

No. 44225

**Latvia
and
Norway**

Bilateral Security Agreement between the Government of the Republic of Latvia and the Government of the Kingdom of Norway (with annexes). Kongsvinger, 26 August 2005

Entry into force: *26 August 2005 by signature, in accordance with article 13*

Authentic texts: *English, Latvian and Norwegian*

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

**Lettonie
et
Norvège**

Accord bilatéral de sécurité entre le Gouvernement de la République de Lettonie et le Gouvernement du Royaume de Norvège (avec annexes). Kongsvinger, 26 août 2005

Entrée en vigueur : *26 août 2005 par signature, conformément à l'article 13*

Textes authentiques : *anglais, letton et norvégien*

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

[ENGLISH TEXT – TEXTE ANGLAIS]

BILATERAL SECURITY AGREEMENT BETWEEN THE GOVERNMENT
OF THE REPUBLIC OF LATVIA AND THE GOVERNMENT OF THE
KINGDOM OF NORWAY

TABLE OF CONTENTS

1. APPLICABILITY
 2. DEFINITIONS
 3. MUTUAL SECURITY PROTECTION
 4. DISCLOSURE OF INFORMATION
 5. SECURITY CLASSIFICATIONS
 6. COMPETENT SECURITY AUTHORITIES
 7. VISITS
 8. CONTRACTS
 9. COMMUNICATIONS AND TRANSMISSIONS
 10. BREACH OF SECURITY
 11. EXPENSES
 12. DISPUTE SETTLEMENT
 13. FINAL PROVISIONS
- ANNEX A TO THE SECURITY AGREEMENT
ANNEX B TO THE SECURITY AGREEMENT

The Government of the Republic of Latvia and The Government of the Kingdom of Norway, hereafter called the 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:

1. APPLICABILITY

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. Co-operation between governmental entities of the two Parties.

b. Co-operation, exchange of information, joint ventures, contracts or any other 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.

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

The Annexes A and B to this Agreement are integral parts of the Agreement.

2. DEFINITIONS

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

3. MUTUAL SECURITY PROTECTION

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 5 and Annex A to this Agreement.

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 granted a security clearance, as defined in Annex A, and who, due to their functions or employment, have a "need to know", as defined in Annex A.

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. DISCLOSURE OF INFORMATION

The Parties shall not disclose classified information under this Agreement to third parties or nationals of other countries 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.

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 such classified information in accordance with its own standards and requirements.

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 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.

5. SECURITY CLASSIFICATIONS

Classified information shall be marked in one of the following security classification levels:

LATVIA	Equivalent	NORWAY
SEVIŠĶI SLEPENI	TOP SECRET	STRENGT HEMMELIG
SLEPENI	SECRET	HEMMELIG
KONFIDENCIĀLI	CONFIDENTIAL	KONFIDENSIELT
DIENESTA VAJADZĪBĀM	RESTRICTED	BEGRENSET

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.

The receiving Party shall additionally mark the received classified information with its own equivalent security classification level. Translations and reproductions shall be marked with the same security classification level as the original, in both languages.

6. COMPETENT SECURITY AUTHORITIES

The receiving Party shall appoint and make known to the other Party a duly authorized 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.

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 Norway:

Norwegian National Security Authority
Postboks 14

1306 Børum postterminal
Norway

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

Both Competent Security Authorities, each within the jurisdiction of its own state, shall prepare, distribute and supervise security instructions and procedures for the protection of the classified information exchanged as a result of any other agreement between the Parties.

Each Competent Security Authority shall, upon request, furnish the other Competent Security Authority information concerning its security organization and procedures 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.

7. VISITS

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 security cleared and have a "need to know".

The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the receiving Party of expected visitors at least three -3- weeks prior to the planned visit, in accordance with the procedures defined in Annex B to this Agreement.

Each Party shall guarantee the protection of personal data of the visitors according to the respective national legislation.

8. CONTRACTS

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 authorize 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 security clearance of appropriate level and has the facilities to handle and store classified information of the same level. For RESTRICTED level a security assurance, as defined in Annex A, will be provided.

Every classified contract between entities of the Parties and/or private organizations (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.

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.

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

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.

Two -2- 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.

9. COMMUNICATIONS AND TRANSMISSIONS

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

Exchange of classified information can also take place through representatives officially appointed by the authorities in both countries. Such authorization may, when required, be given to representatives of industrial undertakings engaged in specific projects.

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

Other approved means of transmission or exchange may be used if agreed upon by each Competent Security Authority.

10. BREACH OF SECURITY

In case of a breach of security, as defined in Annex A, concerning classified information originated or received from the other Party, or if common interests are involved, the Competent Security Authority in whose country the compromise occurs shall inform the Competent Security Authority of the other country as soon as possible and carry out the appropriate investigation. The other Party shall, if required, co-operate in the investigation. In any case, the other Party is to be informed of the results of the investigation and shall receive a final statement as to the reasons and extent of the security violation.

11. EXPENSES

Expenses incurred by either Party with respect to this Agreement, in particular concerning the implementation of security measures, shall not be subject to reimbursement between the Parties.

12. DISPUTE SETTLEMENT

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation between the Parties and will not be referred to any national or international tribunal or third party for settlement.

13. FINAL PROVISIONS

This Agreement shall be effective from the date of signing and remain in force for unlimited time. It may be terminated at any time by either Party in the way of a written notification. In such a case the Agreement expires six -6- months from the date the notification of termination has been received by the other Party.

The review, changes and amendments of the present Agreement may be done at any time with consent of both Parties in written form.

In the event of termination, classified items and/or information transmitted under the terms of this Agreement shall be returned to the other Party as soon as possible. Classified information and/or items that are not returned shall be protected in accordance with the provisions laid down in this Agreement.

Done in Kongsvinger, Norway on 26 August 2005 in two authentic copies in the Latvian, Norwegian and English languages, all texts being equally authentic. In case of difference of interpretation of the provisions of this Agreement, the English text shall prevail.

On behalf of the Government of the Republic of Latvia:

EINARS REPŠE
Minister of Defence

On behalf of The Government of the Kingdom of Norway:

KRISTIN KROHN DEVOLD
Minister of Defence

ANNEX A TO THE SECURITY AGREEMENT

DEFINITIONS

For the purpose of this Agreement:

- 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. The term "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. The term "document" means any form of recorded information regardless of type of recording media.

- Contract means

An agreement between two or more parties creating and defining enforceable rights and obligations between the parties.

- Classified contract means

A contract, which contains or involves classified information.

- Contractor means

An individual or legal entity possessing the legal capability to undertake contracts.

- Breach of security means

An act or an omission contrary to national security regulations, the result of which may endanger or compromise classified information.

- Security compromise means

That classified information is compromised because knowledge of it has, in whole or part, passed to persons or entities or countries without appropriate security clearance or authority to have such access, or when it has been subject to a risk of such passing.

- 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.

- Security assurance means

A statement issued by the Competent Security Authority declaring that classified information at restricted level will be protected in accordance with its national regulations.

- "Need to know" means

That access to classified information may only be granted if the person requiring it has a verified need to know in connection with his/her official duties, within the framework of which the information was released to the receiving Party.

