No. 38510

Hungary
and
Norway

Agreement on the protection of defence relatcd classified information hetween the Governments of the Repnblic of Hungary and the Kingdom of Norway. Oslo, 12 Octoher 1999

Entry into force: *5 May 2000, in accordance with article 13*

Authentic texts: *English, Hungarian and Norwegian*

Registration with the Secretariat of the United Nations: *Hungary, 19 June 2002*

Hongrie
et
Norvège

Accord relatif à la protection des renseignements classifiés en matière de défense entre les Gouvernements de la République de Hongrie et du Royaume de Norvège. Oslo, 12 octobre 1999

Entrée en vigueur : *5 mai 2000, conformément à l'article 13*

Textes authentiques : *anglais, hongrois et norvégien*

Enregistrement auprès du Secrétariat des Nations Unies : *Hongrie, 19 juin 2002*

[ENGLISH TEXT — TEXTE ANGLAIS]

AGREEMENT ON THE PROTECTION OF DEFENCE RELATED CLASSIFIED INFORMATION BETWEEN THE GOVERNMENTS OF THE REPUBLIC OF HUNGARYAND THE KINGDOM OF NORWAY

The Governments of the Republic of Hungary and the Kingdom of Norway (hereinafter referred to as Parties), driven by their intent to protect classified military information (hereinafter referred to as classified information), exchanged directly or through other administrative entities or private organisations who deal with classified information under jurisdiction of the Ministries of Defence of the Parties, setting the objective of establishing conditions of security hereby agree on the following:

Article 1. Applicability

(1) This Agreement shall form an integral part of any contract which will be made or signed in the future between the Parties concerning the following subjects:

a) Co-operation between the two Parties concerning national defence and military issues;

b) Co-operation, exchange of information, joint ventures, contracts or any other relations between entities and/or private companies of the Parties concerning national defence, and military security issues;

c) Sale of equipment and know-how relating to defence, by one Party to the other;

d) Information transferred between the Parties by any representative, employee or consultant (private or otherwise) concerning national defence, security and military issues.

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

Article 2. Definitions

For the purposes of the present Agreement the terms mentioned below shall be interpreted as following:

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) the term "material" includes "documents" 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.

2) Originating Party shall be all individuals or legal entities from whom the classified information originates.

3) Receiving Party shall be all individuals or legal entities who receive the classified information from the transferring Party.

4) Agency shall be all private or public institutions which are under the supervision of the Competent Security Authorities of the Parties which handle, safeguard or store classified information.

5) Third Party shall be all governments which have not been designated as parties for the purpose of the present Agreement, as well as those individuals or legal entities which are not individuals or legal entities of the Parties.

6) Contract means an agreement between two or more parties creating and defining enforceable rights and obligations between the parties.

7) Classified contract means a contract which contains or involves classified information.

8) Contractor means an individual or a legal entity possessing the legal capability to undertake contracts.

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

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

11) 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 in accordance with the respective national security regulations.

12) 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.

13) "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.

Article 3. Mutual conformity of classified information

(1) Obligations undertaken by the Parties within the scope of this Agreement shall be treated in accordance with the relevant domestic legislation of the given country.

(2) The Parties, having been mutually familiarised with the security measures set forth in their respective domestic legislation, hereby decide that for the purposes of implementing the present Agreement the following classifications shall be used

Hungarian

"Szigorúan Titkos!"

"Titkos!"

"Bizalmas!"

"Korlátozott Terjesztésû!"

English

Top Secret

Secret

Confidential

Restricted

Norwegian

Strengt Hemmelig

Hemmelig

Konfidensielt

Begrenset

(3) Both Parties undertake to mark classified information received from the other Party with relevant domestic classification as set forth in paragraph (2) of this Article.

(4) Both Parties shall undertake to mutually inform each other of any modification of the order of classification or any changes in the formal method of designation.

(5) Only the originating Party shall be authorised to modify or annul the level of classification of its classified information. The receiving Party shall be informed of any modification or annulment of the level of classification in writing.

(6) The level of classification designated by the originating Party shall appear on any copies made of classified information.

Article 4. Obligations of the Parties

(1) Both Parties shall be responsible from the moment of transfer of the received classified information.

(2) 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.

(3) Classified information exchanged by the Parties can only be used in accordance with the provisions of the present Agreement. Information originating from one Party may not be passed on to any third party without the prior written consent of the originating Party.

(4) Information resulting from joint activities shall not be transferable to third parties without the prior written consent of both Parties.

(5) 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 Article 2, and who, due to their functions or employment, have a "need to know", as defined in Article 2.

(6) Both Parties undertake to inform agencies under their supervision about the entry into force of this Agreement, the moment their activities pertain to such classified information.

(7) Both Parties oblige themselves to assure that all agencies under their supervision adhere strictly to the provisions of the present Agreement.

(8) The present Agreement shall govern all agreements between the Parties and agencies subordinated to them, signed or yet unsigned, pertaining to the exchange of classified information.

(9) In the event that either Party and/or its agencies or entities concerned with subjects set out in Article 1, award a contract for performance within the territory of the other Party, and such contract involves classified information, 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.

(10) 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) Ensure that an appropriate facility security clearance to the relevant contractors is granted.

c) Ensure that an appropriate personnel security clearance for all personnel whose duties require access to the classified information is granted.

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.

Article 5. Competent Security Authorities

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

- from the part of the Republic of Hungary : Ministry of Defence

1885 Budapest

Pf. 25

Hungary

- from the part of the Kingdom of Norway: Headquarters Defence Command

Norway

Security Division

Postboks 14

1306 Baerum Postterminal

Norway

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

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

Article 6. Consultation

In order to provide for the enforcement of equivalent levels of security rules both Parties shall inform one another of their own security regulations, procedures and practices, any changes in the legislative background pertaining to the protection of classified information and shall be obliged to facilitate contact between the Competent Security Authorities of the Parties.

Article 7. Transmission of classified information

(1) Classified information shall be forwarded by way of diplomatic channels, or by way of a person enjoying similar privileges and immunities as set forth in international law.

(2) Exchange of classified information -- restricted and confidential -- can also take place through representatives officially appointed by the authorities in both states. Such authorisation may, when required be given to the representatives of private undertakings engaged in specific military 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 each Competent Security Authority.

(5) The receiving Party shall duly notify the originating Party of the receipt of classified information.

Article 8. Visits

(1) Visits to premises where classified information is developed. handled or stored, or where classified military projects are carried out, will only be granted by one Party to visitors from the country of the other Party provided 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".

(2) Access to classified information and to establishments and facilities etc. where classified information is stored or handled, shall be allowed by one Party to visitors of the other Party only if they had 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 rcquested visit or visits.

(3) 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 provisions laid down in this Article.

(4) 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.

(5) The request will be submitted:

a) Through the Norwegian Embassy in Budapest for visit requests of Norwegian citizens in Hungary.

b) Through the Hungarian Embassy in Oslo for visit requests of Hungarian citizens in Norway.

c) Other procedures may be used if agreed upon by the two Competent Security Authorities.

(6) The validity of visit authorisations shall not exceed twelve -- 12 -- months.

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

Article 9. Contracts

(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 military project, shall obtain a prior written assurance via 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 Article 2, will be provided.

(2) Every contract between entities of the Parties and/or private organisations 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) Subcontractors interested in classified subcontracts, shall be submitted in advance by tbe contractor to the Competent Security Authority for approval. If approved, the subcontractor must fulfil the same security obligations as have been set for the contractor.

