Dohoda

medzi

vládou

Slovenskej republiky

a

vládou

Luxemburského veľkovojvodstva

o výmene a vzájomnej ochrane

utajovaných skutočností

Vláda Slovenskej republiky
a
vláda Luxemburského veľkovojvodstva

(ďalej len „zmluvné strany“)

Želajúc si zabezpečiť ochranu utajovaných skutočností vymenených medzi štátmi zmluvných strán alebo medzi verejnými právnickými osobami alebo súkromnými právnickými osobami v ich jurisdikcii, s ohľadom na národné záujmy a bezpečnosť,

sa dohodli takto:

Článok 1
Cieľ dohody a rozsah jej použitia

1) Cieľom tejto dohody je zabezpečiť ochranu utajovaných skutočností spoločne vytvorených alebo vymenených medzi štátmi zmluvných strán.

2) Žiadna zmluvná strana sa neodvolá na túto dohodu s cieľom získať utajované skutočnosti, ktoré druhá zmluvná strana prijala od tretej strany.

Článok 2
Vymedzenie pojmov

Pre účely tejto dohody:

a) **“utajované skutočnosti”** sú akékoľvek informácie, dokumenty alebo veci bez ohľadu na svoju podobu alebo povahu, vytvorené alebo vymenené medzi štátmi zmluvných strán, vyžadujúce si ochranu pred neoprávnenou manipuláciou a utajené v súlade s príslušnými vnútroštátnymi právnymi predpismi,

b) **“odovzdávajúca strana”** je štát zmluvnej strany, ktorý odovzdáva utajované skutočnosti štátu druhej zmluvnej strany,

c) **“prijímajúca strana”** je štát zmluvnej strany, ktorému sú utajované skutočnosti postúpené štátom druhej zmluvnej strany,

d) **“príslušný bezpečnostný orgán”** je národný bezpečnostný orgán zodpovedný za implementáciu a dozor nad touto dohodou,

e) **“utajovaný kontrakt”** je kontrakt alebo subkontrakt medzi dvomi alebo viacerými kontrahentmi, ktorý obsahuje alebo zahŕňa utajované skutočnosti,

f) **“kontrahent”** je fyzická osoba alebo právnická osoba právne spôsobilá uzatvárať utajované kontrakty,

g) **“previerka priemyselnej bezpečnosti”** je zistenie príslušným bezpečnostným orgánom, že právnická osoba má fyzickú a organizačnú spôsobilosť používať a uchovávať utajované skutočnosti v súlade s príslušnými vnútroštátnymi právnymi predpismi,

h) **„previerka personálnej bezpečnosti“** je zistenie príslušným bezpečnostným orgánom, že fyzická osoba je v súlade s príslušnými vnútroštátnymi právnymi predpismi oprávnená mať prístup k utajovaným skutočnostiam,

i) **“need-to-know”** je potreba mať prístup k utajovaným skutočnostiam v rozsahu zastávanej funkcie a pre plnenie konkrétnych úloh,

j) **“tretia strana”** je akýkoľvek štát, organizácia, právnická osoba alebo fyzická osoba, ktorá nie je zmluvnou stranou tejto dohody.

Článok 3
Stupne utajenia a oprávnenia

Zmluvné strany sa dohodli, že nasledujúce stupne utajenia a oprávnenia sú rovnocenné a zodpovedajú stupňom utajenia a oprávnenia stanoveným vnútroštátnymi právnymi predpismi ich štátov:

Pre Slovenskú republiku	Pre Luxemburské veľkovojvodstvo
PRÍSNE TAJNÉ	TRES SECRET LUX
TAJNÉ	SECRET LUX
DÔVERNÉ	CONFIDENTIEL LUX
VYHRADENÉ	RESTREINT LUX

Článok 4
Príslušné bezpečnostné orgány

1) Príslušné bezpečnostné orgány štátov zmluvných strán sú:

   Pre Slovenskú republiku:
   Národný bezpečnostný úrad

   Pre Luxemburské veľkovojvodstvo:
   Service de Renseignement de l’Etat
   Autorité nationale de Sécurité

2) Štáty zmluvných strán sa navzájom informujú diplomatickou cestou o akýchkoľvek zmenách v kontaktných údajoch príslušných bezpečnostných orgánov.