Security classifications and use:

To be applied to information of which unauthorized disclosure would have the following consequences for the interest of the State:

LATVIA	NORWAY	
SEVIŠĶI SLEPENI	STRENGT HEMMELIG	exceptionally grave
SLEPENI	HEMMELIG	serious damage
KONFIDENCIĀLI	KONFIDENSIELT	prejudicial
DIENESTA VAJADZĪBĀM	BEGRENSET	undesirable

ANNEX B TO THE SECURITY AGREEMENT

VISITS BY PERSONNEL OF ONE PARTY TO THE ESTABLISHMENTS, FACILITIES, 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 authorized to receive classified information in accordance with the national regulations of the host country, and/or
- b. Authorized by the Competent Security Authority or other competent government authority of the respective country to perform the required visit or visits.

The Competent Security Authority of the requesting Party shall notify the Competent Security Authority of the country to be visited of the planned visit in accordance with the provisions laid down in this annex, and shall make sure that the latter receives the visit request three - 3 - weeks before the visit or visits will take place.

The visit request shall include:

- a. A visitor's surname, name, place and date of birth, nationality and employer, passport or other identity documents of the visitor.
- b. Certification of the visitor's security clearance in accordance with the purpose of the visit.
- c. Object and purpose of the visit or visits. (The indications must be accurate and sufficiently detailed. General indications and abbreviations are to be avoided.)
- d. Expected date and duration of the requested visit or visits.
- 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 or visits

The request will be submitted:

- a. Through the Norwegian Embassy in Riga for visit requests of Norwegian citizens to Latvia.
- b. Through the Latvian Embassy in Oslo for visit requests of Latvian citizens to Norway.
- c. Other procedures may be used if agreed upon by the two Competent Security Authorities.

The validity of visit authorizations shall not exceed twelve - 12 - months.

The classified information exchanged during a visit shall have the same degree of protection and classification level as that of the originating Party.

[LATVIAN TEXT – TEXTE LETTON]

LATVIJAS REPUBLIKAS VALDĪBAS

UN

NORVĒGIJAS KARALISTES VALDĪBAS

DROŠĪBAS LĪGUMS

SATURA RĀDĪTĀJS

1. PIEMĒROŠANA	3
2. DEFINĪCIJAS	3
3. SAVSTARPĒJĀ INFORMĀCIJAS AIZSARDZĪBA	3
4. INFORMĀCIJAS ATKLĀŠANA	4
5. INFORMĀCIJAS AIZSARDZĪBAS PAKĀPES	5
6. ATBILDĪGĀS DROŠĪBAS IESTĀDES	5
7. VIZĪTES	6
8. LĪGUMI	6
9. INFORMĀCIJAS APMAIŅA UN PĀRSŪTĪŠANA	7
10. DROŠĪBAS PRASĪBU PĀRKĀPUMS	8
11. IZDEVUMI	8
12. STRĪDU IZŠĶIRŠANA	8
13. NOBEIGUMA JAUTĀJUMI	8
DROŠĪBAS LĪGUMA PIELIKUMS A	10
DROŠĪBAS LĪGUMA PIELIKUMS B	12

Latvijas Republikas valdība un Norvēģijas Karalistes 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. PIEMĒROŠANA

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.

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

Šī Līguma pielikumi A un B ir Līguma neatņemamas sastāvdaļas.

2. DEFINĪCIJAS

Galvenie šajā Līgumā lietotie termini ir definēti pielikumā A.

3. SAVSTARPĒJA INFORMĀCIJAS AIZSARDZĪBA

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 šī Līguma 5. pantā un pielikumā A.

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 saņēmušas speciālo atļauju, kas definēta pielikumā A, un kurām saistībā ar viņu funkcijām vai darba pienākumiem ir “nepieciešamība zināt”, kas definēta pielikumā A.

Katra Puse pārrauga ar drošību saistīto 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. INFORMĀCIJAS ATKLĀŠANA

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

Ja kāda no Pusēm un/vai tās institūcijas vai juridiskās personas, kas ir saistītas ar 1.pantā 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 tā Puse, kurā tiek veikta darbu izpilde, uzņemas atbildību par šīs klasificētās informācijas pārraudzību saskaņā ar savas valsts standartiem un prasībām.

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 industriālās drošības sertifikātu attiecīgajiem līgumslēdzējiem.
- c. Izsniedz speciālo atļauju visiem darbiniekiem, 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. INFORMĀCIJAS AIZSARDZĪBAS PAKĀPES

Klasificētā informācija tiek apzīmēta ar vienu no sekojošajām informācijas aizsardzības pakāpēm:

Latvija	Ekvivalents	Norvēģija
SEVIŠKI SLEPENI	TOP SECRET	STRENGT HEMMELIG
SLEPENI	SECRET	HEMMELIG
KONFIDENCIĀLI	CONFIDENTIAL	KONFIDENSIELT
DIENESTA VAJADZĪBĀM	RESTRICTED	BEGRENSET

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

Saņēmēja Puse papildus piešķir saņemtajai klasificētai informācijai savu atbilstošo informācijas aizsardzības pakāpi. Tulkojumiem un kopijām tiek piešķirta tāda pati informācijas aizsardzības pakāpe kā oriģinālam, abās Pušu valodās.

6. ATBILDĪGĀS DROŠĪBAS IESTĀDES

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

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

Latvijā:

Satversmes aizsardzības birojs
Miera 85a, Rīga, LV-1013,
LATVIJA

Norvēģijā:

Norvēģijas Nacionālā drošības iestāde
Postboks 14
1306 Baerum postterminal,
NORVĒGIJA

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

Atbildīgās drošības iestādes, katra savas valsts jurisdikcijā, sagatavo, izplata un pārrauga drošības noteikumus un procedūras klasificētās informācijas aizsardzībai, ar kurām Puses apmainās uz cita starp Pusēm noslēgta līguma pamata.

Vienas Puses Atbildīgā drošības iestāde pēc pieprasījuma iesniedz otras Puses Atbildīgajai drošības iestādei informāciju par drošības pasākumu organizāciju un procedūrām, lai salīdzinātu un ievērotu tādas pašas drošības noteikumus, un veicina pilnvarotu amatpersonu kopīgas vizītes abās valstīs. Abām Pusēm ir jāsaņem šādas vizītes.

7. VIZĪTES

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 tikai tad, ja iepriekš ir saņemta rakstiska atļauja no apmeklējošās Puses Atbildīgās drošības iestādes. Šāda atļauja tiek piešķirta tikai personām, kuras ir saņēmušas speciālo atļauju un kurām ir “nepieciešamība zināt”.

Nosūtītājas Puses Atbildīgā drošības iestāde paziņo apmeklējošās Puses Atbildīgajai drošības iestādei par gaidāmajiem apmeklētājiem vismaz trīs 3 nedēļas pirms plānotās vizītes, ievērojot šī līguma pielikumā B noteikto kārtību.

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

8. LĪGUMI

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.

Informācijai “dienesta vajadzībām” tiek izsniegts drošības apliecinājums, kā definēts pielikumā A.