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

(6) 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.

Article 10. Breach of security

In case of a breach of security, as defined in Article 2, of information classified Confidential or above, that results in a security compromise, as defined in Article 2, originating 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 shall be informed of the results of the investigations and receive a final statement as to the reasons and extent of the security violation.

Article 11. Expenses incurred

Both Parties shall themselves bear the costs incurred during the implementation of the Agreement and its provisions.

Article 12. Settlement of disputes

(1) Both Parties shall settle all disputes arising during the interpretation or implementation of the present Agreement by negotiation and shall not turn to third parties or an international court.

(2) During the period of such dispute both Parties shall continue to fulfil all obligations stemming from the present Agreement.

Article 13. Closing provisions

(1) The present Agreement shall enter into force 60 days after both Parties have signed the Agreement and notified each other through diplomatic channels of the fact that they have taken the steps necessary domestically for enforcement.

(2) The present Agreement shall be valid for an unlimited duration. Any of the Parties can cancel the Agreement by written notice sent to the other Party. Cancellation shall be effective six months after the receipt of such written notice. In the case of the present Agreement being annulled, classified information transmitted under the terms of this Agreement, shall be returned to the other Party as soon as possible. Classified information

that is not returned, shall be protected in accordance with the provisions laid down in this Agreement.

(3) The present Agreement may be amended by mutual consent of both Parties. Amendments shall be reconciled through diplomatic channels in writing and shall come into force in accordance with the provisions of paragraph (1) of this Article.

Prepared in two original copies on 12 October 1999 in Oslo in the Hungarian, Norwegian and English languages all texts being equally authentic. In case of a discrepancy between the Norwegian and the Hungarian text, the English text shall prevail.

On behalf of the Government of the Republic of Hungary:

JÁNOS SZABÓ

On behalf of the Government of the Kingdom of Norway:

ELBGUNY LØWER

[HUNGARIAN TEXT — TEXTE HONGROIS]

EGYEZMÉNY

A MAGYAR KÖZTÁRSASÁG KORMÁNYA

ÉS

A NORVÉG KIRÁLYSÁG KORMÁNYA

KÖZÖTT

A MINŐSÍTETT KATONAI INFORMÁCIÓK

VÉDELMÉRŐL

A Magyar Köztársaság Kormánya, valamint a Norvég Királyság Kormánya (továbbiakban: Felek), azon szándékuktól vezérelve, hogy védjék azon minősített katonai információkat (továbbiakban: minősített információk), melyeket közvetlenül, vagy olyan más közfeladatot ellátó szerveken vagy magán szervezeteken keresztül cserélnek ki, amelyek a Felek honvédelmi minisztériumai fennhatósága alatt foglalkoznak a minősített információkkal, kitűzve a biztonsági feltételek létrehozásának célját, az alábbiakban állapodnak meg:

1. Cikk
Alkalmazhatóság

(1) Ezen Egyezmény szerves részét képezi bármely szerződésnek, melyet a jövőben a Felek kötnek vagy aláírnak a következő témákat érintve

a) a két fél közötti együttműködés a honvédelemre és a katonai kérdésekre vonatkozóan,

b) együttműködés, információcsere, közös tevékenységek, szerződések vagy bármilyen más kapcsolat a Felek szervezetei és vagy magán vállalatai között a honvédelemre és a katonai biztonsági kérdésekre vonatkozóan,

c) a védelemhez kapcsolódó felszerelések és know-how eladása az egyik Fél által a másik számára,

d) bármely képviselő, alkalmazott vagy tanácsadó (magát vagy más) által a Felek között átadott információk a honvédelemre, biztonságra és katonai kérdésekre vonatkozóan.

(2) Jelen Egyezményt egyik Fél sem használhatja fel olyan minősített információk megszerzésére, melyet a másik Fél egy harmadik Féltől szerzett be.

2. Cikk
Meghatározások

A jelen Egyezmény szempontjából az alábbiakban szereplő kifejezéseket a következőképpen kell értelmezni:

(1) Minősített információ:

a/ bármely minősített adathordozó, legyen az minősített tartalmú szóbeli közlés, illetve egy minősített üzenet elektronikus úton történő átadása, vagy az alábbi (b) pontban meghatározott "anyag";

b/ az "anyag" kifejezés magában foglalja a (c) pontban meghatározott "dokumentumot", illetve bármely már legyártott vagy még a gyártás folyamatában lévő gépészeti cikket, felszerelést, fegyvert vagy fegyverrendszert;

c/ a "dokumentum" kifejezés a rögzített információ bármely formáját jelenti, tekintet nélkül a rögzítő eszköz típusára.

(2) Átadó Fél: az összes természetes vagy jogi személy, akitől a minősített információ származik.

(3) Fogadó Fél: az összes természetes vagy jogi személy, aki minősített információt kap az átadó Féltől.

(4) Intézmény: az összes magán vagy közintézmény, mely a Felek illetékes biztonsági hatóságainak felügyelete alá tartoznak és minősített információkat kezelnek, őriznek vagy tárolnak.

(5) Harmadik Fél: mindazon kormányok, melyek a jelen Egyezmény szempontjából nem Felek, valamint azok a természetes vagy jogi személyek, akik egyik Félnek sem természetes vagy jogi személyei.

(6) Szerződés: megállapodás két vagy több fél között, amely kikényszeríthető jogokat és kötelezettségeket hoz létre és határoz meg a felek között.

(7) Minősített szerződés: olyan szerződés, mely minősített információt tartalmaz vagy von maga után.

(8) Szerződő: azon természetes vagy jogi személy, akinek törvényes lehetősége van a szerződés megkötésére.

(9) Biztonság megsértése: olyan tett vagy mulasztás, amely ellentétes a nemzeti biztonsági szabályokkal, illetve amely eredménye sértheti vagy veszélyeztetheti a minősített információkat.

(10) Biztonság veszélyeztetése: azt jelenti, hogy a minősített információt veszélyeztetik, mivel annak ismerete részben vagy teljes mértékben olyan természetes vagy jogi személyek birtokába került, akik nem rendelkeztek az ilyen hozzáféréshez szükséges megfelelő biztonsági engedéllyel vagy jogkörrel, vagy amikor az ilyen hozzáférés kockázata fennáll.

(11) Biztonsági engedély: egy vizsgálati eljárást követő pozitív határozat arról, hogy a természetes vagy jogi személy a vonatkozó nemzeti biztonsági szabályok értelmében minősített információt kezelhet vagy ahhoz hozzáférhet.

(12) Biztonsági garancia: az illetékes biztonsági hatóság által kiadott nyilatkozat, amely tanúsítja, hogy a minősített információ korlátozott terjesztésű szinten részesül védelemben a nemzeti szabályok értelmében.

(13) "Csak akire tartozik" elve: azt jelenti, hogy a minősített információkhoz való hozzáférés csak akkor garantálható, ha a hozzáférést kérő személynek azon keretek között ahogy az információt a fogadó Félnek kiadták, hivatalos munkakörével összefüggésben, igazoltan ismernie kell az adott információt.

3. Cikk
A minősített információk kölcsönös megfeleltetése

(1) A Felek által a jelen Egyezményben vállalt kötelezettségek az adott ország vonatkozó belső jogszabályaival összhangban valósulnak meg.

