Dohoda

medzi

Slovenskou republikou

a

Španielskym kráľovstvom

o vzájomnej ochrane

utajovaných skutočností

Slovenská republika
a
Španielske kráľovstvo

ďalej len „zmluvné strany“,

uznávajúc potrebu oboch zmluvných strán zabezpečiť ochranu utajovaných skutočností vzájomne vymieňaných v rámci rokovaní a dohôd o spolupráci, ktoré už sú alebo budú v budúcnosti uzavreté, ako i ďalších zmluvných nástrojov verejných organizácií alebo súkromných organizácií zmluvných strán,

usilujúc sa vytvoriť sústavu pravidiel vzájomnej ochrany utajovaných skutočností vymieňaných medzi zmluvnými stranami,

sa dohodli takto:

Článok 1
Predmet

Táto dohoda zakladá pravidlá bezpečnosti aplikovateľné na všetky zmluvné nástroje, ktoré predpokladajú poskytnutie utajovaných skutočností, už podpísané alebo ešte len na podpis určené medzi príslušnými bezpečnostnými orgánmi oboch zmluvných strán alebo ich podnikmi alebo inými právnickými osobami na to náležite oprávnenými.

Článok 2
Rozsah uplatnenia

(1) Táto dohoda stanovuje postupy pre ochranu utajovaných skutočností vymieňaných medzi zmluvnými stranami.

(2) Žiadna zmluvná strana sa neodvolá na túto dohodu za účelom získania utajovaných skutočností, ktoré druhá zmluvná strana prijala od tretej strany.

Článok 3
Vymedzenie pojmov

Na účely tejto dohody:

a) **„utajované skutočnosti“** sú informácie alebo materiály bez ohľadu na svoju formu alebo povahu, ktoré je potrebné chrániť pred neoprávneným prístupom a ktoré boli za také určené bezpečnostnou klasifikáciou,
b) **„príslušný bezpečnostný orgán“** je národný bezpečnostný orgán/určený bezpečnostný orgán určený zmluvnou stranou ako zodpovedný za implementáciu a dozor nad touto dohodou,
c) **„odovzdávajúca zmluvná strana“** je zmluvná strana, ktorá poskytuje utajované skutočnosti druhej zmluvnej strane,

d) **„prijímajúca zmluvná strana“** je zmluvná strana, ktorej sú utajované skutočnosti poskytnuté odovzdávajúcou zmluvnou stranou,
e) **„tretia strana“** ja akákoľvek medzinárodná organizácia alebo štát, ktorá nie je zmluvnou stranou tejto dohody,
f) **„utajovaný kontrakt“** je dohoda medzi dvoma alebo viacerými kontrahentmi, ktorá zakladá a definuje vynútiteľné práva a povinnosti medzi nimi, pričom obsahuje alebo zahŕňa utajované skutočnosti,
g) **„kontrahent“** je fyzická osoba alebo právnická osoba právne spôsobilá uzatvárať utajované kontrakty,
h) **„previerka personálnej bezpečnosti“** je potvrdenie príslušným bezpečnostným orgánom, že fyzická osoba je spôsobilá mať prístup k utajovaným skutočnostiam v súlade s príslušným vnútroštátnym právnym poriadkom,
i) **„previerka priemyselnej bezpečnosti“** je potvrdenie príslušným bezpečnostným orgánom, že z bezpečnostného hľadiska má právnická osoba fyzickú a organizačnú spôsobilosť používať a uchovávať utajované skutočnosti v súlade s príslušným vnútroštátnym právnym poriadkom,
j) **„need-to-know“** znamená, že prístup k utajovaným skutočnostiam možno udeliť len osobe, ktorá má odôvodnenú požiadavku poznať alebo mať ich pre plnenie svojich úradných povinností, v rámci ktorých boli skutočnosti poskytnuté prijímajúcej zmluvnej strane.

Článok 4
Príslušné bezpečnostné orgány

(1) Príslušné bezpečnostné orgány pre aplikáciu tejto dohody sú:

pre Slovenskú republiku:
Národný bezpečnostný úrad

pre Španielske kráľovstvo:
štátny tajomník, riaditeľ Národného spravodajského centra
Národná bezpečnostná kancelária

(2) Zmluvné strany sa navzájom informujú diplomatickou cestou o akejkoľvek zmene týkajúcej sa ich príslušných bezpečnostných orgánov.