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

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.

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.

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

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

9. INFORMĀCIJAS APMAIŅA UN PĀRSŪTĪŠANA

Parasti klasificētā informācija starp Pusēm tiek nosūtīta caur to attiecīgajiem diplomātiskajiem kanāliem.

Klasificētās informācijas apmaiņa var notikt izmantojot pārstāvjus, kurus oficiāli pilnvaro abu valstu kompetentas institūcijas. Šāda atļauja, ja nepieciešams, var tikt piešķirta attiecīgajos projektos iesaistītajiem uzņēmumu pārstāvjiem.

Klasificētās informācijas lielu objektu vai liela apjoma nosūtīšana tiek saskaņota katrā gadījumā atsevišķi.

Citi apstiprināti informācijas nosūtīšanas vai apmaiņas veidi var tikt izmantoti, ja par to vienojas Pušu Atbildīgās drošības iestādes.

10. DROŠĪBAS PRASĪBU PĀRKĀPUMS

Drošības prasību pārkāpuma gadījumā, kā definēts pielikumā A, 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. Jebkurā gadījumā otra Puse tiek informēta par izmeklēšanas rezultātiem, un tai tiek nosūtīts nobeiguma ziņojums par drošības prasību pārkāpuma iemesliem un apmēru.

11. IZDEVUMI

Abu Pušu izdevumi saistībā ar šo Līgumu, tai skaitā sakarā ar drošības pasākumu īstenošanu, nav atlīdzināmi starp Pusēm.

12. STRĪDU IZŠKIRŠANA

Jebkurš strīds par šī Līguma interpretāciju vai piemērošanu tiek atrisināts konsultāciju ceļā starp Pusēm un netiek nodots risināšanai nevienam nacionālam vai starptautiskam tribunālam vai trešajai pusei.

13. NOBEIGUMA NOTEIKUMI

Šis Līgums stājas spēkā no tā parakstīšanas datuma un ir noslēgts uz nenoteiktu laiku. 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.

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

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

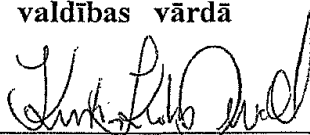
Līgums noslēgts 26.08.2005, Kongslingeā, Norvēģijā divos (2) oriģinālos eksemplāros latviešu, norvēģu un angļu valodās, un visi teksti ir vienlīdz autentiski. Dažādu Līguma noteikumu interpretāciju gadījumā noteicošais ir teksts angļu valodā.

**Latvijas Republikas
valdības vārdā**



EINARS REPŠE
aizsardzības ministrs

**Norvēģijas Karalistes
valdības vārdā**



KRISTIN KROHN DEVOLD
aizsardzības ministre

Drošības Līguma pielikums A

Definīcijas

Šī Līguma ietvaros lieto sekojošus terminus:

•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 ir izgatavota vai ir izgatavošanas procesā,
- c. Termins “dokuments” nozīmē jebkuru pierakstītas informācijas formu, neatkarīgi no pieraksta veida.

•Līgums

Līgums starp divām vai vairākām pusēm, kas nodibina un nosaka izpildāmas pušu tiesības un pienākumus.

•Klasificēts līgums

Līgums, kas satur vai ir saistīts ar klasificēto informāciju.

•Līgumslēdzējs

Individuāla vai juridiska persona, kas ir tiesīga uzņemties līguma izpildi.

•Drošības prasību pārkāpums

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

•Klasificētas informācijas nesankcionēta izpaušana

Klasificētā informācija ir pilnībā vai daļēji nonākušas tādu personu, institūciju vai valstu rīcībā, kas nav saņēmušas speciālās atļaujas vai industriālās drošības sertifikātus, vai kam nav šādu pieejas tiesību, vai arī gadījumā, ja informācija ir tikusi pakļauta šādas nodošanas riskam.

• **Speciālā atļauja**

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

• **Drošības apliecinājums**

Atbildīgās drošības iestādes izsniegts paziņojums, ka informācija dienesta vajadzībām tiks aizsargāta saskaņā ar nacionāliem normatīviem aktiem.

• **“Nepieciešamība zināt”**

Pieeja klasificētai informācijai var tikt piešķirta vienīgi tad, ja personai, kas to pieprasa, ir nepieciešamība to zināt saistībā ar viņa/viņas darba pienākumiem, ja līguma ietvaros informācija ir tikusi nodota saņēmējai Līgumslēdzējai Pusei.

Informācijas aizsardzības pakāpes un to pielietošana:

Attiecas uz informāciju, kuras nesankcionētai izpaušanai būtu sekojoša ietekme uz valsts interesēm:

LATVIJA	NORVĒGIJA	
SEVIŠKI SLEPENI	STRENGT HEMMELIG	ārkārtīgi nopietna
SLEPENI	HEMMELIG	nopietns kaitējums
KONFIDENCIĀLI	KONFIDENSIELT	kaitīga
DIENESTA VAJADZĪBĀM	BEGRENSET	nevēlama

Drošības Līguma pielikums B

Vienas Līgumslēdzējas Puses pilnvaroto personu vizītes otras Līgumslēdzējas 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 tikai 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 vai vizītes.

Nosūtītājas Puses Atbildīgā drošības iestāde paziņo tās valsts Atbildīgajai drošības iestādei, kuru paredzēts apmeklēt, par plānoto vizīti saskaņā ar noteikumiem, kas izklāstīti šajā pielikumā, un nodrošina, lai tā saņemtu vizītes pieprasījumu trīs nedēļas pirms šīs vizītes vai vizīšu sākuma.

Vizītes pieprasījumā jāietver:

- a. Apmeklētāja uzvārds, vārds, dzimšanas vieta un datums, tautība un darba vieta, informācija par apmeklētāja pasēs datiem vai citiem personību apliecinošiem dokumentiem.
- b. Apmeklētāja speciālās atļaujas apstiprinājums saskaņā ar vizītes mērķi.
- c. Vizītes vai vizīšu mērķis un uzdevumi. (Informācijai ir jābūt precīzai un detalizētai. Netiek iekļauta vispārēja rakstura informācija un saīsinājumi).
- d. Vizītes vai vizīšu plānotais datums un ilgums.
- e. Kontaktpersona institūcijā / objektā, ko paredzēts apmeklēt, iepriekšēja sadarbība un cita informācija par vizītes vai vizīšu pamatojumu.

Pieprasījums tiek iesniegts, izmantojot:

- a. Norvēģijas vēstniecību Rīgā, lai pieteiktu Norvēģijas pilsoņu vizītes Latvijā.

b. Latvijas vēstniecību Oslo, lai pieteiktu Latvijas pilsoņu vizītes Norvēģijā.

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

Vizītes apstiprinājuma derīguma termiņš nepārsniedz divpadsmit mēnešus.

Klasificētajai informācijai, ar ko apmainās vizītes laikā, tiek nodrošināta tāda pati aizsardzības pakāpe, kādu ir noteikusi tā Puse, kurai informācija pieder.