(2) A Felek, miután kölcsönösen megismerték egymás belső jogszabályaiban szereplő biztonsági intézkedéseket, elhatározzák, hogy a jelen Egyezmény alkalmazásakor a következő jelöléseket használják:

Magyar	Angol	Norvég
„Szigorúan titkos!"	Top secret	Strengt Hemmelig
„Titkos!"	Secret	Hemmelig
„Bizalmas!"	Confidential	Konfidensielt
„Korlátozott terjesztésű!"	Restricted	Begrenset

(3) Mindkét Fél vállalja, hogy a másik Féltől származó minősített információk átvételekor azokat ellátja saját, ezen cikk (2) bekezdésében meghatározott nemzeti minősítési megjelöléssel

(4) Mindkét Fél vállalja, hogy kölcsönösen tájékoztatják egymást minden - a minősítési rendben vagy a jelölés formális módszereiben bekövetkezett - változásról.

(5) A minősített információk minősítésének módosítására vagy megszüntetésére csak az eredeti minősítést végző Fél jogosult. A minősítés módosításának vagy megszüntetésének szándékáról a másik Felet írásban értesíteni kell.

(6) A minősített információk bármilyen jellegű másolásánál fel kell tüntetni az átadó Fél által megkívánt minősítési fokozatot

4. Cikk
A Felek kötelezettségei

(1) Mindkét Fél a minősített információkért azok átvételétől számítva felel

(2) Nemzeti jogszabályaikkal, szabályzataikkal és gyakorlatukkal összhangban, mindkét Fél megfelelő intézkedéseket foganatosít azon minősített információk megvédésére, amelyeket a Felek közötti bármely egyezmény vagy kapcsolat keretében adtak át, kaptak, állítottak elő vagy dolgoztak ki

(3) A Felek által kicserélt minősített információkat csak a jelen Egyezmény intézkedéseivel összhangban lehet felhasználni. Az egyik Féltől származó információt az átadó Fél előzetes írásos jóváhagyása nélkül nem lehet továbbadni harmadik fél részére.

(4) A közös tevékenységből származó minősített információk nem adhatók át harmadik félnek mindkét Fél előzetes írásbeli beleegyezése nélkül.

(5) A minősített információkhoz vagy olyan helyekhez és létesítményekhez való hozzáférés, ahol minősített tevékenységeket folytatnak, illetve ahol minősített információt tárolnak, azon személyekre korlátozódik, akik megkapták a 2. Cikkben meghatározott biztonsági engedélyt, illetve akiknek funkciója vagy beosztása szükségessé teszi ezt, vagyis ha a 2. Cikkben meghatározott „csak akire tartozik" elv szerint ismernie kell azt.

(6) Mindkét Fél vállalja, hogy a felügyelete alá tartozó intézmények tudomására hozza a Felek között aláírt jelen Egyezmény létezését, mihelyt azok tevékenysége minősített információkat érint.

(7) Mindkét Fél kötelezi magát, hogy a felügyelete alá tartozó összes intézmény szigorúan betartja a jelen Egyezményben foglaltakat.

(8) Jelen Egyezmény hatálya kiterjed minden a Felek között, illetve a Felekkel kapcsolatban álló intézmények között aláírt vagy aláírandó a minősített információk cseréjével, illetve átadásával kapcsolatos szerződésre.

(9) Abban az esetben, ha az egyik Fél és/vagy annak intézményei vagy személyei, akik az 1. Cikkben felsorolt témákkal foglalkoznak, és a másik Fél területén belül teljesítendő szerződést kötnek, és az ilyen szerződés minősített információkkal jár együtt, akkor azon Fél, melynek országában az Egyezmény értelmében sor kerül a teljesítésre, felelősséget vállal az ilyen minősített információk saját szabványaikkal és követelményeikkel összhangban történő kezelésére.

(10) Mielőtt bármilyen, a másik Féltől kapott minősített információt kiadnának valamelyik Fél vállalkozóinak vagy leendő vállalkozóinak, a fogadó Fél

a/ biztosítja, hogy az ilyen vállalkozók vagy leendő vállalkozók és létesítményeik rendelkeznek azon képességgel, hogy kielégítően megvédik a minősített információt;

b/ biztosítja, hogy az adott vállalkozók megkapják a megfelelő biztonsági engedélyt;

c/ biztosítja, hogy a teljes állomány, amelynek feladata szükségessé teszi a minősített információhoz való hozzáférést, megkapja a megfelelő személyi biztonsági engedélyt;

d/ biztosítja, hogy az összes olyan személy, aki hozzáférhet a minősített információkhoz, tájékoztatva lesz azon felelősségéről, amely szerint a vonatkozó jogszabályokkal összhangban meg kell védenie a minősített információkat.

5. Cikk
Az illetékes biztonsági hatóságok

(1) A jelen Egyezmény valamennyi rendelkezésének végrehajtásáért és felügyeletéért felelős illetékes biztonsági hatóságok a következők:

- a Magyar Köztársaság részéről: Honvédelmi Minisztérium
1885 Budapest
Postafiók 25
Magyarország.

- a Norvég Királyság részéről: Védelmi Parancsnokság
Biztonsági Osztály
Postafiók 14
1306 Baerum Postterminal
Norvégia

(2) Mindkét Fél vállalja annak biztosítását, hogy az illetékes biztonsági hatóság ezen Egyezmény intézkedéseit kellőképpen figyelemmel kíséri.

(3) Mindkét illetékes biztonsági hatóság, a saját államának joghatóságán belül előkészíti, elosztja vagy felügyeli azon minősített információk védelmével kapcsolatos biztonsági utasításokat és eljárásokat, amelyeket a Felek közötti bármely egyezmény eredményeként cseréltek ki.

6. Cikk
Konzultáció

Annak érdekében, hogy azonos szintű biztonsági szabályokat használjanak és tarthassanak fenn, mindkét Fél köteles tájékoztatni a másik Felet saját biztonsági szabályairól, eljárásairól és gyakorlatáról, illetve a minősített információk védelmére vonatkozó jogszabályi háttér változásáról és köteles e célból elősegíteni a Felek illetékes biztonsági hatóságai közötti kapcsolatfelvételt.

7. Cikk
A minősített információk átadása

(1) A minősített információk továbbítása diplomáciai csatornákon keresztül, valamint a nemzetközi jog alapján velük azonos kiváltságokat és mentességeket élvező személy útján történik.

(2) A korlátozott terjesztésű és bizalmas minősített információk kicserélésére a biztonsági hatóságok által hivatalosan kinevezett képviselőkön keresztül is sor kerülhet mindkét államban. Ilyen felhatalmazást - ha szükséges - a sajátos katonai projektekkel foglalkozó magánvállalkozások képviselői is kaphatnak.

(3) Minősített információk nagy tételben vagy mennyiségben történő átadását illetve szállítását esetenként állapítják meg.

(4) Az átadás vagy kicserélés más jóváhagyott eszközeit is használhatják, ha mindegyik illetékes biztonsági hatóság egyetért azzal.

(5) A fogadó Fél köteles megfelelő módon visszajelezni az átadó Félnek a kapott minősített információk megérkezését.

8. Cikk
Látogatások

(1) Olyan épületekbe tett látogatásokat, ahol minősített információt dolgoznak ki, kezelnek vagy tárolnak, illetve ahol minősített katonai projekteket valósítanak meg, a Felek csak akkor teszik lehetővé a másik Fél látogatói számára, ha előzetes írásos engedélyt kaptak a fogadó Fél illetékes biztonsági hatóságától. Az ilyen engedélyt a „csak akire tartozik" elv alapján azon személyeknek adják meg, akiknek a biztonsági ellenőrzése megtörtént.