3) Na žiadosť sa príslušné bezpečnostné orgány informujú o príslušných vnútroštátnych právnych predpisoch o ochrane utajovaných skutočností a vymieňajú si informácie o bezpečnostných štandardoch, postupoch a praxi pri ochrane utajovaných skutočností.

Článok 5
Ochrana utajovaných skutočností

1) Štáty zmluvných strán vykonajú v súlade so svojimi vnútroštátnymi právnymi predpismi všetky príslušné opatrenia na ochranu utajovaných skutočností vymieňaných alebo vytvorených podľa tejto dohody. Takým utajovaným skutočnostiam sa prizná rovnaký stupeň ochrany, aký sa poskytuje národným utajovaným skutočnostiam so zodpovedajúcim stupňom utajenia v súlade s článkom 3.

2) Odovzdávajúca strana upovedomí prijímajúcu stranu písomne o akejkoľvek zmene v stupni utajenia postúpených utajovaných skutočností.

3) Prístup k utajovaným skutočnostiam sa obmedzí na základe need-to-know na osoby, ktoré sú v súlade s vnútroštátnymi právnymi predpismi oprávnené na prístup k utajovaným skutočnostiam zodpovedajúceho stupňa utajenia.

4) V rámci tejto dohody si štáty zmluvných strán navzájom uznajú previerky personálnej a priemyselnej bezpečnosti udelené v súlade s vnútroštátnymi právnymi predpismi štátu druhej zmluvnej strany. Bezpečnostné previerky sú ekvivalentné v súlade s článkom 3.

5) Príslušné bezpečnostné orgány si na žiadosť navzájom pomáhajú v súlade s vnútroštátnymi právnymi predpismi pri vykonávaní previerkového procesu potrebného pre vykonávanie tejto dohody.

6) V rámci tejto dohody sa príslušné bezpečnostné orgány navzájom bezodkladne informujú o akejkoľvek zmene týkajúcej sa previerok personálnej alebo priemyselnej bezpečnosti, najmä o ich odňatí alebo znížení stupňa oprávnenia.

7) Prijímajúca strana:

   a) postúpi utajované skutočnosti akejkoľvek tretej strane iba na základe predchádzajúceho písomného súhlasu odovzdávajúcej strany,

   b) označí prijaté utajované skutočnosti v súlade s článkom 3,

   c) použije utajované skutočnosti výlučne na účely, na ktoré boli postúpené.

Článok 6
Postupovanie utajovaných skutočností

1) Utajované skutočnosti sa postupujú v súlade s príslušnými vnútroštátnymi právnymi predpismi diplomatickou cestou, ak sa príslušné bezpečnostné orgány nedohodnú inak. Prijímajúca strana potvrdí prijatie utajovaných skutočností písomne.

2) Elektronicky sa postupovanie utajovaných skutočností uskutoční prostredníctvom šifrových prostriedkov, na ktorých sa dohodnú príslušné bezpečnostné orgány.

Článok 7
Rozmnožovanie a preklad utajovaných skutočností

1) Preklady a rozmnožovanie utajovaných skutočností sa uskutočňujú v súlade s vnútroštátnymi právnymi predpismi prijímajúcej strany a týmito postupmi:

   a) fyzické osoby majú príslušnú previerku personálnej bezpečnosti v súlade s ich vnútroštátnymi právnymi predpismi,

b) preklady a kópie sa označia a ochraňujú rovnako ako pôvodné utajované skutočnosti,

c) preklady a počet kópií sú obmedzené úradnou potrebou,

d) preklady obsahujú príslušnú poznámku v jazyku prekladu označujúcu, že preklad obsahuje utajované skutočnosti odovzdávajúcej strany.

2) Utajované skutočnosti označené TAJNÉ/ SECRET LUX alebo vyšším stupňom utajenia sa prekladajú alebo rozmnožujú iba na základe predchádzajúceho písomného súhlasu odovzdávajúcej strany.

Článok 8
Zničenie utajovaných skutočností

1) Utajované skutočnosti sa zničia tak, aby sa vylúčilo ich čiastočné alebo úplné obnovenie.

2) Utajované skutočnosti označené TAJNÉ/ SECRET LUX a nižším stupňom utajenia sa zničia v súlade s vnútroštátnymi právnymi predpismi.