Článok 5
Zásady bezpečnosti

(1) Ochrana a používanie utajovaných skutočností vymieňaných medzi zmluvnými stranami sa spravuje nasledovnými zásadami:

a) prijímajúca zmluvná strana prizná prijatým utajovaným skutočnostiam úroveň ochrany ekvivalentnú označeniam výslovne daným utajovaným skutočnostiam odovzdávajúcou zmluvnou stranou,
b) prístup k utajovaným skutočnostiam je obmedzený na princípe „need-to-know“ na osoby poverené príslušnými bezpečnostnými orgánmi, ktoré potrebujú mať prístup k utajovaným skutočnostiam na plnenie svojich povinností, pričom majú previerku

personálnej bezpečnosti rovnakého alebo vyššieho stupňa ako stupeň utajenia utajovaných skutočností, o prístup ku ktorým ide,

c) prijímajúca zmluvná strana neposkytne utajované skutočnosti žiadnej tretej strane, ktorejkoľvek fyzickej osobe tretej strany alebo právnickej osobe akejkoľvek tretej strany bez predchádzajúceho písomného súhlasu odovzdávajúcej zmluvnej strany,
d) poskytnuté utajované skutočnosti nesmú byť použité na iný účel, ako na ten, na ktorý boli poskytnuté v súlade s touto dohodou.

(2) Príslušné bezpečnostné orgány si na žiadosť navzájom poskytnú informácie o svojich bezpečnostných štandardoch, postupoch a praxi v oblasti ochrany utajovaných skutočností s cieľom dosiahnuť a udržať porovnateľné bezpečnostné štandardy.

(3) Každá zmluvná strana informuje o existencii tejto dohody vždy, keď ide o utajované skutočnosti.

(4) Každá zmluvná strana zabezpečí, aby všetci príjemcovia utajovaných skutočností konali v súlade so záväzkami v tejto dohode.

Článok 6
Stupne utajenia a stupne bezpečnostných previerok a ekvivalencie

Zmluvné strany sa dohodli, že nasledujúce stupne utajenia a stupne bezpečnostných previerok sú ekvivalentné a zodpovedajú stupňom utajenia a stupňom bezpečnostných previerok vo vnútroštátnom právnom poriadku jednotlivých zmluvných strán:

Slovenská republika	Španielske kráľovstvo	Ekvivalent v anglickom jazyku
PRÍSNE TAJNÉ	SECRETO	TOP SECRET
TAJNÉ	RESERVADO	SECRET
DÔVERNÉ	CONFIDENCIAL	CONFIDENTIAL
VYHRADENÉ	DIFUSIÓN LIMITADA	RESTRICTED

Článok 7
Spolupráca v previerkovom procese

(1) Príslušné bezpečnostné orgány zmluvných strán, berúc do úvahy svoj vnútroštátny právny poriadok na žiadosť spolupracujú pri previerkovom procese svojich občanov žijúcich alebo právnických osôb sídliacich na území druhej zmluvnej strany, predchádzajúcom rozhodnutiu o previerke personálnej bezpečnosti alebo previerke priemyselnej bezpečnosti.

(2) Zmluvné strany si uznajú previerky personálnej bezpečnosti a previerky priemyselnej bezpečnosti v súlade s vnútroštátnym právnym poriadkom druhej zmluvnej strany. Bezpečnostné previerky sú ekvivalentné podľa článku 6.

(3) Príslušné bezpečnostné orgány si navzájom oznámia akékoľvek informácie o zmenách v previerkach personálnej bezpečnosti alebo previerkach priemyselnej bezpečnosti, najmä vo vzťahu k prípadom ich zrušenia alebo zníženia ich stupňa.

Článok 8
Klasifikácia, príjem a zmeny

(1) Prijímajúca zmluvná strana označí prijaté, vyrobené alebo vyvinuté utajované skutočnosti vlastným stupňom utajenia v súlade s ekvivalenciou uvedenou v článku 6.

(2) Zmluvné strany sa navzájom informujú o všetkých následných zmenách v stupňoch utajenia poskytnutých utajovaných skutočností.

(3) Prijímajúca zmluvná strana a/alebo jej právnické osoby neznížia stupeň utajenia ani neodtajnia prijaté utajované skutočnosti bez predchádzajúceho písomného súhlasu odovzdávajúcej zmluvnej strany.

Článok 9
Preklad, rozmnožovanie a zničenie

(1) Utajované skutočnosti označené stupňom PRÍSNE TAJNÉ/SECRETO/TOP SECRET sa prekladajú alebo rozmnožujú len s písomným súhlasom príslušného bezpečnostného orgánu odovzdávajúcej zmluvnej strany.