(2) Hozzáférést olyan minősített információkhoz valamint olyan épületekhez illetve létesítményekhez, stb., ahol minősített információkat tárolnak vagy kezelnek, az egyik Fél csak akkor engedélyezi a másik Fél látogatói számára, ha azokat már:

a/ a küldő ország illetékes biztonsági hatósága vagy más illetékes kormányszerve ellenőrizte, illetve felhatalmazták őket a minősített információknak a fogadó ország nemzeti szabályzataival összhangban történő átvételére, és/vagy

b/ az adott ország illetékes biztonsági hatósága vagy más illetékes kormányszerve engedélyezte részükre a kért látogatás vagy látogatások teljesítését.

(3) A küldő Fél illetékes biztonsági hatósága, a várt látogatókkal kapcsolatosan legalább három (3) héttel a tervezett látogatás előtt az ezen Cikkben lefektetett intézkedéseknek megfelelően, visszajelez a fogadó Fél illetékes biztonsági hatóságának.

(4) A látogatási kérelem a következőket tartalmazza:

a/ a látogató vezetékneve, keresztneve, születésének helye és ideje, állampolgársága, munkaadója, útlevele vagy más azonosító dokumentuma;

b/ a látogató biztonsági engedélyét a látogatás céljának megfelelően,

c/ a látogatás vagy látogatások tárgya és célja (az utalásoknak pontosnak és kielégítően részletesnek kell lenniük, az általános utalásokat és rövidítéseket kerülni kell).

d/ a kért látogatás vagy látogatások várható időpontja és időtartama;

e/ az összekötő személy a meglátogatandó létesítménynél, korábbi kapcsolatok, illetve bármely információ, mely fontos lehet a látogatás vagy látogatások indokoltságának meghatározásához.

(5) A kérést a következőképpen nyújtják be:

a/ a norvég állampolgárok magyarországi látogatási kérelmeit a budapesti Norvég Nagykövetségen keresztül;

b/ a magyar állampolgárok norvégiai látogatási kérelmeit az oslo-i Magyar Nagykövetségen keresztül,

c/ másfajta eljárásokra is sor kerülhet, ha a két illetékes biztonsági hatóság megállapodik a dologról.

(6) A látogatási engedélyek érvényesség nem lépi túl a tizenkét (12) hónapot

(7) A látogatás során kicserélt minősített információkat ugyanolyan fokú védelemmel és minősítési szinttel látják el, mint az átadó Felét

9. Cikk
Szerződések

(1) Azon Fél illetékes biztonsági hatósága, mely minősített szerződést kíván kötni egy vállalkozóval a másik Fél országában, illetve engedélyezni kívánja egyik saját vállalkozója számára minősített szerződés kötését a másik Fél országában egy minősített katonai projekt keretében, előzetes írásos biztosítékot kell kapjon a másik Fél illetékes biztonsági hatóságán keresztül arról, hogy a javasolt vállalkozó rendelkezik a megfelelő szintű biztonsági engedéllyel, illetve olyan létesítményekkel, ahol a minősített információkat ugyanazon szinten tudja kezelni és tárolni. A korlátozott terjesztésű szinthez a 2. Cikkben meghatározott biztonsági garanciát adnak.

(2) A Felek és/vagy magán szervezetek személyei közötti minden szerződés megfelelő biztonsági részt és biztonsági minősítési listát tartalmaz, mely ezen Egyezmény feltételein alapszik

(3) Azon illetékes biztonsági hatóság, amely országában a munka elvégzésre kerül, vállalja a felelősséget a szerződésre vonatkozó biztonsági intézkedések meghozatalára és adminisztrálására ugyanazon szabványok és követelmények alapján, amelyeket a saját minősített szerződéseik védelmével kapcsolatban alkalmaznak.

(4) A vállalkozó jóváhagyás végett már előre benyújtja a minősített alvállalkozói szerződésekben érdekelt alvállalkozók névsorát az illetékes biztonsági hatóságnak. Jóváhagyás esetén az alvállalkozónak ugyanazon biztonsági kötelezettségeknek kell eleget tenniük, mint a vállalkozónak

(5) Bármely minősített katonai projekt, egyezmény, szerződés vagy alvállalkozói szerződés bejelentését előre továbbítják azon ország illetékes biztonsági hatóságának, ahol a projekt megvalósításra kerül

(6) Bármely minősített szerződés biztonsági részének két (2) példányát továbbítják azon ország illetékes biztonsági hatóságának, ahol a projekt megvalósításra kerül

10. Cikk
A titoksértés

A másik Fél által átadott vagy kapott, vagy közös érdekeket érintő bizalmas vagy magasabb szintű minősített információ 2. Cikkben meghatározott megsértése esetén, amely a biztonság 2. Cikkben meghatározott veszélyeztetését eredményezi, azon ország illetékes biztonsági hatósága, ahol a biztonság megsérült, a lehető leghamarabb tájékoztatja a másik ország illetékes biztonsági hatóságát, és lefolytatja a megfelelő vizsgálatot. A másik Fél, - kérés esetén - együttműködik a vizsgálatban. Bármely más esetben tájékoztatni kell a másik Felet a vizsgálatok eredményeiről, és végső nyilatkozatot kell kiállítani az okokról és a biztonság megszegésének mértékéről

11. Cikk
A költségek

Mindkét Fél saját maga viseli a jelen Egyezmény végrehajtásával és annak rendelkezéseivel kapcsolatban felmerülő költségeket.

12. Cikk
A viták rendezése

(1) Mindkét Fél képviselői tárgyalásos úton rendezik a jelen Egyezményben foglaltak értelmezése vagy végrehajtása kapcsán felmerült összes vitát, és nem fordulnak sem harmadik félhez, sem nemzetközi bírósághoz.

(2) E vita időtartalma alatt mindkét Fél továbbra is betartja a jelen Egyezményből fakadó kötelezettségeit.

13. Cikk
Záró rendelkezések

(1) Jelen Egyezmény 60 nappal az után lép hatályba, hogy a Felek diplomáciai úton írásban értesítik egymást arról, hogy eleget tettek a hatályba lépéshez szükséges belső jogi követelményeiknek.

(2) A Felek jelen Egyezményt határozatlan időre kötik. Jelen Egyezményt bármelyik Fél felmondhatja a másik Félnek küldött írásos értesítéssel. A felmondás az értesítés kézhezvételétől számított hat hónap elteltével hatályosul. Jelen Egyezmény megszűnése esetén, a jelen Egyezmény alapján már átadott minősített információkat, amilyen hamar csak lehet visszaküldik a másik Fél részére. Azon minősített információkat, melyeket nem küldtek vissza, továbbra is a jelen Egyezményben foglalt intézkedések szerint kell védeni.

(3) A jelen Egyezmény a Felek kölcsönös egyetértésével módosítható. A módosításokat diplomáciai úton írásban kell javasolni, és azok ezen Cikk (1) bekezdésében foglaltaknak megfelelően lépnek hatályba.