[NORWEGIAN TEXT – TEXTE NORVÉGIEN]

BILATERAL SIKKERHETSAVTALE
mellom
REPUBLIKKEN LATVIAS REGJERING
og
KONGERIKET NORGES REGJERING

Innhold

1 VIRKEOMRÅDE	3
2 DEFINISJONER	3
3 GJENSIDIGE SIKKERHETSTILTAK	3
4 UTLEVERING AV INFORMASJON	4
5 GRADERINGER	4
6 KOMPETENTE SIKKERHETSMYNDIGHETER	5
7 BESØK	6
8 KONTRAKTER	7
9 FORMIDLING OG OVERFØRING	7
10 SIKKERHETSBRUDD	8
11 KOSTNADER	8
12 TVISTELØSNING	8
13 SLUTTBESTEMMELSER	8
Vedlegg A til sikkerhetsavtalen	10
Vedlegg B til sikkerhetsavtalen	11

Republikken Latvias regjering og Kongeriket Norges regjering, heretter kalt partene, er, for å sikre gradert informasjon som utveksles direkte eller via andre administrative enheter eller private rettssubjekter som håndterer gradert informasjon under hver av partenes jurisdiksjon, blitt enige om følgende

1 VIRKEOMRÅDE

Denne avtale skal utgjøre en integrert del av enhver framtidig kontrakt eller avtale som innebærer utveksling av gradert informasjon og som partene inngår eller undertegner på følgende områder:

- a. samarbeid mellom de to partenes statlige enheter,
- b. samarbeid, utveksling av informasjon, fellesforetak, kontrakter eller andre forbindelser mellom partenes statlige enheter og/eller private rettssubjekter,
- c. salg av utstyr og kompetanse fra den ene part til den annen.

Ingen av partene kan påberope seg denne avtale for å få hånd om gradert informasjon som den annen part har mottatt fra en tredjepart.

Vedlegg A og B til denne avtale er integrerte deler av avtalen.

2 DEFINISJONER

De sentrale begrepene i denne avtale er definert i vedlegg A.

3 GJENSIDIGE SIKKERHETSTILTAK

I samsvar med sine nasjonale lover og forskrifter og sin nasjonale praksis skal begge parter treffe hensiktsmessige tiltak for å beskytte gradert informasjon som overføres, mottas, produseres eller utvikles som et resultat av enhver avtale eller forbindelse mellom partene. Partene skal gi all gradert informasjon som er overført, mottatt, produsert eller utviklet, den samme sikkerhetsbeskyttelse som de gir sin egen graderte informasjon med tilsvarende gradering, som definert i denne avtales artikkel 5 og vedlegg A.

Tilgangen til gradert informasjon og til steder og anlegg der gradert virksomhet utføres eller der gradert informasjon oppbevares, begrenses til personer som er sikkerhetsklarert som definert i vedlegg A og som på grunn av sine oppgaver eller sin stilling har behov for innsyn som definert i vedlegg A

Hver part skal, blant annet gjennom kontrollbesøk, føre tilsyn med overholdelsen av lover, forskrifter og praksis vedrørende sikkerhet i de institusjoner, kontorer og anlegg innenfor dens jurisdiksjon som besitter, utvikler, produserer og/eller bruker den annen parts gradert informasjon.

4 UTLEVERING AV INFORMASJON

Partene skal ikke utlevere gradert informasjon i henhold til denne avtale til tredjeparter eller borgere av andre land uten skriftlig forhåndssamtykke fra den utstedende part. Gradert informasjon som en part har mottatt fra den annen part, skal utelukkende benyttes til det fastsatte formål.

Dersom en av partene og/eller dens institusjoner eller enheter som befatter seg med de saker som er nevnt i artikkel 1, tildeler en kontrakt som skal oppfylles på den annen parts territorium, og denne kontrakt innbefatter gradert informasjon som partens utførende leverandør sitter inne med, skal den part i hvis land oppfyllelsen i henhold til denne avtale finner sted, påta seg ansvaret for å administrere slik gradert informasjon i samsvar med sine egne standarder og krav

Før gradert informasjon mottatt fra den ene part frigis overfor den annen parts leverandører eller potensielle leverandører, skal den mottakende part:

- a. sikre at disse leverandører eller potensielle leverandører og deres anlegg er i stand til å beskytte den graderte informasjonen på tilfredsstillende måte,
- b. utstede nødvendig leverandørklarering,
- c. utstede nødvendig sikkerhetsklarering for alt personell hvis tjenesteoppgaver krever adgang til den graderte informasjonen,
- d. sikre at alle som har adgang til den graderte informasjonen, blir gjort kjent med sitt ansvar for å beskytte informasjonen i samsvar med den lovgivning som kommer til anvendelse,
- e. foreta regelmessige sikkerhetsinspeksjoner ved aktuelle klarerte anlegg

5 GRADERINGER

Gradert informasjon skal merkes med en av følgende graderinger:

LATVIA	Tilsvarende gradering	NORGE
SEVIŠĶI SLEPENI	TOP SECRET	STRENGT HEMMELIG
SLEPENI	SECRET	HEMMELIG
KONFIDENCIĀLI	CONFIDENTIAL	KONFIDENSIELT
DIENESTA VAJADZĪBĀM	RESTRICTED	BEGRENSET

Den mottakende part skal verken benytte en lavere gradering for mottatt gradert informasjon eller avgradere informasjonen uten skriftlig forhåndssamtykke fra den utstedende part. Den utstedende part skal gjøre den mottakende part kjent med eventuelle endringer i graderingen av den informasjon som utveksles.

Den mottakende part skal i tillegg merke den mottatte graderte informasjon med sin egen tilsvarende gradering. Oversettelser og gjengivelser skal merkes med samme gradering som originalen, på begge språk

6 KOMPETENTE SIKKERHETSMYNDIGHETER

Den mottakende part skal utpeke og kunngjøre for den annen part en sikkerhetsmyndighet med behørig fullmakter, heretter kalt den kompetente sikkerhetsmyndighet, som skal føre tilsyn med alle sikkerhetsaspekter ved gjennomføringen av enhver avtale som definert i artikkel 1 i denne avtale.

De kompetente sikkerhetsmyndigheter med ansvar for gjennomføringen av og kontrollen med alle sider av denne avtale er:

I Latvia:
Constitution Protection Bureau
Miera 85a, Riga, LV-1013,
LATVIA

I Norge:
Nasjonal sikkerhetsmyndighet
Postboks 14
1306 Bærum postterminal
NORGE

Hver av partene forplikter seg til å sikre at bestemmelsene i denne avtale blir behørig overholdt av dens kompetente sikkerhetsmyndighet

De to kompetente sikkerhetsmyndighetene skal, hver innenfor sin egen stats jurisdiksjon, utarbeide, distribuere og føre tilsyn med sikkerhetsinstruksjer og prosedyrer for beskyttelse av gradert informasjon som utveksles som et resultat av andre avtaler mellom partene.

Hver kompetente sikkerhetsmyndighet skal etter anmodning gi den annen parts kompetente sikkerhetsmyndighet opplysninger om sin organisering av sikkerheten og sine sikkerhetsrutiner for å gjøre det mulig å sammenlikne og opprettholde de samme sikkerhetsstandarder, og legge forholdene til rette for felles besøk i begge land av godkjente tjenestemenn. Begge parter må samtykke i slike besøk.

