

Gruzijas valdības
vārdā

Aizsardzības ministrijas
valsts sekretārs Edgars Rinkēvičs

Aizsardzības ministra vietnieks
Vasil Sikharulidze





Pielikums A

Latvijas Republikas valdības un Gruzijas valdības līgumam par savstarpēju klasificētās informācijas aizsardzību

Definīcijas

Šī Līguma ietvaros lieto sekojošus terminus:

1. “Klasificētā informācija”
 - a. Jebkurš klasificēts objekts, kas var būt gan mutisks paziņojums ar klasificētu saturu, gan arī elektriski vai elektroniski nosūtīts klasificēts ziņojums, vai arī “materiāls”, kā definēts punktā (b),
 - b. Termins “materiāls” nozīmē “dokumentu”, kā definēts punktā (c), kā arī jebkuru mašīnu, iekārtu, ieroču vai ieroču sistēmu vienību, kas vai ir izgatavota vai ir izgatavošanas procesā,
 - c. Termins “dokuments” nozīmē jebkuru pierakstītas informācijas formu, neatkarīgi no pieraksta veida,

kam katras Puses nacionālās drošības interesēs un saskaņā ar tās valstī spēkā esošajiem normatīvajiem aktiem, ir nepieciešama aizsardzība pret nesankcionētu piekļūšanu un kas ir klasificēta saskaņā ar nacionālajiem normatīvajiem aktiem.

2. “Klasificēts līgums”

Līgums starp diviem vai vairākiem līgumslēdzējiem, kas nodibina un definē izpildāmas pušu tiesības un pienākumus, un kas satur vai iekļauj klasificētu informāciju.

3. “Līgumslēdzējs”

Individuāla vai juridiska persona, kas ir tiesīga uzņemties klasificēto līgumu izpildi.

4. “Nepieciešamība zināt”

Princips, saskaņā ar kuru tiek konstatēts, ka pieeja klasificētai informācijai var tikt piešķirta, jo personai, kas to pieprasa, ir obligāta nepieciešamība to zināt sakarā ar viņa/viņas darba pienākumiem.

5. “Speciālā atļauja”

Pozitīvs lēmums pēc pārbaudes procedūras, kas veikta, lai pārlicinātos, vai personai vai uzņēmumam var tikt dota pieeja, un vai tā /tas drīkst strādāt ar klasificēto informāciju noteiktā pakāpē saskaņā ar nacionāliem normatīviem aktiem.

6. “Drošības prasību pārkāpums”

Darbība vai bezdarbība, kas ir pretrunā ar nacionāliem normatīviem aktiem, kā rezultātā var tikt apdraudēta vai nesankcionēti izpausta klasificētā informācija.

Pielikums B

Latvijas Republikas valdības un Gruzijas valdības līgumam par savstarpēju klasificētās informācijas aizsardzību

Vienas Puses pilnvaroto personu vizītes otras Puses institūcijās, objektos u.c.

Pieeju klasificētai informācijai un institūcijām un objektiem, kur tiek veiktas darbības ar klasificēto informāciju vai kur tā tiek glabāta vai apstrādāta, viena Puse atļauj otras Puses apmeklētājiem vienīgi tad, ja viņus:

- a. ir pārbaudījusi nosūtītājas Puses Atbildīgā drošības iestāde vai cita kompetenta iestāde un ja viņiem ir atļauts saņemt klasificēto informāciju saskaņā ar uzņēmējas valsts nacionāliem normatīviem aktiem un/vai
- b. ir pilnvarojusi attiecīgās valsts Atbildīgā drošības iestāde vai cita kompetenta iestāde veikt nepieciešamo vizīti.

Vizītes pieprasījumā jāietver:

- a. Apmeklētāja vārds un uzvārds, dzimšanas datums un vieta, tautība un informācija par apmeklētāja pasēs datiem vai citiem personību apliecinājošiem dokumentiem,
- b. Apmeklētāja nodarbinātības statuss, tai skaitā, institūcijas, uzņēmuma vai organizācijas nosaukums, kuru apmeklētājs pārstāv,
- c. Apmeklētāja speciālās atļaujas apstiprinājums,
- d. Vizītes objekts (institūcijas / objekta nosaukums un adrese) un mērķis,
- e. Kontaktpersona institūcijā/ objektā, ko paredzēts apmeklēt, iepriekšēja sadarbība un cita informācija par vizītes pamatošanu.
- ģ. Vizītes plānotais datums un ilgums.