Készült 1999 október 12. é-n, Oslóban -n, két eredeti példányban magyar, norvég és angol nyelven, valamennyi példány egyaránt hiteles. A magyar és a norvég szöveg közötti ellentmondás esetén az angol nyelvű szöveg a mérvadó.

a Magyar Köztársaság Kormánya részéről

a Norvég Királyság Kormánya részéről

[NORWEGIAN TEXT — TEXTE NORVÉGIEN]

AVTALE

OM BESKYTTELSE AV FORSVARSRELATERTE GRADERTE OPPLYSNINGER

MELLOM REGJERINGENE I

REPUBLIKKEN UNGARN

OG

KONGERIKET NORGE

Regjeringene i Republikken Ungarn og Kongeriket Norge (heretter kalt partene) har – ut fra et sterkt ønske om å sikre beskyttelse av graderte militære opplysninger (heretter benevnt graderte opplysninger) som utveksles direkte eller gjennom andre administrative enheter eller private organisasjoner som handterer graderte opplysninger, og som står under jurisdiksjonen til partenes respektive forsvarsministerier – inngått følgende avtale:

Artikkel 1
Virkeområde

1 Denne avtale skal utgjøre en integrerende del av enhver kontrakt som måtte inngås eller undertegnes mellom partene på følgende områder:

a) samarbeid mellom de to partene om nasjonale forsvarsrelaterte og militære spørsmål,

b) samarbeid, utveksling av opplysninger, fellesforetak, kontrakter eller andre forbindelser mellom enheter og eller private selskaper hos partene som gjelder nasjonale forsvarsrelaterte, og militære sikkerhetsrelaterte spørsmål,

c) salg av forsvarsrelatert utstyr og ekspertise fra den ene part til den annen,

d) opplysninger som overføres mellom partene av representanter, ansatte eller konsulenter (private eller annet), og som gjelder nasjonale forsvarsrelaterte, sikkerhetsrelaterte og militære spørsmål.

2 Ingen av partene kan påberope seg denne avtale for å få hånd om graderte opplysninger som den annen part har mottatt fra tredjemann.

Artikkel 2
Definisjoner

I denne avtalen forstås med:

1) Graderte opplysninger:

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

b) begrepet "materiell" omfatter "dokument" som definert under c), samt maskineri, utstyr, våpen eller våpensystemer, eller deler av slikt, som er produsert eller er under produksjon.

c) begrepet "dokument" betyr enhver form for registrerte opplysninger, uansett type registreringsmedium.

2) Utstedende part

Enhver fysisk eller juridisk person som de graderte opplysningene stammer fra.

3) Mottakende part

Enhver fysisk eller juridisk person som mottar de graderte opplysningene fra den oversendende part

4) Organ

Enhver privat eller offentlig institusjon som står under tilsyn av partenes respektive nasjonale sikkerhetsmyndigheter, og som håndterer, beskytter eller lagrer graderte opplysninger

5) Tredjemann

Enhver regjering som ikke er utpekt som part for denne avtalens formål, samt enhver fysisk eller juridisk person som ikke er fysiske eller juridiske personer hos partene

6) Kontrakt

En avtale mellom to eller flere parter som inneholder og fastsetter rettskraftige rettigheter og plikter mellom partene

7) Gradert kontrakt

En kontrakt som inneholder eller omfatter graderte opplysninger

8) Leverandør

En fysisk eller juridisk person som har kontraktshabilitet

9) Sikkerhetsbrudd

En handling eller en unnlatelse som er i strid med nasjonale sikkerhetsbestemmelser, og som kan medføre at graderte opplysninger settes i fare eller kompromitteres

10) Sikkerhetskompromittering

At graderte opplysninger blir kompromittert ved at kunnskapen om dem helt eller delvis er eller har stått i fare for å bli brakt videre til personer eller enheter uten hensiktsmessig sikkerhetsklarering eller autorisasjon til slik tilgang

11) Sikkerhetsklarering

En positiv beslutning vedrørende en person eller enhet, som følge av en undersøkelse med sikte på å fastslå om vedkommende person eller enhet er skikket til å ha tilgang til og håndtere graderte opplysninger i samsvar med de respektive nasjonale sikkerhetsbestemmelser.

12) Sikkerhetsforsikring

En erklæring utstedt av den nasjonale sikkerhetsmyndighet som forsikrer at opplysninger sikkerhetsgradert begrenset vil bli beskyttet i samsvar med nasjonale bestemmelser.

13) "Behov for innsyn" ("Need to know")

At tilgang til graderte opplysninger bare kan innvilges dersom vedkommende som framsetter anmodningen har et dokumentert tjenstlig behov for innsyn, i forbindelse med det formål som ligger til grunn for at opplysningene er utlevert til den mottakende part

Artikkel 3
Gjensidig samsvarende sikkerhetsgradering

1) Forpliktelsene hver av partene påtar seg innenfor denne avtalens virkeområde skal behandles i samsvar med relevant nasjonal lovgivning

2) Partene har gjort seg gjensidig kjent med sikkerhetstiltakene fastsatt i deres respektive nasjonale lovgivninger og avtaler slik at følgende sikkerhetsgradering skal benyttes med sikte på gjennomføring av denne avtale:

Ungarsk	**Engelsk**	**Norsk**
"Szigorúan Titkos"	Top Secret	Strengt Hemmelig
"Titkos"	Secret	Hemmelig
"Bizalmas"	Confidential	Konfidensielt
"Korlátozott Terjesztésű"	Restricted	Begrenset

3) Begge parter forplikter seg til å merke graderte opplysninger mottatt fra den annen part med den aktuelle nasjonale sikkerhetsgrad i henhold til nr. 2 i denne artikkel.

4) Begge parter forplikter seg til å underrette den annen om enhver endring i rekkefølgen av sikkerhetsgraderingene og om enhver endring av de formelle betegnelsene.

5) Bare den utstedende part skal ha myndighet til a endre eller oppheve sikkerhetsgraden for sine graderte opplysninger. Den mottakende part skal underrettes skriftlig om enhver endring eller opphevelse av sikkerhetsgrad

6) Sikkerhetsgraden den utstedende part har fastsatt skal fremkomme pa enhver kopi som tas av de graderte opplysningene

Artikkel 4
Partenes forpliktelser

1) Begge parter skal sta ansvarlig fra det øyeblikk de mottatte graderte opplysningene overføres.

2) I samsvar med nasjonale lover og forskrifter og nasjonal praksis skal hver av partene treffe de nødvendige tiltak for a beskytte graderte opplysninger som overføres, mottas, produseres eller utvikles som følge av enhver avtale eller forbindelse mellom partene

3) Graderte opplysninger som utveksles mellom partene kan bare brukes i samsvar med denne avtalens bestemmelser. Opplysninger som stammer fra en av partene kan ikke bringes videre til tredjemann uten den utstedende parts forutgående skriftlige samtykke

4) Opplysninger som er et resultat av felles aktiviteter skal ikke kunne overføres til tredjemann uten begge parters forutgående skriftlige samtykke

5) Tilgang til graderte opplysninger og til lokaliteter og anlegg der graderte aktiviteter blir utført eller graderte opplysninger blir lagret, skal være begrenset til personer som er sikkerhetsklarert i henhold til artikkel 2, og som pa grunn av sin funksjon eller stilling har "behov for innsyn" i henhold til artikkel 2.

6) Hver av partene forplikter seg til å underrette organer de fører tilsyn med om at denne avtalen trer i kraft, så snart deres aktiviteter berører slike graderte opplysninger.