3) Utajované skutočnosti označené PRÍSNE TAJNÉ/ TRES SECRET LUX sa nezničia. Vrátia sa príslušnému bezpečnostnému orgánu odovzdávajúcej strany.

4) O zničení utajovaných skutočností sa vyhotoví správa, ktorej anglický preklad sa doručí príslušnému bezpečnostnému orgánu odovzdávajúcej strany.

Článok 9
Utajované kontrakty

1) Štátu zmluvnej strany, ktorý má v úmysle uzavrieť utajovaný kontrakt s kontrahentom štátu druhej zmluvnej strany, alebo zamýšľa splnomocniť jedného zo svojich kontrahentov na uzavretie utajovaného kontraktu na území štátu druhej zmluvnej strany v rámci utajovaného projektu, sa doručí prostredníctvom jeho príslušného bezpečnostného orgánu predchádzajúce písomné uistenie od príslušného bezpečnostného orgánu štátu druhej zmluvnej strany, že navrhovaný kontrahent má previerku priemyselnej bezpečnosti príslušného stupňa oprávnenia v súlade s príslušnými právnymi predpismi.

2) Utajovaný kontrakt zahŕňa zvláštnu časť alebo prílohu označujúcu bezpečnostné požiadavky utajovaného kontraktu.

3) Každý utajovaný kontrakt uzavretý v súlade s touto dohodou obsahuje:

a) záväzok kontrahenta zabezpečiť, aby jeho priestory mali potrebné podmienky pre zaobchádzanie s utajovanými skutočnosťami príslušného stupňa utajenia a ich uchovávanie,

b) záväzok kontrahenta zabezpečiť, aby osoby, ktoré potrebujú na vykonávanie svojich povinností prístup k utajovaným skutočnostiam, mali príslušný stupeň previerky personálnej bezpečnosti,

c) záväzok kontrahenta zabezpečiť, aby všetky osoby, ktoré majú prístup k utajovaným skutočnostiam, boli oboznámené so svojou zodpovednosťou vo vzťahu k ochrane utajovaných skutočností v súlade s vnútroštátnymi právnymi predpismi,

d) záväzok kontrahenta vykonávať periodické bezpečnostné kontroly svojich priestorov,

e) zoznam utajovaných skutočností a zoznam oblastí, v ktorých môžu utajované skutočnosti vzniknúť,

f) postup pre oznámenie zmien stupňa utajenia utajovaných skutočností,

g) zoznam komunikačných a elektronických prostriedkov pre postúpenie,

h) postup pri preprave utajovaných skutočností,

i) zoznam príslušných oprávnených fyzických osôb alebo právnických osôb zodpovedných za koordináciu dozoru nad utajovanými skutočnosťami vo vzťahu k utajovanému kontraktu,

j) záväzok kontrahenta oznámiť každú skutočnú alebo domnelú stratu, únik informácií alebo ohrozenie bezpečnosti utajovaných skutočností,

k) záväzok kontrahenta postúpiť kópiu utajovaného kontraktu svojmu príslušnému bezpečnostnému orgánu,

l) záväzok subkontrahenta splniť rovnaké bezpečnostné záväzky ako kontrahent.

4) Keď sa začnú predkontraktné rokovania medzi potenciálnym kontrahentom na území štátu jednej zmluvnej strany a iným potenciálnym kontrahentom z územia štátu druhej zmluvnej strany, s cieľom podpísať utajované kontrakty, príslušný bezpečnostný orgán informuje štát druhej zmluvnej strany o stupni utajenia utajovaných skutočností súvisiacich s predkontraktnými rokovaniami.

5) S cieľom umožniť adekvátny bezpečnostný dohľad a kontrolu sa kópia utajovaného kontraktu postúpi príslušnému bezpečnostnému orgánu štátu zmluvnej strany, kde sa majú práce vykonať.

6) Zástupcovia príslušných bezpečnostných orgánov môžu uskutočňovať vzájomné návštevy s cieľom analyzovať účinnosť opatrení prijatých kontrahentom na ochranu utajovaných skutočností, ktorých sa utajovaný kontrakt týka. Oznámenie o návšteve sa zašle najmenej dvadsať dní vopred.