(2) Preklady a kópie utajovaných skutočností sa vykonajú v súlade s nasledovnými zásadami:

a) fyzické osoby majú previerku personálnej bezpečnosti umožňujúcu prístup k utajovaným skutočnostiam príslušného stupňa utajenia,
b) preklady a kópie sa označia a ochraňujú rovnako ako originály,
c) preklady a počet kópií je obmedzený úradnou potrebou,
d) preklady majú príslušnú poznámku v jazyku, do ktorého sa preklad vykonáva, označujúcu, že obsahuje utajované skutočnosti prijaté od odovzdávajúcej zmluvnej strany.

(3) Utajované skutočnosti označené stupňom PRÍSNE TAJNÉ/SECRETO/TOP SECRET sa nezničia ale vrátia sa príslušnému bezpečnostnému orgánu odovzdávajúcej zmluvnej strany.

(4) Utajované skutočnosti označené stupňom TAJNÉ/RESERVADO/SECRET možno zničiť po poskytnutí písomného súhlasu odovzdávajúcej zmluvnej strany.

(5) Utajované skutočnosti označené stupňom DÔVERNÉ/CONFIDENCIAL/ CONFIDENTIAL a nižšieho stupňa utajenia možno zničiť v súlade s vnútroštátnym právnym poriadkom.

Článok 10
Poskytnutie utajovaných skutočností medzi zmluvnými stranami

(1) Utajované skutočnosti sa medzi zmluvnými stranami zvyčajne poskytujú diplomatickou cestou.

(2) Ak by bolo použitie diplomatickej cesty nepraktické alebo by neúmerne oddialilo príjem utajovaných skutočností, možno ich zaslať prostredníctvom osoby s príslušnou previerkou personálnej bezpečnosti, splnomocnenej certifikátom kuriéra vydaným zmluvnou stranou poskytujúcou utajované skutočnosti.

(3) Zmluvné strany môžu utajované skutočnosti zasielať elektronicky v súlade s bezpečnostnými postupmi, na ktorých sa vzájomne dohodnú príslušné bezpečnostné orgány.

(4) Na dodaní veľkého množstva alebo utajovaných skutočností veľkých rozmerov sa príslušné bezpečnostné orgány dohodnú od prípadu k prípadu.

(5) Prijímajúca zmluvná strana potvrdí príjem utajovaných skutočností a poskytne ich používateľom.

Článok 11
Bezpečnostné opatrenia

(1) Ak jedna zmluvná strana mieni uzatvoriť utajovaný kontrakt s kontrahentom z druhej zmluvnej strany, alebo ak mieni poveriť jedného z vlastných kontrahentov, aby uzatvoril utajovaný kontrakt na území druhej zmluvnej strany, získa prostredníctvom svojho príslušného bezpečnostného orgánu v rámci utajovaného projektu predchádzajúce písomné uistenie príslušného bezpečnostného orgánu druhej zmluvnej strany, že navrhovaný kontrahent má potvrdenie o priemyselnej bezpečnosti na príslušný stupeň utajenia.

(2) Každý subkontrahent musí splniť rovnaké bezpečnostné záväzky ako kontrahent.

(3) Akonáhle sa začnú predkontraktné rokovania medzi právnickou osobou so sídlom na území jednej zmluvnej strany a inou právnickou osobou so sídlom na území druhej zmluvnej strany, s cieľom podpísať zmluvné nástroje, zmluvné strany sa prostredníctvom príslušných bezpečnostných orgánov informujú o stupňoch utajenia daných utajovaným skutočnostiam, o ktoré v predkontraktnom rokovaní ide.

(4) Každý utajovaný kontrakt uzavretý v súlade s touto dohodou obsahuje príslušný bezpečnostný odsek identifikujúci:

a) záväzok kontrahenta zabezpečiť, že jeho priestory majú adekvátne podmienky pre zaobchádzanie a uchovávanie utajovaných skutočností príslušného stupňa utajenia,
b) záväzok kontrahenta zabezpečiť, že osoby vykonávajúce povinnosti vyžadujúce prístup k utajovaným skutočnostiam majú previerku personálnej bezpečnosti príslušného stupňa,