Pieprasījums tiek iesniegts, izmantojot:

- a. Atbildīgo drošības iestādi, lai pieteiktu Gruzijas pilsoņu vizītes Latvijas Republikā.
- b. Atbildīgo drošības iestādi, lai pieteiktu Latvijas Republikas pilsoņu vizītes Gruzijā.

- c.** Var tikt izmantots cits pieprasījuma iesniegšanas veids, ja par to vienojas abu Pušu Atbildīgās drošības iestādes.

Vizītes apstiprinājuma derīguma termiņš nepārsniedz 12 mēnešus.

Visiem apmeklētājiem jāievēro uzņēmējas Puses nacionālie normatīvie akti klasificētās informācijas aizsardzības jomā.

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE DE LETTONIE ET LE GOUVERNEMENT DE LA GÉORGIE RELATIF À LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République de Lettonie et le Gouvernement de la Géorgie, ci-après dénommés les «Parties», souhaitant garantir la protection des informations classifiées échangées directement ou par l'entremise d'autres entités administratives ou organisations privées qui traitent des informations classifiées sous l'autorité de l'une ou l'autre Partie, sont convenus de ce qui suit :

Article premier. Applicabilité

1. Le présent Accord a pour objet d'établir le cadre juridique de la coopération entre les Parties en ce qui concerne la protection des informations classifiées.

2. Le présent Accord fait partie intégrante de tout contrat ou accord portant sur l'échange d'informations classifiées à conclure ou à signer à l'avenir entre les Parties concernant les sujets suivants :

- a) La coopération entre les entités gouvernementales des deux Parties,
- b) La coopération, l'échange de renseignements, les co-entreprises, les contrats ou toute autre relation entre des entités gouvernementales et/ou des entités juridiques privées des Parties,
- c) La vente, par l'une des Parties, de matériel et de savoir-faire à l'autre Partie.

3. Le présent Accord ne peut être invoqué par l'une des Parties pour obtenir des informations classifiées obtenues par l'autre Partie d'une tierce partie.

4. Les annexes A et B du présent Accord font partie intégrante de l'Accord.

Article 2. Définitions

Les principaux termes utilisés dans le présent Accord sont définis dans l'annexe A.

Article 3. Protection mutuelle en matière de sécurité

1. Conformément à leur législation, réglementations et pratiques nationales, les Parties appliquent toutes les mesures voulues pour la protection des informations classifiées devant être transmises, reçues, produites ou élaborées au titre de tout Accord ou relation entre les Parties. Les Parties accordent à toutes les informations classifiées transmises, reçues, produites ou élaborées le même niveau de protection que celui qui est accordé aux informations classifiées nationales jouissant du niveau correspondant de classification de sécurité, tel qu'il est défini à l'article 6.

2. Seules peuvent avoir accès aux sites et établissements où s'accomplissent des activités classifiées ou où sont conservées des informations classifiées, les personnes auxquelles a été délivrée une habilitation de sécurité leur permettant d'accéder à l'information RESTREINTE, ou une habilitation de sécurité leur permettant d'accéder à l'information CONFIDENTIELLE et qui, de par leur fonction ou emploi, ont «besoin d'en connaître».

3. Chaque Partie surveille l'application des lois, normes et procédures en matière de sécurité par les organismes, les bureaux et les installations relevant de sa juridiction qui détiennent, élaborent, produisent et/ou utilisent des informations classifiées de l'autre Partie, grâce notamment à des visites d'inspection.

4. Les informations classifiées sont détruites de façon à empêcher toute reconstitution totale ou partielle.

Article 4. Déclassification de l'information

1. Les Parties sont tenues de ne pas fournir d'informations classifiées au titre du présent Accord à une tierce partie sans le consentement écrit préalable de la Partie d'origine. Les informations classifiées envoyées par l'une des Parties à l'autre Partie ne peuvent être utilisées que dans le but spécifié.

2. Lorsqu'une des Parties et/ou l'une de ses organisations ou entités, auxquelles s'appliquent les dispositions de l'article premier, attribue un contrat pour des services sur le territoire de l'autre Partie, et que le contrat en question met en jeu des informations classifiées possédées par l'entrepreneur de la Partie qui réalise le travail, la Partie sur le territoire de laquelle les services faisant l'objet de l'Accord en question doivent être fournis est responsable de la gestion de l'information classifiée de l'autre Partie conformément à ses propres normes et prescriptions.