Článok 10
Návštevy

1) Návštevy zahŕňajúce prístup príslušníkov štátu jednej zmluvnej strany k utajovaným skutočnostiam štátu druhej zmluvnej strany sú predmetom predchádzajúceho písomného súhlasu daného príslušným bezpečnostným orgánom hostiteľského štátu.

2) Návštevy zahŕňajúce prístup k utajovaným skutočnostiam povolí štát jednej zmluvnej strany návštevníkom zo štátu druhej zmluvnej strany, len ak návštevníkom bola udelená príslušným bezpečnostným orgánom vysielajúceho štátu previerka personálnej bezpečnosti príslušného stupňa oprávnenia a ak sú oprávnení prijať alebo mať prístup k utajovaným skutočnostiam v súlade s ich vnútroštátnymi právnymi predpismi.

3) Návštevy zahŕňajúce prístup príslušníkov tretieho štátu sa povolia len na základe spoločnej dohody štátov zmluvných strán.

4) Príslušnému bezpečnostnému orgánu hostiteľského štátu žiadosť o vykonanie návštevy doručí príslušný bezpečnostný orgán druhého štátu aspoň tridsať dní vopred.

5) V súrnych prípadoch sa žiadosť o návštevu postúpi najmenej sedem dní vopred.

6) Žiadosť o vykonanie návštevy obsahuje:

   a) meno a priezvisko, dátum a miesto narodenia, štátnu príslušnosť, číslo pasu alebo identifikačného dokladu návštevníka,

   b) názov právnickej osoby, ktorú návštevník zastupuje,

   c) názov a adresu právnickej osoby, ktorá má byť navštívená,

   d) potvrdenie o previerke personálnej bezpečnosti návštevníka a jej platnosti,

   e) cieľ a účel návštevy, ako aj údaj o najvyššom stupni utajenia zahrnutých utajovaných skutočností,

   f) predpokladaný dátum a trvanie návštevy, o ktorú sa žiada. V prípade opakovaných návštev celkové obdobie pokrývajúce všetky návštevy,

   g) dátum, podpis a odtlačok úradnej pečiatky príslušného bezpečnostného orgánu.

7) Po schválení návštevy príslušný bezpečnostný orgán hostiteľského štátu poskytne kópiu žiadosti o návštevu bezpečnostným zamestnancom právnickej osoby, kde sa má návšteva uskutočniť.

8) Platnosť povolenia návštevy nepresiahne jeden rok.

9) Štáty zmluvných strán môžu zostaviť zoznamy fyzických osôb oprávnených vykonávať opakované návštevy. Zoznamy sú platné dvanásť mesiacov. Termíny konkrétnych návštev sa dohodnú s príslušnými kontaktnými osobami právnických osôb, ktoré majú tieto fyzické osoby navštíviť, v súlade s dohodnutými termínmi a podmienkami.

10) Každý štát zmluvnej strany zabezpečí ochranu osobných údajov návštevníkov v súlade so svojimi príslušnými právnymi predpismi.

Článok 11
Porušenie bezpečnosti

1) V prípade porušenia bezpečnosti podľa vnútroštátnych právnych predpisov, ktoré má za následok skutočné alebo možné ohrozenie bezpečnosti utajovaných skutočností pochádzajúcich alebo prijatých od štátu druhej zmluvnej strany, príslušný bezpečnostný orgán štátu zmluvnej strany, kde k porušeniu alebo ohrozeniu bezpečnosti došlo, čo najskôr informuje príslušný bezpečnostný orgán štátu druhej zmluvnej strany a začne príslušné vyšetrovanie.

2) Ak k porušeniu bezpečnosti dôjde v štáte inom ako štáty zmluvných strán, príslušný bezpečnostný orgán vysielajúceho štátu vykoná úkony podľa odseku 1.

3) Štát druhej zmluvnej strany na žiadosť pri vyšetrovaní spolupracuje v súlade s odsekom 1.

4) Štát druhej zmluvnej strany je oboznámený s výsledkami vyšetrovania a dostane konečnú správu o dôvodoch a rozsahu spôsobenej škody.

Článok 12
Náklady

Každá zmluvná strana hradí vlastné náklady, pokiaľ ide o vykonávanie a dohľad nad vykonávaním tejto dohody.

Článok 13
Riešenie sporov

Akýkoľvek spor ohľadom výkladu alebo uplatňovania tejto dohody sa rieši diplomatickou cestou, ak ho nemožno urovnať príslušnými bezpečnostnými orgánmi.