c) záväzok kontrahenta zabezpečiť, že všetky osoby s prístupom k utajovaným skutočnostiam boli informované o svojej zodpovednosti vo vzťahu k ochrane utajovaných skutočností v súlade s vnútroštátnym právnym poriadkom,
d) záväzok kontrahenta uskutočňovať periodické bezpečnostné kontroly svojich priestorov,
e) zoznam utajovaných skutočností a oblastí, v ktorých môžu utajované skutočnosti vzniknúť,
f) postup pre oznamovanie zmien v stupni utajenia utajovaných skutočností,
g) komunikačné kanály a prostriedky elektronického prenosu,
h) postup pre prepravu utajovaných skutočností,
i) príslušné poverené fyzické osoby alebo právnické osoby zodpovedné za koordináciu ochrany utajovaných skutočností, ktorých sa utajovaný kontrakt týka,
j) povinnosť oznámiť akúkoľvek skutočnú alebo predpokladanú stratu, prezradenie alebo ohrozenie utajovaných skutočností.

(5) Kópia bezpečnostného odseku každého utajovaného kontraktu sa postúpi príslušnému bezpečnostnému orgánu zmluvnej strany, kde sa má práca vykonať, čo umožní adekvátny dozor nad bezpečnosťou a riadenie.

(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. Oznam o návšteve sa zašle aspoň dvadsať dní vopred.

Článok 12
Návštevy

(1) Návštevy zahŕňajúce prístup štátnych príslušníkov jednej zmluvnej strany k utajovaným skutočnostiam druhej zmluvnej strany sa uskutočnia na základe predchádzajúceho písomného súhlasu od príslušného bezpečnostného orgánu hostiteľskej strany.

(2) Návštevy zahŕňajúce prístup k utajovaným skutočnostiam povolí jedna zmluvná strana návštevníkom druhej zmluvnej strane len ak:

a) majú previerku personálnej bezpečnosti príslušného stupňa od príslušného bezpečnostného orgánu vysielajúcej strany,
b) sú oprávnení prijať alebo mať prístup k utajovaným skutočnostiam v súlade s vnútroštátnym právnym poriadkom svojej zmluvnej strany.

(3) Príslušný bezpečnostný orgán zmluvnej strany, ktorá prijme žiadosť o návštevu, žiadosť posúdi, rozhodne o nej a svoje rozhodnutie oznámi príslušnému bezpečnostnému orgánu žiadajúcej zmluvnej strany.

(4) Návštevy zahŕňajúce prístup štátnych príslušníkov tretieho štátu k utajovaným skutočnostiam sa povolia len na základe spoločnej dohody zmluvných strán.

(5) Príslušný bezpečnostný orgán vysielajúcej strany upovedomí o plánovanej návšteve príslušný bezpečnostný orgán hostiteľskej strany žiadosťou o návštevu doručenou aspoň tridsať dní pred uskutočnením návštevy.

(6) V súrnych prípadoch sa žiadosť o návštevu zašle aspoň sedem dní vopred.

(7) Žiadosť o návštevu obsahuje:

a) meno a priezvisko návštevníka, miesto a dátum narodenia, štátnu príslušnosť, číslo pasu alebo identifikačnej karty,
b) názov spoločnosti alebo inej právnickej osoby, ktoré návštevník zastupuje alebo ku ktorým patrí,
c) názov a adresa spoločnosti alebo inej právnickej osoby, ktoré majú byť navštívené,
d) potvrdenie o previerke personálnej bezpečnosti návštevníka a jej platnosti,
e) predmet a účel návštevy alebo návštev,
f) predpokladaný dátum a trvanie návštevy alebo návštev, o ktoré sa žiada. V prípade opakovaných návštev sa uvedie aj ich celkové trvanie,
g) meno a telefónne číslo kontaktnej osoby v spoločnosti alebo inej právnickej osobe, kde má byť návšteva uskutočnená, predchádzajúce kontakty a akékoľvek iné informácie nápomocné pri odôvodnení návštevy alebo návštev,
h) dátum, podpis a odtlačok úradnej pečiatky príslušného bezpečnostného orgánu.

(8) Po odsúhlasení návštevy príslušný bezpečnostný orgán hostiteľskej zmluvnej strany poskytne kópiu žiadosti o návštevu bezpečnostným zamestnancom spoločnosti alebo inej právnickej osoby, kde sa má návšteva uskutočniť.

(9) Platnosť povolenia návštevy nepresiahne jeden rok.

(10) Pre akýkoľvek projekt, program alebo kontrakt sa zmluvné strany môžu dohodnúť na zoznamoch osôb oprávnených zúčastniť sa opakovaných návštev. Takéto zoznamy sú platné spočiatku jeden rok.