3. Avant que l'une des Parties ne communique à ses entrepreneurs ou futurs entrepreneurs toutes informations envoyées par l'autre Partie, la Partie destinataire doit :

a) Donner les assurances nécessaires que lesdits entrepreneurs ou futurs entrepreneurs et leurs entreprises sont capables de protéger adéquatement les informations classifiées,

b) Accorder les habilitations personnelles adéquates auxdits entrepreneurs,

c) Accorder les habilitations personnelles adéquates ou d'accès administratif à toutes les personnes qui, du fait de leur fonction, auront besoin d'accéder aux informations classifiées,

d) Veiller à ce que toutes les personnes qui ont accès aux informations classifiées soient informées de leurs responsabilités en matière de protection des informations classifiées aux termes de la législation en vigueur,

e) Réaliser des inspections de sécurité périodiques des installations pour lesquelles les habilitations de sécurité ont été accordées.

Article 5. Autorités compétentes en matière de sécurité

1. La Partie destinataire communique à l'autre Partie l'autorité dûment autorisée en matière de sécurité, ci-après dénommée l'autorité compétente en matière de sécurité, qui

est chargée de surveiller la mise en œuvre de tout accord, tel que défini à l'article premier du présent Accord, portant sur tous les aspects liés à la sécurité.

2. Chacune des Parties s'engage à veiller à ce que son autorité de sécurité compétente respecte comme il se doit les dispositions du présent Accord.

3. Les autorités de sécurité compétentes responsables de l'application et de la supervision de tous les aspects du présent Accord sont les suivantes :

En Lettonie :

Bureau de protection de la Constitution

Miera 85a, Riga, LV-1013

Lettonie

En Géorgie :

Ministère des affaires intérieures

Didi Kheivani str. 10

0114 Tbilisi, Géorgie

4. Sur demande, chacune des autorités compétentes en matière de sécurité fournit des informations à l'autre autorité compétente sur sa propre organisation et ses procédures en matière de sécurité pour protéger les informations classifiées, en vue de comparer et de maintenir le même niveau de normes de sécurité et de faciliter les visites communes dans les deux pays par le personnel habilité. Les deux Parties conviennent des dispositions concernant ces visites.

Article 6. Classifications de sécurité

1. Les classifications de sécurité des Parties et leurs équivalents sont les suivants :

République de Lettonie	Équivalent en français	Géorgien
SEVIŠĶI SLEPENI	SECRET DÉFENSE	Gansakutrebuli mnishvnelobis
SLEPENI	SECRET	Sruliad saidumlo
KONFIDENCIĀLI	CONFIDENTIEL	saidumlo
DIENESTA VAJADZĪBĀM	RESTREINT	saidumlo

2. La Partie destinataire et/ou ses entités ne peuvent ni utiliser une classification de sécurité inférieure pour les informations classifiées reçues, ni déclassifier cette information sans le consentement écrit préalable de la Partie d'origine. La Partie d'origine tient l'autorité compétente de la Partie destinataire informée de tout changement relatif à la protection des informations classifiées échangées.

Article 7. Marquage des informations classifiées

1. La Partie destinataire ajoutera une nouvelle marque à l'information classifiée reçue indiquant sa propre classification de sécurité équivalente.
2. Les reproductions et les traductions d'informations classifiées doivent porter les mêmes marquages de sécurité et faire l'objet de la même protection que les originaux.
3. Les traductions doivent inclure une note rédigée dans la langue dans laquelle elles ont été traduites indiquant que les traductions comportent des informations classifiées de la Partie d'origine.

Article 8. Transmission d'informations classifiées

1. Les informations classifiées sont normalement transmises physiquement entre les Parties par les voies diplomatiques respectives.
2. L'échange d'informations classifiées peut aussi se faire par l'intermédiaire de représentants désignés officiellement par les autorités des deux pays. Cette habilitation peut être accordée aux représentants d'entreprises industrielles participant à des projets particuliers.
3. La remise d'éléments ou de quantités importantes d'informations classifiées peut être convenue au cas par cas.
4. D'autres moyens approuvés de transmission ou d'échange peuvent être utilisés si les deux autorités compétentes en matière de sécurité en conviennent.

Article 9. Visites

1. Les visites organisées pour échanger des informations classifiées aux locaux où ces informations classifiées sont produites, manipulées ou emmagasinées ou des projets classifiés sont réalisés, ne sont accordées par l'une des Parties aux visiteurs du pays de l'autre Partie que sur autorisation écrite préalable de l'autorité compétente en matière de sécurité de la Partie qui reçoit ces visiteurs. Cette autorisation ne sera accordée qu'à des personnes qui ont reçu une habilitation de sécurité appropriée et qui ont «besoin d'en connaître».
2. L'autorité de sécurité compétente de la Partie des visiteurs notifie à l'autorité de sécurité compétente de la Partie d'accueil l'identité des visiteurs attendus, trois semaines au moins avant la visite prévue, conformément aux dispositions figurant dans l'annexe B du présent Accord.
3. Chacune des Parties garantit la protection des données personnelles des visiteurs conformément aux lois et réglementations nationales respectives.