Článok 14
Záverečné ustanovenia

1) Táto dohoda sa uzaviera na neurčitý čas a nadobudne platnosť v prvý deň druhého mesiaca nasledujúceho po dátume prijatia poslednej písomnej notifikácie, ktorou si zmluvné strany diplomatickou cestou oznamujú, že boli splnené všetky vnútroštátne právne podmienky potrebné pre nadobudnutie jej platnosti.

2) Túto dohodu možno kedykoľvek meniť na základe vzájomného písomného súhlasu zmluvných strán.

3) Každá zmluvná strana môže túto dohodu kedykoľvek vypovedať písomným oznámením diplomatickou cestou. V takom prípade sa platnosť tejto dohody skončí uplynutím šiestich mesiacov odo dňa prijatia oznámenia o vypovedaní.

4) Zmluvné strany zabezpečia ochranu utajovaných skutočnosti aj po skončení platnosti tejto dohody, kým odovzdávajúca strana nezbaví prijímajúcu stranu tohto záväzku.

5) Štát zmluvnej strany, na území ktorého sa táto dohoda podpíše, ju postúpi na registráciu na sekretariát Organizácie Spojených národov v súlade s článkom 102 Charty Organizácie Spojených národov a upovedomí o tom štát druhej zmluvnej strany, vrátane príslušného registračného čísla.

Na dôkaz toho splnomocnení a riadne poverení, podpísali túto dohodu.

Dané v Bratislave, dňa júla 2011, v dvoch pôvodných vyhotoveniach, každé v slovenskom, francúzskom a anglickom jazyku, pričom každé znenie má rovnakú platnosť. V prípade rozdielnosti výkladu je rozhodujúce znenie v anglickom jazyku.

Za vládu Slovenskej republiky	**Za vládu Luxemburského veľkovojvodstva**
.....	.....
František Blanárik	**Marc Thill**
riaditeľ Národného bezpečnostného úradu	mimoriadny a splnomocnený veľvyslanec

AGREEMENT

BETWEEN
THE GOVERNMENT

OF THE SLOVAK REPUBLIC

AND

THE GOVERNMENT

OF THE GRAND DUCHY OF LUXEMBOURG

ON EXCHANGE AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

The Government of the Slovak Republic
and
the Government of the Grand Duchy of Luxembourg

(hereinafter referred to as "the Parties"),

Wishing to ensure protection of Classified Information exchanged between the States of the Parties or between the public legal entities and private legal entities under their jurisdiction, with respect to the national interests and security,

Have agreed as follows:

Article 1
Objective and Scope

1. The objective of this Agreement is to ensure protection of Classified Information that is commonly generated or exchanged between the States of the Parties.

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 this Agreement:

k) "**Classified Information**" means any information, document or material, irrespective of its form or nature, generated by or exchanged between the States of the Parties, requiring protection against unauthorized manipulation and having been classified in accordance with the respective national legislations;

l) "**Originating Party**" means the State of the Party which transmits Classified Information to the State of the other Party;

m) "**Receiving Party**" means the State of the Party which Classified Information is transmitted to by the State of the other Party;

n) "**Competent Security Authority**" means the national security body responsible for the implementation and supervision of this Agreement;

o) "**Classified Contract**" means a contract or subcontract between two or more Contractors, which contains or involves Classified Information;

p) "**Contractor**" means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;

q) "**Facility Security Clearance**" means the determination by the Competent Security Authority confirming, that the legal entity has the physical and organizational capability to use and store Classified Information in accordance with the respective national legislation;

r) "**Personnel Security Clearance**" means the determination by the Competent Security Authority confirming, in accordance with the respective national legislation, that the individual is eligible to have access to Classified Information;

s) "**Need-to-know**" means the necessity to have access to Classified Information in the scope of a given official position and for the performance of a specific task;

t) "**Third Party**" means any State, organization, legal entity or individual, which is not a party to this Agreement.