7) Hver av partene forplikter seg til å påse at alle organer de fører tilsyn med strengt overholder denne avtalens bestemmelser

8) Denne avtalen er overordnet alle eksisterende og fremtidige avtaler mellom partene og organer underlagt dem, som gjelder utveksling av graderte opplysninger.

9) Dersom en av partene og eller dens organer eller enheter som befatter seg med saker omhandlet i artikkel 1, tildeler en kontrakt som skal oppfylles på den annen parts territorium, og denne kontrakt innbefatter graderte opplysninger, skal den part som representerer det land der oppfyllelsen i henhold til denne avtale finner sted, påta seg ansvaret for å forvalte slike graderte opplysninger i samsvar med egne standarder og krav

10) For den ene parts leverandører eller potensielle leverandører gis tilgang til graderte opplysninger mottatt fra den annen part, skal den mottakende part

a) sikre at slike leverandører eller potensielle leverandører og deres anlegg er i stand til å gi de graderte opplysningene tilstrekkelig beskyttelse,

b) sikre nødvendig sikkerhetsklarering til anlegget for de aktuelle leverandører,

c) sikre nødvendig sikkerhetsklarering for alt personell hvis oppgaver forutsetter tilgang til de graderte opplysningene,

d) sikre at alle personer som har tilgang til de graderte opplysningene er kjent med sitt ansvar for å beskytte de graderte opplysningene i samsvar med gjeldende lovgivning

Artikkel 5
Nasjonale sikkerhetsmyndigheter

1) Følgende nasjonale sikkerhetsmyndigheter er ansvarlige for gjennomføringen og overvåkingen av alle sider ved denne avtale

- I Republikken Ungarn:

Ministry of Defence
1885 Budapest
Pf. 25
Ungarn

- I Kongeriket Norge

Forsvarets overkommando
Sikkerhetsstaben
Postboks 14
1306 Bærum Postterminal
Norge

2) Hver av partene forplikter seg til å sikre at denne avtalens bestemmelser blir behørig overholdt av deres respektive nasjonale sikkerhetsmyndigheter

3) Begge parters nasjonale sikkerhetsmyndigheter skal, hver innenfor sin egen stats jurisdiksjon, utarbeide, distribuere og overvåke sikkerhetsinstrukser og -rutiner for å beskytte graderte opplysninger som utveksles som følge av eventuelle andre avtaler mellom partene

Artikkel 6
Konsultasjon

For å legge til rette for gjennomføring av likeverdige standarder på sikkerhetsreglene skal hver av partene underrette den annen om sine sikkerhetsbestemmelser, -rutiner og praksis - og om enhver endring i den underliggende lovgivning som gjelder beskyttelse av graderte opplysninger, og skal ha plikt til å fremme kontakten mellom deres nasjonale sikkerhetsmyndigheter

Artikkel 7
Overføring av graderte opplysninger

1) Graderte opplysninger skal oversendes gjennom diplomatiske kanaler eller med en person som nyter tilsvarende privilegier og immunitet i henhold til folkeretten.

2) Utveksling av opplysninger sikkerhetsgradert Begrenset og Konfidensielt kan også skje via representanter som er offisielt utnevnt av myndighetene i de to landene. Slik autorisasjon kan om nødvendig gis til representanter for private foretak som er engasjert i konkrete militære prosjekter.

3) Levering av graderte opplysninger i store enheter eller mengder skal avtales særskilt i det enkelte tilfelle.

4) Andre godkjente metoder for overføring eller utveksling kan benyttes etter avtale med den enkelte nasjonale sikkerhetsmyndighet.

5) Den mottakende part skal behørig underrette den utstedende part om at de graderte opplysningene er mottatt.

Artikkel 8
Besøk

1) Besøk i lokaliteter der graderte opplysninger utvikles, håndteres eller lagres eller der graderte militære prosjekter utføres, skal bare tillates av den ene part for besøkende fra den annen parts land dersom det på forhånd er innhentet skriftlig tillatelse fra mottakende parts nasjonale sikkerhetsmyndighet. Slik tillatelse skal bare gis til personer som er sikkerhetsklarert og har "behov for innsyn".

2) Tilgang til graderte opplysninger og til installasjoner, anlegg osv. der graderte opplysninger lagres eller håndteres, skal bare tillates av den ene parten for besøkende fra den annen part dersom de er blitt

   a) kontrollert av den nasjonale sikkerhetsmyndighet eller annen ansvarlig statlig myndighet i det land som sender dem, og er bemyndiget til å motta graderte opplysninger i samsvar med de nasjonale bestemmelser i vertslandet, og/eller

b) bemyndiget av den nasjonale sikkerhetsmyndighet eller annen ansvarlig statlig myndighet i vedkommende land til å gjennomføre det eller de besøk anmodningen gjelder.

3) Den nasjonale sikkerhetsmyndighet hos den sendende part skal, i samsvar med bestemmelsene i denne artikkel, varsle den nasjonale sikkerhetsmyndighet hos den mottakende part om de besøkende minst tre - 3 - uker før besøket skal finne sted.

4) Besøksanmodningen skal inneholde:

a) den besøkendes etternavn, fornavn, fødested og fødselsdato, nasjonalitet og arbeidsgiver, samt den besøkendes pass eller andre legitimasjonsbevis,

b) bekreftelse av den besøkendes sikkerhetsklarering i samsvar med besøkets formål,

c) målet for og formålet 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 anmodningen gjelder,

e) kontaktpunkt ved installasjonen/anlegget som skal besøkes, tidligere kontakter og eventuelle andre opplysninger som måtte være nyttige for å fastslå motivet for besøket eller besøkene.

5) Anmodningen skal sendes:

a) gjennom den norske ambassade i Budapest for anmodninger fra norske statsborgere om besøk i Ungarn,

b) gjennom den ungarske ambassade i Oslo for anmodninger fra ungarske statsborgere om besøk i Norge.

c) Andre fremgangsmåter kan benyttes dersom de to nasjonale sikkerhetsmyndighetene omforenes om det.

6) Besøkstillatelsens gyldighet skal ikke overstige tolv - 12 - måneder.

7) Graderte opplysninger som utveksles under et besøk, skal ha samme beskyttelsesnivå og sikkerhetsgrad som hos den utstedende part.

Artikkel 9
Kontrakter

1) Den ene parts nasjonale sikkerhetsmyndighet, som ønsker a tildele en gradert kontrakt til en leverandør i den annen parts land, eller som ønsker a gi en av sine egne leverandører tillatelse til å tildele en gradert kontrakt i den annen parts land innenfor et gradert militært prosjekt, skal på forhånd innhente en skriftlig forsikring fra den annen parts nasjonale sikkerhetsmyndighet om at den foreslåtte leverandør er sikkerhetsklarert på nødvendig nivå og har kapasitet til å håndtere og lagre graderte opplysninger på dette nivå. For sikkerhetsgraden BEGRENSET utstedes en sikkerhetsforsikring i henhold til artikkel 2.

2) Alle kontrakter mellom enheter hos partene og eller private organisasjoner skal inneholde et sikkerhetsavsnitt og en oversikt over sikkerhetsgraderingen på grunnlag av denne avtalens vilkår.

3) Den nasjonale sikkerhetsmyndighet i det land der arbeidet skal utføres, skal påta seg ansvaret for a fastsette og forvalte sikkerhetstiltak for kontrakten etter de samme standarder og krav som gjelder for beskyttelse av egne graderte kontrakter.