Article 10. Sécurité industrielle

1. L'autorité de sécurité compétente de l'une des Parties qui souhaitent passer un contrat classifié avec un entrepreneur dans le pays de l'autre Partie, ou qui souhaite autoriser un de ses propres entrepreneurs à passer un contrat classifié dans le pays de l'autre Partie dans le cadre d'un projet classifié, doit obtenir préalablement, par l'intermédiaire

de l'autorité de sécurité compétente de l'autre Partie, l'assurance écrite que l'entrepreneur envisagé possède une habilitation de sécurité de niveau approprié ainsi que les infrastructures nécessaires pour manipuler et stocker des informations classifiées de même niveau.

2. Tout contrat classifié passé entre des entités des Parties et/ou des organisations privées (tels que des industries, des centres de recherche, des organismes d'assistance et/ou de services) comporte une section appropriée relative à la sécurité et une liste des classifications de sécurité conformes aux termes du présent Accord.

3. L'autorité de sécurité compétente du pays où le travail doit être effectué est tenue de prescrire et d'administrer les mesures de sécurité relatives au contrat selon les mêmes normes et les mêmes exigences que celles qui régissent la protection de ses propres contrats classifiés.

4. Les sous-traitants qui briguent des contrats de sous-traitance classifiés doivent être préalablement soumis pour approbation par l'entrepreneur à l'autorité de sécurité compétente. S'il est agréé, le sous-traitant doit remplir les mêmes obligations de sécurité que celles qui ont été fixées pour l'entrepreneur.

5. Une notification de tout projet, accord, contrat ou contrat de sous-traitance classifié devra être adressé préalablement à l'autorité de sécurité compétente du pays où le projet doit être exécuté.

6. La section relative à la sécurité de tout contrat classifié est transmise en double exemplaire à l'autorité de sécurité compétente du pays où les travaux doivent être effectués.

Article 11. Infraction à la sécurité

En cas d'infraction à la sécurité relative à des informations classifiées qui sont émises ou reçues de l'autre Partie, ou lorsque des intérêts communs sont en jeu, l'autorité de sécurité compétente dans le pays de laquelle la compromission en matière de sécurité s'est produite en informe dès que possible l'autorité de sécurité compétente de l'autre pays et procède à l'enquête qui s'impose. Si elle y est invitée, l'autre Partie coopère à cette enquête. L'autre Partie est informée, par écrit, des résultats de l'instruction, des raisons et de l'ampleur de l'atteinte à la sécurité et des mesures adoptées pour y mettre fin.

Article 12. Dépenses

Les Parties assument chacune les dépenses consenties lors de l'application du présent Accord.

Article 13. Règlement des différends

Les Parties règlent tout différend qui surgirait de l'interprétation ou de l'application du présent Accord par voie de consultation entre les Parties, sans avoir recours à une juridiction externe.

Article 14. Dispositions finales

1. Le présent Accord entrera en vigueur à la date de réception de la dernière notification écrite par laquelle les Parties s'informent mutuellement que les procédures internes nécessaires à sa mise en œuvre ont été accomplies. Il peut être dénoncé à tout moment par l'une et l'autre Partie moyennant une notification écrite. Dans ce cas, le présent Accord prend fin six mois à partir de la date de notification de dénonciation.

2. Chaque Partie informe rapidement l'autre de tout changement apporté à sa propre législation et à ses réglementations susceptible d'exercer une influence sur la protection des informations classifiées mentionnées dans le présent Accord.

3. Le présent Accord peut faire l'objet d'une révision, de modifications et d'amendements en tout temps, après accord mutuel et écrit des Parties.

4. En cas de dénonciation, les informations classifiées transmises en vertu du présent Accord seront restituées. Toute information classifiée non restituée à l'autre Partie sera protégée conformément aux dispositions du présent Accord.

Fait à Riga, le 6 juillet 2005, en deux exemplaires originaux dans chacune des langues suivantes : le letton, le géorgien et l'anglais, tous les textes faisant également foi. En cas de divergence sur l'interprétation, le texte anglais prévaudra.