Article 3
Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national legislation of their respective States:

For the Slovak Republic	For the Grand Duchy of Luxembourg
PRÍSNE TAJNÉ	TRES SECRET LUX
TAJNÉ	SECRET LUX
DÔVERNÉ	CONFIDENTIEL LUX
VYHRADENÉ	RESTREINT LUX

Article 4
Competent Security Authorities

1. The Competent Security Authorities of the States of the Parties are:

   For the Slovak Republic:
   Národný bezpečnostný úrad

   For the Grand Duchy of Luxembourg:
   Service de Renseignement de l'Etat
   Autorité nationale de Sécurité

2. The States of the Parties shall inform each other through diplomatic channels of any modification of contact data of the Competent Security Authorities.

3. On request, the Competent Security Authorities shall inform each other of respective national legislation on Classified Information and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

Article 5
Protection of Classified Information

1. In accordance with their national legislation, the States of the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. The same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent security classification level in accordance with the Article 3.

2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information.

3. Access to Classified Information shall be limited to persons on a Need-to-know basis who are authorized in accordance with the national legislation to have access to Classified Information of the equivalent security classification level.

4. Within the scope of this Agreement, State of each Party shall mutually recognize the Personnel and Facility Security Clearances granted in accordance with the national legislation of the State of the other Party. The security clearances shall be equivalent in accordance with Article 3.

5. The Competent Security Authorities shall, in accordance with the national legislation, assist each other upon request at carrying out vetting procedures necessary for the application of this Agreement.

6. Within the scope of this Agreement, the Competent Security Authorities shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about their withdrawal or downgrading.

7. The Receiving Party shall:
   a) submit Classified Information to any Third Party only upon prior written consent of the Originating Party;
   b) mark the received Classified Information in accordance with the Article 3;
   c) use Classified Information solely for the purposes it has been provided for.

Article 6
Transmission of Classified Information

1. Classified Information shall be transmitted in accordance with the respective national legislation through diplomatic channels unless otherwise approved on by the Competent Security Authorities. The Receiving Party shall confirm the receipt of Classified Information in writing.

2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means approved on by the Competent Security Authorities.

Article 7
Reproduction and Translation of Classified Information

1. Translations and reproductions of Classified Information shall be made in accordance with the national legislation of the Receiving Party and the following procedures:
   a) the individuals shall be granted the appropriate Personnel Security Clearance in accordance with their national legislation;
   b) the translations and the reproductions shall be marked and protected as the original Classified Information;
   c) the translations and the number of copies shall be limited to that required for official purposes;
   d) the translations shall bear an appropriate note in the language of the translation indicating that it contains Classified Information received from the Originating Party.

2. Classified Information marked TAJNÉ/ SECRET LUX or above shall be translated or reproduced only upon prior written consent of the Originating Party.

Article 8
Destruction of Classified Information

1. Classified Information shall be destroyed so as to prevent its partial or total reconstruction.

2. Classified Information marked up to TAJNÉ/ SECRET LUX shall be destroyed in accordance with the national legislation.

3. Classified Information marked PRÍSNE TAJNÉ/ TRES SECRET LUX shall not be destroyed. It shall be returned to Competent Security Authority of the Originating Party.

4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the Competent Security Authority of the Originating Party.

Article 9
Classified Contracts

1. State of one Party, wishing to place a Classified Contract with a Contractor of the State of the other Party, or wishing to authorize one of its own Contractors to place a Classified Contract in the territory of the State of the other Party within a classified project shall obtain, through its Competent Security Authority, prior written assurance from the Competent Security Authority of the State of the other Party that the proposed Contractor is granted Facility Security Clearance of the appropriate security classification level in accordance with the respective national legislation.

2. A Classified Contract shall include a specific section or annex identifying the security requirements of the Classified Contract.

3. Each Classified Contract concluded in accordance with this Agreement shall include:
   a) commitment of the Contractor to ensure that its premises have necessary conditions for handling and storing Classified Information of appropriate security classification level;
   b) commitment of the Contractor to ensure that persons who perform duties requiring access to Classified Information are granted the appropriate level of Personnel Security Clearance;
   c) commitment of the Contractor to ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national legislation;
   d) commitment of the Contractor to perform periodical security inspections of its premises;
   e) list of Classified Information and list of areas in which Classified Information may arise;
   f) procedure for reporting any changes in the security classification level of Classified Information;
   g) list of communication means and electronic means for transmission;
   h) procedure for the transportation of Classified Information;
   i) list of appropriate authorized individuals or legal entities responsible for the co-ordination of the safeguarding of Classified Information related to the Classified Contract;
   j) commitment of the Contractor to notify of any actual or suspected loss, leak or compromise of the Classified Information;
   k) commitment of the Contractor to forward a copy of the Classified Contract to its own Competent Security Authority;
   l) commitment of the subcontractor to fulfill the same security obligations as the Contractor.