7 BESØK

Besøk med henblikk på utveksling av gradert informasjon i lokaliteter der gradert informasjon utvikles, håndteres eller oppbevares, eller der graderte prosjekter utføres, vil bli innvilget av en part for besøkende fra den annen parts land bare dersom det på forhånd er innhentet skriftlig tillatelse fra den mottakende parts kompetente sikkerhetsmyndighet. Slik tillatelse vil bare bli gitt til personer som er sikkerhetsklarert og har behov for innsyn.

Den kompetente sikkerhetsmyndighet hos den part som sender besøkende, skal varsle den mottakende parts kompetente sikkerhetsmyndighet om besøkende som ventes minst tre -3- uker før det planlagte besøk, i samsvar med de rutiner som er definert i vedlegg B til denne avtale

Hver part skal garantere at besøkendes personvern blir ivaretatt i samsvar med partens nasjonale lovgivning.

8 KONTRAKTER

Den kompetente sikkerhetsmyndighet hos den part som ønsker å inngå en gradert kontrakt med en leverandør i den annen parts land, eller som ønsker å gi en av sine egne leverandører tillatelse til å inngå en gradert kontrakt innenfor et gradert prosjekt i den annen parts land, skal på forhånd innhente en skriftlig forsikring fra den annen parts kompetente sikkerhetsmyndighet om at den foreslåtte leverandør har sikkerhetsklarering på nødvendig nivå og har de anlegg som skal til for å håndtere og oppbevare gradert informasjon på samme nivå. For graderingen BEGRENSET vil det bli gitt en sikkerhetsforsikring som definert i vedlegg A.

Alle graderte kontrakter mellom partenes enheter og/eller private organisasjoner (for eksempel industriforetak, forskningssentre, støtte- og/eller serviceanlegg osv) skal inneholde passende sikkerhetsbestemmelse(r), samt en graderingsliste, basert på bestemmelsene i denne avtale.

Den kompetente sikkerhetsmyndighet i landet der arbeidet skal utføres, skal ta ansvar for å pålegge og administrere sikkerhetstiltak for kontrakten etter de samme standarder og krav som dem som gjelder for beskyttelse av egne graderte kontrakter.

Underleverandører med interesse i graderte underleverandørkontrakter skal av leverandøren på forhånd presenteres for den kompetente sikkerhetsmyndighet til godkjenning. Underleverandøren skal, dersom han godkjennes, oppfylle de samme sikkerhetsforpliktelser som dem som er fastsatt for leverandøren.

Underretning om graderte prosjekter, avtaler, kontrakter eller underleverandørkontrakter skal på forhånd oversendes den kompetente sikkerhetsmyndighet i landet der prosjektet skal utføres

To (2) kopier av sikkerhetsbestemmelsen(e), enhver gradert kontrakt, oversendes til den kompetente sikkerhetsmyndighet i landet der arbeidet skal utføres

9 FORMIDLING OG OVERFØRING

Gradert informasjon skal normalt overføres fysisk mellom partene via deres respektive diplomatiske kanaler

Utveksling av gradert informasjon kan også skje via representanter som er offisielt utpekt av begge parters myndigheter. Slik fullmakt kan om

kan om nødvendig gis til representanter for industriforetak som deltar i konkrete prosjekter.

Levering av gradert informasjon i store enheter eller mengder skal avtales særskilt i hvert enkelt tilfelle.

Andre godkjente metoder for overføring eller utveksling kan benyttes dersom begge kompetente sikkerhetsmyndigheter er enige om det.

10 SIKKERHETSBRUDD

Ved sikkerhetsbrudd, som definert vedlegg A, i forbindelse med gradert informasjon utstedt av eller mottatt fra den annen part, eller dersom felles interesser blir berørt, skal den kompetente sikkerhetsmyndighet i landet der kompromitteringen finner sted, snarest mulig underrette det annet lands kompetente sikkerhetsmyndighet og gjennomføre nødvendig undersøkelse. Den annen part skal om nødvendig bistå i undersøkelsen. I ethvert tilfelle skal den annen part underrettes om resultatene av undersøkelsen, og skal motta en endelig redegjørelse for grunnene til og omfanget av sikkerhetsovertredelsen.

11 KOSTNADER

Kostnader som partene påføres i forbindelse med denne avtale, særlig med hensyn til gjennomføringen av sikkerhetstiltak, refunderes ikke partene imellom.

12 TVISTELØSNING

Enhver tvist om tolkningen eller gjennomføringen av denne avtale skal løses ved konsultasjoner mellom partene, og skal ikke henvises til noen nasjonal eller internasjonal domstol eller tredjepart for avgjørelse.

13 SLUTTBESTEMMELSER

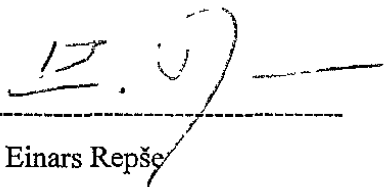
Denne avtale trer i kraft på undertegningsdatoen og gjelder på ubestemt tid. Den kan når som helst sies opp av hver av partene ved skriftlig underretning. I så fall opphører avtalen seks -6- måneder etter datoen da underretningen om oppsigelse er mottatt av den annen part.

Gjennomgang av, endringer i eller tilføyelser til denne avtale kan foretas på ethvert tidspunkt etter skriftlig samtykke fra begge parter

Ved opphør skal graderte enheter og/eller informasjon som er overført i henhold til denne avtale, returneres til den annen part så snart som mulig. Gradert informasjon og/eller enheter som ikke returneres, skal beskyttes i samsvar med bestemmelsene i denne avtale.

Utferdiget i *Kongsvinger, Norge*... den *26 August 2005*... i to autentiske eksemplarer på latvisk, norsk og engelsk, hvorav alle tekster har samme gyldighet. Ved avvikende tolkninger skal engelsk tekst gjelde

For Republikken Latvias
regjering



Einars Repše

forsvarsminister

For Kongeriket Norges
regjering



Kristin Krohn Devold

forsvarsminister

Vedlegg A til sikkerhetsavtalen

Definisjoner

I denne avtale menes med

- **Gradert informasjon:**

a. enhver gradert enhet, enten det dreier seg om en muntlig formidling av et gradert innhold, elektrisk eller elektronisk overføring av en gradert melding, eller ”materiale” som definert under b) nedenfor,

b. uttrykket ”materiale” omfatter ”dokument” som definert under c) nedenfor, samt deler av maskineri, utstyr, våpen eller våpensystem som er produsert eller er under produksjon,

c. uttrykket ”dokument” omfatter enhver form for registrerte opplysninger uansett type registreringsmedium.

- **Kontrakt:**

en avtale mellom to eller flere parter som stifter og definerer bindende rettigheter og forpliktelser mellom partene.

- **Gradert kontrakt:**

en kontrakt som inneholder eller involverer gradert informasjon.