4) Underleverandører som er interessert i graderte underkontrakter, skal av leverandøren på forhånd presenteres for den nasjonale sikkerhetsmyndighet for godkjenning. Hvis slik godkjenning oppnås, må underleverandøren oppfylle de samme sikkerhetsforpliktelser som de som er fastsatt for leverandøren.

5) Varsel om alle graderte militære prosjekter, avtaler, kontrakter eller underkontrakter skal på forhånd oversendes den nasjonale sikkerhetsmyndighet i det land der prosjektet skal utføres.

6) To - 2 - eksemplarer av sikkerhetsavsnittet i enhver gradert kontrakt skal oversendes den nasjonale sikkerhetsmyndighet i det land der arbeidet skal utføres.

Artikkel 10
Sikkerhetsbrudd

Ved sikkerhetsbrudd i henhold til artikkel 2 i forbindelse med opplysninger sikkerhetsgradert Konfidensielt eller høyere, som stammer fra eller er mottatt fra den annen part, og som medfører en sikkerhetskompromittering i henhold til artikkel 2, eller dersom felles interesser er berørt, skal den nasjonale sikkerhetsmyndighet i det land der kompromitteringen finner sted, snarest mulig underrette det annet lands nasjonale sikkerhetsmyndighet og iverksette hensiktsmessig etterforskning. Den annen part skal, om den anmodes om det, bistå i etterforskningen. Den annen part skal i alle tilfeller underrettes om utfallet av etterforskningen og motta en endelig redegjørelse for grunnene til og omfanget av sikkerhetsbruddet.

Artikkel 11
Kostnader

Hver part skal selv bære de kostnader den påføres i forbindelse med gjennomføringen av denne avtale og dens bestemmelser

Artikkel 12
Tvistelosning

1) Alle tvister i forbindelse med fortolkningen eller gjennomføringen av denne avtale skal løses av partene ved forhandling og skal ikke bringes inn for tredjemann eller noen internasjonal domstol

2) Så lenge tvisten pågår, skal begge parter fortsatt oppfylle alle sine forpliktelser etter denne avtale

Artikkel 13
Sluttbestemmelser

1) Denne avtale trer i kraft 60 dager etter at begge parter har undertegnet avtalen og underrettet hverandre via diplomatiske kanaler om at de har truffet de nødvendige nasjonale tiltak for at den skal bli rettskraftig

2) Avtalen skal gjelde på ubestemt tid. Den kan sies opp av hver av partene ved skriftlig varsel til den annen part. Avtalen opphører å gjelde seks måneder etter at slikt skriftlig varsel er mottatt. Ved oppsigelse skal graderte opplysninger som er oversendt i henhold til denne avtale snarest mulig sendes tilbake til den annen part. Graderte opplysninger som ikke sendes tilbake, skal beskyttes i samsvar med bestemmelsene fastsatt i denne avtale

3) Avtalen kan endres ved gjensidig overenskomst mellom partene Enhver endring skal avtales skriftlig gjennom diplomatiske kanaler og trer i kraft i samsvar med bestemmelsene i nr 1 i denne artikkel.

Utferdiget i . 1999
i to originale eksemplarer pa ungarsk, norsk og engelsk, der alle tekster har samme gyldighet I tilfelle av avvik mellom den norske og den ungarske teksten skal den engelske teksten ha fortrinn

for Regjeringen i
Republikken Ungarn

For Regjeringen i
Kongeriket Norge

[TRANSLATION - TRADUCTION]

ACCORD RELATIF À LA PROTECTION DES RENSEIGNEMENTS CLASSIFIÉS EN MATIÈRE DE DÉFENSE ENTRE LES GOUVERNEMENTS DE LA RÉPUBLIQUE DE HONGRIE ET DU ROYAUME DE NORVÈGE

Les Gouvernements de la République de Hongrie et du Royaume de Norvège (ci-après dénommés "les Parties"), motivés par leur volonté de protéger les renseignements militaires classifiés (ci-après: "les renseignements classifiés") échangés directement ou par l'entremise d'autres entités administratives ou organisations privées qui traitent des renseignements classifiés sous l'autorité des ministres de la Défense des Parties, dans le but d'établir des conditions de sécurité, sont convenus de ce qui suit:

Article premier. Applicabilité

1. Le présent Accord fait partie intégrante de tout contrat portant sur les sujets suivants, à conclure ou à signer à l'avenir entre les Parties:

a) la coopération entre les deux Parties dans le domaine militaire et de la défense nationale;

b) la coopération, l'échange de renseignements, les coentreprises, les contrats ou toute autre relation entre des entités et/ou des entreprises privées des Parties portant sur des questions de défense nationale et de sécurité militaire;

c) la vente, par l'une des Parties, de matériel et de savoir-faire liés à la défense;

d) les renseignements relatifs à la défense nationale, à la sécurité et aux questions militaires, transférés entre les Parties par tout représentant, membre du personnel ou conseiller (privé ou non).

2. 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.

Article 2. Définitions

Aux fins du présent Accord, les termes et expressions ci-dessous sont à interpréter comme suit:

1. 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.

2. L'expression "Partie émettrice" s'entend de toute personne physique ou morale qui communique les renseignements classifiés.

3. L'expression "Partie réceptrice" s'entend de toute personne physique ou morale qui reçoit les renseignements classifiés de la Partie qui les communique.

4. Le terme "organisme" désigne les institutions privées ou publiques relevant des autorités de sécurité compétentes des Parties qui traitent, protègent ou emmagasinent des renseignements classifiés.

5. L'expression "tierce Partie" s'entend de tous les gouvernements qui n'ont pas été désignés comme parties aux fins du présent Accord ainsi que des personnes physiques ou morales qui ne sont pas des personnes physiques ou morales des Parties.

6. Le terme "contrat" désigne un accord entre deux parties ou plus qui crée et définit des droits et des obligations exécutoires entre les parties.

7. L'expression "contrat classifié" s'entend d'un contrat qui contient ou traite des renseignements classifiés.

8. Le terme "contractant" désigne une personne physique ou morale dotée de la capacité juridique de conclure des contrats.

9. 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.

10. 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 ou morales non autorisées ou habilitées à y avoir accès.

11. 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 et à manier ceux-ci conformément aux règlements nationaux de sécurité concernés.

12. 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.

13. 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.

Article 3. Conformité réciproque des renseignements classifiés

1. Les obligations contractées par les Parties au titre du présent Accord sont traitées conformément à la législation nationale du pays en question.

2. Les Parties, après s'être mutuellement informées des mesures de sécurité définies dans leur législation nationale respective, décident que les classifications suivantes seront utilisées aux fins de l'application du présent Accord:

Hongrois	Anglais	Norvégien
"Szigorúan Titkos!"	Top Secret	Strengt Hemmelig
"Titkos!"	Secret	Hemmelig
"Bizalmas!"	Confidential	Konfidensielt
"Korlátozott Terjesztésû!"	Restricted	Begrenset

3. Les Parties s'engagent toutes deux à marquer les renseignements classifiés reçus de l'autre Partie au moyen de la classification nationale correspondante, telle que définie au paragraphe 2 du présent article.

4. Les Parties s'engagent toutes deux à s'informer mutuellement de toute modification de l'ordre de classification ou de tous changements dans la méthode formelle de désignation.

5. Seule la Partie émettrice est autorisée à modifier ou à annuler le niveau de classification de ses renseignements classifiés. La Partie réceptrice est informée par écrit de toute modification ou annulation du niveau de classification.