Pour le Gouvernement de la République de Lettonie :

EDGARS RINKĒVIČS

Secrétaire d'État du Ministère de la défense

Pour le Gouvernement de la Géorgie :

VASIL SIKHARULIDZE

Vice-Ministre de la défense

ANNEXE A DE L'ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE DE LETTONIE ET LE GOUVERNEMENT DE LA GÉORGIE RELATIF À LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

DÉFINITIONS

Aux fins du présent Accord, les termes suivants sont définis comme suit :

1. On entend par «informations classifiées»

a) Tout objet classifié, qu'il s'agisse d'une communication verbale de contenu classifié ou de la transmission électrique ou électronique d'un message classifié ou d'un «matériel» au sens de la définition donnée à l'alinéa b) ci-dessous,

b) «Matériel» inclut les «documents» au sens de la définition qui en est donnée à l'alinéa c) ainsi que toute machine, tout élément d'équipement, toute arme ou tous systèmes d'armes fabriqués ou en cours de fabrication,

c) «Document» s'entend de toute forme d'informations consignées, quel que soit le type de média utilisé pour sa consignation,

qui, dans l'intérêt de la sécurité nationale de la Partie et conformément à ses lois et réglementations en vigueur, ont besoin d'être protégés contre toute divulgation non autorisée et qui a été classifiée conformément à la législation nationale.

2. L'expression «contrat classifié» s'entend d'un accord entre deux ou plusieurs entrepreneurs qui crée et définit des droits et des obligations exécutoires entre ceux-ci, qui contient ou traite d'informations classifiées.

3. Le terme «entrepreneur» désigne une personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés.

4. L'expression «besoin d'en connaître» s'entend du principe selon lequel une décision positive détermine qu'un demandeur potentiel a besoin d'accéder à des informations classifiées pour réaliser des tâches ou des services officiels.

5. L'expression «habilitation de sécurité» désigne une décision positive qui fait suite à une procédure d'enquête destinée à vérifier la capacité d'une personne physique ou morale à avoir accès à des informations classifiées et à manier celles-ci à un certain niveau conformément aux règlements nationaux de sécurité concernés.

6. L'expression «infraction à la sécurité» s'entend d'un acte ou d'une omission contraire aux règles nationales de sécurité dont le résultat peut mettre en danger ou compromettre des informations classifiées.

ANNEXE B DE L'ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE DE LETTONIE ET LE GOUVERNEMENT DE LA GÉORGIE RELATIF À LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

VISITE DU PERSONNEL D'UNE PARTIE AUX INSTALLATIONS, ÉTABLISSEMENTS ETC. DE
L'AUTRE PARTIE

L'accès aux informations classifiées et aux établissements et infrastructures etc. où des activités classifiées sont réalisées ou où des informations classifiées sont stockées ou manipulées n'est accordé par l'une des Parties à des visiteurs de l'autre Partie que si ceux-ci :

- a) Ont subi une vérification par l'autorité de sécurité compétente ou une autre autorité publique compétente du pays qui les envoie et sont habilités à recevoir des informations classifiées conformément aux réglementations nationales du pays d'accueil, et/ou
- b) Sont autorisés par l'autorité de sécurité compétente ou une autre autorité publique compétente à effectuer la visite demandée.

Une demande de visite doit comporter l'information suivante :

- a) Le nom et le prénom, la date et le lieu de naissance, la nationalité et le passeport ou autre document d'identité du visiteur,
- b) Le statut (emploi) officiel du visiteur, y compris le nom de l'établissement, de la société ou de l'organisation que le visiteur représente,
- c) L'attestation de l'habilitation de sécurité ou de l'autorisation administrative du visiteur,
- d) L'objet (nom et adresse de l'établissement/infrastructure à visiter) et le but de la visite,
- e) Le point de contact dans l'établissement/l'infrastructure à visiter, les contacts antérieurs et toute autre information utile pour déterminer le caractère justifié de la visite,
- f) La date et la durée prévues de la visite.

La demande de visite sera introduite :

- a) Par l'intermédiaire de l'autorité de sécurité compétente pour les demandes de visite des citoyens de Géorgie en République de Lettonie,
- b) Par l'intermédiaire de l'autorité de sécurité compétente pour les demandes de visite des citoyens de la République de Lettonie en Géorgie,
- c) D'autres procédures peuvent être utilisées si elles sont approuvées par les deux autorités de sécurité compétentes.

La validité des autorisations de visite n'excédera pas douze (12) mois.

Tous les visiteurs doivent respecter les réglementations nationales en matière de sécurité sur la protection des informations de la Partie d'accueil.