- **Leverandør:**

en fysisk eller juridisk person med rettshandelseevne til å inngå kontrakter.

- **Sikkerhetsbrudd:**

en handling eller en unnlatelse som er i strid med nasjonale sikkerhetsbestemmelser og som kan medføre at gradert informasjon settes i fare eller kompromitteres.

- **Kompromittering:**

at gradert informasjon er kompromittert ved at den, enten delvis eller i sin helhet, er blitt gjort kjent for, eller blitt utsatt for risiko for å bli gjort kjent for, personer eller enheter eller land uten nødvendig sikkerhetsklarering eller tillatelse til slik tilgang.

- **Sikkerhetsklarering:**

en positiv beslutning som følge av en undersøkelse med det formål å fastslå om en person eller enhet er skikket til å ha tilgang til og å

informasjon på et bestemt nivå, i samsvar med de respektive lands nasjonale bestemmelser.

- **Sikkerhetsforsikring:**

en erklæring utstedt av den kompetente sikkerhetsmyndighet som slår fast at gradert informasjon på BEGRENSET nivå vil bli beskyttet i samsvar med nasjonale bestemmelser.

- **Behov for innsyn:**

at tilgang til gradert informasjon bare kan innvilges dersom den som ber om det har et dokumentert behov for innsyn i forbindelse med sine tjenesteoppgaver, innenfor de rammer som lå til grunn for at informasjonen ble frigitt overfor den mottakende part.

- **Graderinger og deres bruk:**

Brukes om informasjon hvor uautorisert utlevering ville ha følgende konsekvenser for statens interesser:

LATVIA	NORGE	
SEVIŠĶI SLEPENI	STRENGT HEMMELIG	særlig graverende
SLEPENI	HEMMELIG	til alvorlig skade
KONFIDENCIĀLI	KONFIDENSIELT	skadelig
DIENESTA VAJADZĪBĀM	BEGRENSET	ikke ønskelig

Vedlegg B til sikkerhetsavtalen

Besøk av personell fra en part i den annen parts virksomheter, anlegg osv.

En part skal gi besøkende fra den annen part tilgang til gradert informasjon og til virksomheter og anlegg osv. der gradert virksomhet utøves eller der gradert informasjon oppbevares eller håndteres, bare dersom de besøkende:

- a. er kontrollert av den kompetente sikkerhetsmyndighet eller annen kompetent offentlig myndighet i landet som sender dem, og har tillatelse til å motta gradert informasjon i henhold til de nasjonale bestemmelser i vertslandet, og/eller
- b. har tillatelse fra den kompetente sikkerhetsmyndighet eller annen kompetent offentlig myndighet i det respektive land til å gjennomføre det eller de nødvendige besøk.

Den kompetente sikkerhetsmyndighet hos den part som fremmer anmodningen, skal underrette den kompetente sikkerhetsmyndighet hos parten som skal motta besøk om det planlagte besøket i samsvar med bestemmelsene i dette vedlegg, og skal sørge for at sistnevnte mottar besøksanmodningen tre -3- uker før besøket eller besøkene vil finne sted.

Besøksanmodningen skal omfatte:

- a. den besøkendes fornavn, etternavn, fødested og fødselsdato, nasjonalitet og arbeidsgiver, samt den besøkendes pass eller annet identifikasjonsdokument,
- b. bekreftelse på den besøkendes sikkerhetsklarering i samsvar med hensikten med besøket,
- c. målet og hensikten med besøket eller besøkene. (Disse opplysningene må være nøyaktige og tilstrekkelig detaljerte. Generelle opplysninger og forkortelser skal unngås.),
- d. forventet dato og varighet for besøket eller besøkene som det anmodes om,
- e. kontaktperson ved virksomheten/anlegget som skal besøkes, tidligere kontakter og eventuelle andre opplysninger som kan tjene til å fastslå om besøket eller besøkene er berettiget.

Anmodningen skal fremmes:

- a. gjennom Norges ambassade i Riga hva angår anmodninger fra norske statsborgere om besøk i Latvia,
- b. gjennom Latvias ambassade i Oslo hva angår anmodninger fra latviske statsborgere om besøk i Norge,
- c. på annen måte dersom de to kompetente sikkerhetsmyndighetene er enige om det.

Besøkstillatelser skal ikke være gyldige i mer enn tolv -12- måneder.

Gradert informasjon som utveksles under et besøk, skal ha samme grad av beskyttelse og samme gradering som hos den utstedende part.

ACCORD BILATÉRAL DE SÉCURITÉ ENTRE LE GOUVERNEMENT DE
LA RÉPUBLIQUE DE LETTONIE ET LE GOUVERNEMENT DU
ROYAUME DE NORVÈGE

TABLE DES MATIÈRES

1. APPLICABILITÉ
 2. DÉFINITIONS
 3. PROTECTION DE SÉCURITÉ RÉCIPROQUE
 4. DIVULGATION D'INFORMATIONS
 5. CLASSIFICATIONS EN MATIÈRE DE SÉCURITÉ
 6. AUTORITÉS COMPÉTENTES EN MATIÈRE DE SÉCURITÉ
 7. VISITES
 8. CONTRATS
 9. COMMUNICATIONS ET TRANSMISSIONS
 10. VIOLATION DE LA SÉCURITÉ
 11. DÉPENSES
 12. RÈGLEMENT DES DIFFÉRENDS
 13. DISPOSITIONS FINALES
- ANNEXE A À L'ACCORD DE SÉCURITÉ
- ANNEXE B À L'ACCORD DE SÉCURITÉ

Le Gouvernement de la République de Lettonie et le Gouvernement du Royaume de Norvège, ci-après dénommés les Parties, souhaitant garantir la protection mutuelle de toutes les informations classifiées, échangées directement ou par l'intermédiaire d'autres organismes publics ou d'entités juridiques privées agissant dans ce cadre en application de la juridiction de chacune des Parties, sont convenus de ce qui suit :

1. APPLICABILITÉ

Le présent Accord fait partie intégrante de tout contrat ou accord impliquant l'échange d'informations classifiées, à conclure ou à signer à l'avenir entre les Parties à propos des sujets suivants :

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

Le présent Accord ne peut être invoqué par l'une des Parties pour obtenir des renseignements classifiés obtenus par l'autre Partie d'une tierce Partie.

Les annexes A et B au présent Accord font partie intégrante dudit Accord.

2. DÉFINITIONS

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

3. PROTECTION DE SÉCURITÉ RÉCIPROQUE

Dans le respect de leurs lois, réglementations et pratiques domestiques, les deux Parties prendront les mesures appropriées pour protéger les renseignements classifiés, qui sont transmis, reçus, produits ou mis au point dans le cadre de tout accord ou de toute relation entre les Parties. Les Parties accorderont à tous les renseignements classifiés qui sont transmis, reçus, produits ou mis au point le même niveau de protection en matière de sécurité que celui qui est accordé à leurs propres renseignements classifiés ayant un niveau de classification équivalent, tel que défini à l'article 5 et à l'annexe A au présent Accord.