6. Le niveau de classification désigné par la Partie émettrice apparaît sur toute copie des renseignements classifiés.

Article 4. Obligations des Parties

1. Les Parties sont responsables des renseignements classifiés reçus à compter du moment du transfert.

2. Conformément à leurs lois, règlements et pratiques nationaux, les Parties prennent les mesures qui s'imposent pour protéger les renseignements classifiés qui sont transmis, reçus, produits ou créés suite à tout accord ou toute relation entre les Parties.

3. Les renseignements classifiés échangés par les Parties ne peuvent être utilisés que conformément aux dispositions du présent Accord. Les renseignements provenant d'une des Parties ne peuvent être transmis à une tierce partie sans l'accord écrit préalable de la Partie émettrice.

4. Les renseignements qui découlent d'activités conjointes ne sont pas transférables à de tierces parties sans l'accord écrit préalable des deux Parties.

5. L'accès aux renseignements classifiés et aux lieux et aux installations où des activités classifiées sont effectuées ou des renseignements classifiés sont stockés sera limité aux personnes ayant reçu une habilitation de sécurité au sens de la définition de l'article 2 et qui, en raison de leurs fonctions ou de leur emploi, ont "besoin d'en connaître" au sens de la définition de cette expression donnée à l'article 2.

6. Les Parties s'engagent à informer les organismes qu'elles contrôlent de l'entrée en vigueur du présent Accord dès lors que leurs activités se rapportent à ces renseignements classifiés.

7. Les Parties s'obligent à veiller à ce que tous les organismes qu'elles contrôlent respectent rigoureusement les dispositions du présent Accord.

8. Le présent Accord régit tous les accords, conclus ou à conclure, entre les Parties et les organismes qui dépendent d'elles et qui ont trait à l'échange de renseignements classifiés.

9. 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, 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.

10. 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) s'assure qu'une habilitation de sécurité appropriée soit accordée aux contractants concernés pour l'accès aux installations,

c) veille à ce qu'une habilitation de sécurité appropriée soit accordée 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.

Article 5. Autorités de sécurité compétentes

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

- pour la République de Hongrie: le Ministère de la Défense

1885 Budapest

B.P. 25

Hongrie

- pour le Royaume de Norvège: le Quartier-Général du commandement de la Défense de la Norvège

Division de la sécurité

B.P. 14

1306 Baerum Postterminal

Norvège

2. Chaque Partie s'engage à veiller à ce que les dispositions du présent Accord soient dûment respectées par son autorité de la sécurité compétente.

3. Les deux autorités de la 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.

Article 6. Consultation

Les Parties, afin de veiller à l'application de règles de sécurité de niveaux équivalents, s'informent mutuellement de leurs propres règlements, procédures et pratiques en matière de sécurité et de toute modification du cadre législatif relatif à la protection des renseignements classifiés, et sont tenues de faciliter les contacts entre leurs autorités de sécurité compétentes.

Article 7. Transmission de renseignements classifiés

1. Les renseignements classifiés sont transmis par la voie diplomatique ou par l'intermédiaire d'une personne bénéficiant de privilèges et d'immunités similaires à ceux prévus en droit international.

2. L'échange de renseignements classifiés (confidentiels et à diffusion restreinte) peut aussi se faire par l'intermédiaire de représentants désignés officiellement par les autorités des deux États. Le cas échéant, cette habilitation peut être accordée aux représentants d'entreprises privées qui participent à des projets militaires particuliers.

3. La remise d'éléments ou de quantités importantes de renseignements classifiés peut être convenue cas par cas.

4. D'autres moyens approuvés de transmission ou d'échange peuvent être utilisés si les deux autorités de sécurité compétentes en conviennent.

5. La Partie réceptrice accuse réception en bonne et due forme à la Partie émettrice des renseignements classifiés.

Article 8. Visites

1. Les visites aux locaux dans lesquels des renseignements classifiés sont produits, manipulés ou emmagasinés ou des projets militaires 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 et qui ont "besoin d'en connaître".

2. L'accès aux renseignements classifiés et aux établissements, infrastructures, etc. où ces informations 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 renseignements classifiés 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 ou les visites demandées.

3. 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 dispositions du présent article.

4. 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 l'établissement/l'infrastructure à visiter, les contacts antérieurs et toute autre information utile pour déterminer le caractère justifié de la visite ou des visites.

5. La demande sera introduite:

a) par l'intermédiaire de l'ambassade de Norvège à Budapest pour les demandes de visite de citoyens norvégiens en Hongrie;

b) par l'intermédiaire de l'ambassade de Hongrie à Oslo pour les demandes de visite de citoyens hongrois en Norvège;

c) d'autres procédures peuvent être utilisées si elles sont approuvées par les deux autorités de sécurité compétentes.

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

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

Article 9. Contrats

1. L'autorité de sécurité 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 militaire 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 ACCES RESTREINT, une garantie de sécurité telle que celle définie à l'article 2 sera fournie.

2. Tout contrat passé entre des entités des Parties et/ou des organisations privées comportera une section appropriée relative à la sécurité et une liste de classification 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 eontrat 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 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.

5. Une notification de tout projet militaire, accord, contrat ou contrat de sous-traitance classifiés devra être adressée 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 10. Infraction à la sécurité

En cas d'infraction à la sécurité au sens de la définition de l'article 2 relative à des renseignements du niveau "confidentiel" ou au-dessus dont le résultat est une compromission de la sécurité au sens de la définition de l'article 2 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 laquelle la compromission 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. Dans tous les cas de figure, l'autre Partie est informée des résultats de l'instruction et reçoit un rapport final sur les raisons et l'ampleur de l'atteinte à la sécurité.

Article 11. Dépenses engagées

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

Article 12. Règlement des différends

1. Les Parties règlent tout différend qui surgirait au sujet de l'interprétation ou de l'application du présent Accord par voie de négociation et ne saisiront ni des parties tierces, ni une juridiction internationalc.

2. Pendant la durée de ce différend, les Parties continuent de remplir toutes les obligations qui découlent du présent Accord.

Article 13. Dispositions finales

1. Le présent Accord entrera en vigueur 60 jours après la date à laquelle les Parties l'auront signé et se seront informées par la voie diplomatique qu'elles ont pris les mesures internes nécessaires à son application.

2. Le présent Accord a une durée de validité illimitée et peut être dénoncé par l'une des Parties moyennant notification écrite adressée à l'autre Partie. Cette dénonciation prend effet six mois après ladite notification. En cas de dénonciation du présent Accord, les renseignements classifiés transmis en vertu du présent Accord seront restitués dès que possible à l'autre Partie. Tout renseignement classifié non restitué sera protégé conformément aux dispositions du présent Accord.

3. La présent Accord peut être modifié d'un commun accord entre les Parties. La concordance de ces modifications se fera par écrit par la voie diplomatique et les modifications entreront en vigueur conformément aux dispositions du paragraphe 1 du présent article.

Fait à Oslo le 12 octobre 1999 en deux exemplaires en hongrois, norvégien et anglais, tous les textes faisant également foi. En cas de discordance entre les textes en norvégien et en hongrois, le texte anglais l'emportera.

Pour le Gouvernement de la République de Hongrie :
JÁNOS SZABÓ

Pour le Gouvernement du Royaume de Norvège :
ELBGUNY LØWER