4. As soon as pre-contractual negotiations begin between a potential Contractor in the territory of one State of the Parties and another possible Contractor located in the State of the other Party's territory, aiming at the signing of Classified Contracts, the Competent Security Authority shall inform the State of the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.

5. Copy of each Classified Contract shall be forwarded to the Competent Security Authority of the State of the Party where the work is to be performed, to allow adequate security supervision and control.

6. Representatives of the Competent Security Authorities may visit each other in order to analyze the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract. Notice of the visit shall be provided, at least, twenty days in advance.

Article 10
Visits

1. Visits involving access to Classified Information by nationals from the State of one Party to the State of the other Party shall be subject to prior written consent given by the Competent Security Authority of the host State.
2. Visits involving access to Classified Information shall be allowed by the State of one Party to visitors from the State of the other Party only if they have been granted the appropriate Personnel Security Clearance and authorized to receive or to have access to Classified Information in accordance with their national legislation.
3. Visits involving access to Classified Information by nationals from a third State shall only be authorized by a common agreement between the States of the Parties.
4. The Competent Security Authority of the host State shall receive a request for visit from the other Competent Security Authority at least thirty days in advance.
5. In urgent cases, the request for visit shall be transmitted at least seven days before.
6. The request for visit shall include:
   a) visitor's name and surname, place and date of birth, nationality, passport or identification document number;
   b) name of the legal entity represented by the visitor;
   c) name and address of the legal entity to be visited;
   d) confirmation of the visitor's Personnel Security Clearance and its validity;
   e) object and purpose of the visit, as well as a statement of the highest security classification level of the Classified Information to be involved;
   f) expected date and duration of the requested visit. In case of recurring visits the total period covered by the visits shall be stated;
   g) the date, signature and stamping of the official seal of the Competent Security Authority.
7. Once the visit has been approved the Competent Security Authority of the host State shall provide a copy of the request for visit to the security officers of the legal entity to be visited.
8. The validity of visit approval shall not exceed one year.
9. The States of the Parties may draw up lists of individuals authorized to make recurring visits. The lists shall be valid for twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.
10. Either State of the Party shall guarantee the protection of personal data of the visitors according to its respective national legislation.

Article 11
Breach of Security

1. In case of breach of security in accordance with the national legislation that results in an actual or suspected compromise of Classified Information originated by or received from the State of the other Party, the Competent Security Authority of the State of the Party where the breach or compromise has arisen shall inform the Competent Security Authority of the State of the other Party, as soon as possible, and initiate the appropriate investigation.

2. If a breach of security arises in a State other than States of the Parties, the Competent Security Authority of the dispatching State shall take the actions prescribed in Paragraph 1.

3. The State of the other Party shall, upon request, co-operate in the investigation in accordance with Paragraph 1.

4. The State of the other Party shall be informed of the results of the investigation and shall receive English translation of the final report on the reasons and extent of the damage.

Article 12
Costs

Each Party shall bear its own costs incurred in the course of application and supervision of this Agreement.

Article 13
Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be solved through diplomatic channels unless a settlement by the Competent Security Authorities can be achieved.

Article 14
Final Provisions

1. This Agreement is concluded for an indefinite period of time and enters into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.
2. This Agreement may be amended any time on the basis of mutual written approval of the Parties.
3. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the termination takes effect six months after the date of the receipt of the respective notification.

4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Originating Party dispenses the Receiving Party from this obligation.
5. The State of the Party, in whose territory this Agreement is signed, shall submit it for registration to the Secretariat of the United Nations in accordance with the article 102 of the Charter of the United Nations and shall notify the State of other Party thereof, including the respective number of the registration.

In witness whereof the undersigned, duly authorized, have signed this Agreement.

Done at Bratislava on 26 July 2011 in two originals, each one in the Slovak, French and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Slovak Republic	**For the Government of Grand Duchy of Luxembourg**
……..	……
František Blanárik	**Marc Thill**
Director of the National Security Authority	Extraordinary and Plenipotentiary Ambassador