L'accès aux renseignements classifiés et aux sites et endroits où des activités classifiées sont réalisées ou dans lesquels des renseignements classifiés sont entreposés sera limité aux personnes qui disposent d'une habilitation en matière de sécurité, telle que définie à l'annexe A au présent Accord, et qui, du fait de leurs attributions ou de leur emploi, ont « besoin de savoir » tel que défini à l'annexe A.

Chaque Partie surveille l'application des lois, réglementations et pratiques en matière de sécurité par les agences, entités et sites au sein de leur juridiction qui détiennent, élaborent, produisent et/ou utilisent les informations classifiées de l'autre Partie, grâce notamment à des visites d'inspection.

4. DIVULGATION D'INFORMATIONS

Les Parties s'abstiendront de communiquer les informations classifiées relevant du présent Accord à des tierces parties ou à des ressortissants de pays tiers sans avoir obtenu au préalable le consentement de la Partie qui a fourni l'information. Les informations classifiées reçues d'une Partie à l'autre Partie seront utilisées uniquement aux fins spécifiées.

Au cas où l'une ou l'autre des Parties et/ou ses organismes ou entités concernés par les sujets visés à l'article premier attribue un contrat appelé à être exécuté sur le territoire de l'autre Partie et qui implique des renseignements classifiés détenus par l'entrepreneur de la Partie réalisant les travaux, la Partie sur le territoire de laquelle l'exécution au titre de l'Accord doit avoir lieu assume la charge de l'administration de ces renseignements classifiés conformément à ses propres normes et prescriptions.

Avant la communication aux contractants ou aux contractants potentiels de l'une des Parties de renseignements classifiés obtenus de l'autre Partie, la Partie réceptrice :

- a) S'assure que ces contractants ou contractants potentiels ainsi que leurs installations sont en mesure de protéger de manière adéquate les renseignements classifiés.
- b) Accorde une habilitation de sécurité appropriée aux contractants concernés.
- c) Accorde une habilitation de sécurité appropriée à tous les membres du personnel dont les fonctions nécessitent l'accès à des renseignements classifiés.

d) Veille à ce que toutes les personnes qui ont accès à des renseignements classifiés soient informées du fait qu'elles sont tenues de protéger les renseignements classifiés conformément aux lois en vigueur.

e) Mène des inspections de sécurité périodiques des installations ainsi habilitées.

5. CLASSIFICATIONS EN MATIÈRE DE SÉCURITÉ

Les informations classifiées seront assorties de l'un des niveaux de classification de sécurité suivants :

LETTONIE	Équivalent	NORVÈGE
SEVIŠĶI SLEPENI	SECRET D'ÉTAT	STRENGT HEMMELIG
SLEPENI	SECRET	HEMMELIG
KONFIDENCIĀLI	CONFIDENTIEL	KONFIDENSIELT
DIENESTA VAJADZĪBĀM	RESTREINT	BEGRENST

La partie réceptrice et/ou ses entités s'abstiendra (s'abstiendront), en ce qui concerne les renseignements classifiés reçus, d'employer un niveau de classification en matière de sécurité inférieur et de déclassifier ces renseignements sans avoir obtenu l'autorisation écrite préalable de la Partie qui a fourni les informations. La Partie qui a fourni les informations informera la partie réceptrice de tout changement apporté à la classification en matière de sécurité des informations échangées.

En outre, la partie réceptrice marquera les renseignements classifiés reçus de son propre niveau de classification en matière de sécurité. Les traductions et les reproductions seront assorties du même niveau de classification en matière de sécurité que l'original, dans les deux langues.

6. AUTORITÉS DE SÉCURITÉ COMPÉTENTES

La partie réceptrice désignera une Autorité de la sécurité dûment autorisée et le notifiera à l'autre Partie; cette autorité, désignée ci-après l'autorité de sécurité compétente, supervisera la mise en œuvre de tout accord, tel que défini à l'article premier du présent accord, à propos de tous les aspects de sécurité.

Les Autorités de sécurité compétentes chargées de la mise en œuvre et de la supervision de tous les aspects du présent Accord sont :

En Lettonie :

Le Bureau de Protection de la Constitution

Miera 85a, Riga, LV-1013

LETTONIE

En Norvège :

L'autorité nationale de sécurité norvégienne

Boîte postale 14

1306 Berum postterminal

NORVÈGE

Chaque Partie s'engage à veiller à ce que les dispositions du présent Accord soient dûment respectées par sa propre Autorité de sécurité compétente.

Les deux Autorités de sécurité compétentes, chacune sur le territoire de son propre État, établissent, distribuent ou supervisent les instructions et les procédures de sécurité pour la protection des renseignements classifiés qui sont échangés en vertu de tout autre accord conclu entre les Parties.

Sur demande, chacune des Autorités de sécurité compétentes fournira des informations à l'autre Autorité de sécurité compétente sur sa propre organisation et ses procédures en matière de sécurité, 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 doivent convenir des dispositions concernant ces visites.

7. VISITES

Les visites dans les secteurs où les informations classifiées sont élaborées, traitées ou stockées ou dans ceux où les projets classifiés sont exécutés, ne sont accordées par l'une des Parties aux visiteurs du pays de l'autre Partie que sur autorisation écrite préalable de l'autorité de sécurité compétente de la Partie qui reçoit ces visiteurs. Cette autorisation ne sera accordée qu'à des personnes qui ont reçu une habilitation de sécurité et qui ont « besoin d'en connaître ».

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 3 (trois) semaines au moins avant la visite prévue, conformément aux procédures définies à l'annexe B du présent Accord.

Chaque Partie veille à ce que les données personnelles des visiteurs soient protégées conformément à la législation nationale en vigueur.

8. CONTRATS

L'autorité de sécurité compétente de l'une des Parties qui souhaite passer un contrat classifié avec un contractant dans le pays de l'autre Partie ou qui souhaite autoriser un de ses propres contractants 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 le contractant envisagé possède une habilitation de sécurité de niveau approprié ainsi que les infrastructures nécessaires pour manipuler et stocker des renseignements classifiés de même niveau. Pour le niveau de sécurité ACCÈS RESTREINT, une garantie de sécurité telle que celle définie à l'annexe A sera fournie.

Tout contrat classifié passé entre des entités des Parties et/ou des organisations privées (comme des entreprises, des centres de recherche, des équipements d'assistance et/ou de service, etc.) comportera une section appropriée relative à la sécurité et une liste de classification de sécurité, conformes aux termes du présent Accord.

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.

Les sous-traitants qui briguent des contrats de sous-traitance classifiés doivent être préalablement soumis pour approbation par le contractant 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 le contractant.

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

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.

9. TRANSFERT DES INFORMATIONS CLASSIFIÉES

Les informations classifiées sont normalement transmises physiquement entre les Parties par les voies diplomatiques respectives.

L'échange d'informations classifiées peut également avoir lieu par l'intermédiaire de représentants officiellement accrédités par les autorités compétentes des deux pays. Cette autorisation pourra, le cas échéant, être également accordée aux représentants d'entreprises industrielles chargées de projets spécifiques.

L'échange de matériel très volumineux ou de grandes quantités d'informations classifiées est mis au point au cas par cas.

D'autres moyens de transmission et d'échange approuvés peuvent être utilisés s'ils sont convenus entre les Autorités de sécurité compétentes.

10. INFRACTION À LA SÉCURITÉ

En cas d'infraction à la sécurité, au sens de la définition figurant à l'annexe A, relative à des renseignements classifiés qui sont émis ou reçus par l'autre Partie, ou lorsque des intérêts communs sont en jeu, l'autorité de sécurité compétente dans le pays de lequel la compromission s'est produite en informera dès que possible l'autorité de sécurité compétente de l'autre pays et procédera à l'enquête qui s'impose. Si elle y est invitée, l'autre Partie coopèrera à cette enquête. Dans tous les cas de figure, l'autre Partie devra être informée des résultats de l'instruction et recevra un rapport final sur les raisons et l'ampleur de l'atteinte à la sécurité.

11. DÉPENSES

Les Parties ne pourront prétendre au remboursement des dépenses qu'elles ont exposées dans le cadre du présent Accord, et notamment relativement à la mise en œuvre des mesures en matière de sécurité.

12. RÈGLEMENT DES DIFFÉRENDS

Tout différend résultant de l'interprétation ou de l'application du présent Accord sera résolu à l'amiable après consultation entre les Parties; les Parties acceptent de ne pas soumettre le règlement de ce litige à des parties tierces, ou à toute juridiction domestique ou internationale.

13. DISPOSITIONS FINALES

Le présent Accord produira ses effets le premier jour qui suit la date de sa signature et restera en vigueur pour une durée indéterminée. Il pourra être résilié à tout moment par l'une des Parties par le biais d'une notification écrite. Dans ce cas, le présent Accord cessera de produire ses effets six (6) mois à compter de la date de réception par l'autre Partie de ladite notification de cessation.

Le présent Accord peut faire l'objet d'une révision, de modifications et d'amendements à tout moment, moyennant l'autorisation écrite préalable des deux Parties.

En cas de dénonciation du présent Accord, les renseignements et/ou les informations classifiés transmis en vertu du présent Accord seront restitués dès que possible à l'autre Partie. Le matériel et/ou les informations classifié(s) qui ne sont pas renvoyés seront protégés conformément aux dispositions stipulées dans le présent Accord.

Fait à Kongsvinger, Norvège, le 26 août 2005 en double exemplaire en langues lettone, norvégienne et anglaise, tous les textes faisant également foi. En cas de divergences d'interprétation des dispositions du présent Accord, le texte en anglais prévaudra.

Pour le Gouvernement de la République de Lettonie :

EINARS REPŠE
Ministre de la défense

Pour le Gouvernement du Royaume de Norvège :

KRISTIN KROHN DEVOID
Ministre de la défense

ANNEXE A À L'ACCORD DE SÉCURITÉ

DÉFINITIONS

Aux fins du présent Accord :

- On entend par renseignements classifiés

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 qui en est donnée à l'alinéa b) ci-dessous;

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

c) Le terme « document » s'entend de toute forme de renseignement consigné, quel que soit le type de média utilisé pour sa consignation.

- Le terme « contrat » désigne

Un accord entre deux parties ou plus qui crée et définit des droits et des obligations exécutoires entre les parties.

- L'expression « contrat classifié » s'entend d'un contrat qui contient ou traite des renseignements classifiés.

- Le terme « contractant » désigne

Une personne physique ou morale dotée de la capacité juridique de conclure des contrats.

- 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 renseignements classifiés.

- L'expression « violation de la sécurité » désigne

Une violation de renseignements classifiés due au fait que la connaissance de ces renseignements a été transmise ou risque d'être transmise en totalité ou en partie à des personnes physiques, des personnes morales ou des pays non autorisé(e)s ou habilité(e)s à y avoir accès.

- 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 renseignements classifiés

à un niveau donné et à manier ceux-ci conformément aux règlements nationaux de sécurité concernés.

- L'expression « garantie de sécurité » s'entend

D'une déclaration, faite par l'autorité compétente en matière de sécurité, selon laquelle des renseignements classifiés à niveau d'accès restreint seront protégés conformément à ses règlements nationaux.

- L'expression « besoins d'en connaître » signifie

Que l'accès à des renseignements classifiés ne peut être accordé que sous réserve de vérification de la nécessité, pour le demandeur, d'en prendre connaissance en raison de ses fonctions officielles dans le cadre desquelles les renseignements ont été communiqués à la Partie réceptrice.

- Classifications et usage en matière de sécurité :

À appliquer à des informations dont la divulgation non autorisée aurait les conséquences suivantes pour les intérêts de l'État concerné :

LETTONIE

NORVÈGE

SEVIŠĶI SLEPENI

STRENGT HEMMELIG

exceptionnellement grave

SLEPENI

HEMMELIG

préjudice grave

KONFIDENCIALI

KONFIDENSIELT

dommageable

DIENESTA VAJADZIBAM

BEGRENST

indésirable

ANNEXE B À L'ACCORD DE SÉCURITÉ

VISITES PAR DES MEMBRES DU PERSONNEL D'UNE PARTIE D'ÉTABLISSEMENTS, SITES, ETC.,
DE L'AUTRE PARTIE

L'accès aux renseignements classifiés et aux établissements, infrastructures, etc., où sont réalisées des activités classifiées ou dans lesquels sont stockés ou manipulés ces renseignements classifiés 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 par une autre autorité publique compétente du pays qui les envoie et sont habilités à recevoir des renseignements classifiés conformément aux réglementations nationales du pays d'accueil, et/ou

b) Sont autorisés par l'autorité de sécurité compétente ou par une autre autorité publique compétente à effectuer la visite ou les visites demandées.

L'autorité de sécurité compétente de la Partie demandeuse notifie à l'autorité de sécurité compétente de la Partie du pays à visiter la visite planifiée conformément aux dispositions de la présente annexe et s'assure que cette dernière reçoive cette demande de visite trois (3) semaines au moins avant la (les) visite(s) prévue(s).

La demande de visite comporte :

a) Le prénom, le nom, le lieu et la date de naissance, la nationalité et l'employeur, le passeport ou autres documents d'identité du visiteur.

b) L'attestation de l'habilitation de sécurité du visiteur par rapport à l'objet de la visite.

c) L'objet et le but de la visite ou des visites (Ces indications doivent être précises et suffisamment détaillées. Il convient d'éviter les indications générales et les abréviations).

d) La date et la durée prévues de la visite ou des visites demandées.

e.) Le point de contact dans rétablissement/l'infrastructure à visiter, les contacts antérieurs et toute autre information utile pour déterminer le caractère justifié de la visite ou des visites.

La demande sera introduite :

a) Par l'intermédiaire de l'ambassade de Norvège à Riga pour les demandes de visite de citoyens norvégiens en Lettonie.

b) Par l'intermédiaire de l'ambassade de Lettonie à Oslo pour les demandes de visite de citoyens lettons en Norvège.

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'excèdera pas douze (12) mois.

Les renseignements classifiés échangés au cours de la visite bénéficieront du même niveau de protection et de classification que ceux de la Partie émettrice.