(11) Po schválení týchto zoznamov zmluvnými stranami sa termíny konkrétnych návštev dohodnú s príslušnými kontaktnými osobami v spoločnosti alebo inej právnickej osobe, ktoré majú tieto osoby navštíviť v súlade s dohodnutými termínmi a podmienkami.

Článok 13
Porušenie a ohrozenie bezpečnosti

(1) V prípade porušenia alebo ohrozenia bezpečnosti, ktoré má za následok isté alebo predpokladané ohrozenie utajovanej skutočnosti pochádzajúcej alebo prijatej z druhej zmluvnej strany, alebo podozrenia, že utajovaná skutočnosť bola prezradená neoprávneným osobám, príslušný bezpečnostný orgán zmluvnej strany, kde k porušeniu alebo ohrozeniu došlo, upovedomí čo najskôr príslušný bezpečnostný orgán druhej zmluvnej strany a vykoná príslušné vyšetrovanie.

(2) Ak k porušeniu alebo ohrozeniu bezpečnosti dôjde v štáte inom ako sú zmluvné strany, príslušný bezpečnostný orgán odovzdávajúcej zmluvnej strany koná podľa odseku 1.

(3) Druhá zmluvná strana pri vyšetrovaní na žiadosť spolupracuje.

(4) V každom prípade druhá zmluvná strana sa upovedomí o výsledkoch vyšetrovania a zašle sa jej konečná správa o príčinách a rozsahu škody.

Článok 14
Náklady

Každá zmluvná strana znáša vlastné náklady vynaložené v súvislosti s aplikáciou a dozorom nad všetkými aspektmi tejto dohody.

Článok 15
Riešenie sporov

Akýkoľvek spor ohľadom výkladu alebo aplikácie opatrení stanovených touto dohodou sa rieši diplomatickou cestou, ak nedôjde k dohode prostredníctvom príslušných bezpečnostných orgánov.

Článok 16
Zmeny

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

(2) Zmeny a dodatky nadobudnú platnosť v súlade s článkom 18.

Článok 17
Trvanie a ukončenie platnosti

(1) Táto dohoda sa uzatvára na neurčitý čas.

(2) Každá zmluvná strana môže vypovedať túto dohodu písomným oznámením druhej zmluvnej strane diplomatickou cestou.

(3) Vypovedanie dohody nadobudne platnosť šesť mesiacov po dátume doručenia príslušného oznámenia.

(4) Napriek vypovedaniu dohody, všetky utajované skutočnosti poskytnuté, vyrobené alebo vyvinuté podľa tejto dohody sa budú naďalej chrániť v súlade s týmito ustanoveniami, kým odovzdávajúca zmluvná strana nezbaví prijímajúcu zmluvnú stranu tohto záväzku.

Článok 18
Nadobudnutie platnosti

Táto dohoda nadobudne platnosť v prvý deň druhého mesiaca po prijatí posledného písomného oznámenia zaslaného diplomatickou cestou potvrdzujúceho, že boli splnené všetky vnútroštátne podmienky ustanovené pre nadobudnutie platnosti.

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

Dané v Bratislave, dňa 20. januára 2009 vo dvoch pôvodných vyhotoveniach, každé v slovenskom, španielskom a anglickom jazyku, pričom každý text má rovnakú platnosť.

Za Slovenskú republiku	**Za Španielske kráľovstvo**
František Blanárik riaditeľ Národného bezpečnostného úradu Slovenská republika	**José Ángel López Jorrin** veľvyslanec Španielskeho kráľovstva v Slovenskej republike

Agreement

on the Mutual Protection of

Classified Information

between

the Slovak Republic

and

the Kingdom of Spain

The Slovak Republic
and
the Kingdom of Spain

Hereinafter referred to as "the Parties",

Recognising the need of both Parties to guarantee protection of the Classified Information exchanged between them within the scope of the negotiations and cooperation agreements concluded, or to be concluded, as well as other contractual instruments of both, public or private organizations of the Parties;

Desiring to create a set of rules on mutual protection of Classified Information exchanged between the Parties,

Agree as follows:

Article 1

Object

This Agreement establishes the security rules applicable to all contractual instruments, which envisage the transmission of Classified Information, signed or to be signed between the Competent Security Authorities of both Parties or by companies or other legal entities duly authorized to that end.

Article 2

Scope of Application

1. This Agreement sets out procedures for the protection of Classified Information exchanged between the Parties.
2. Either Party shall not invoke this Agreement in order to obtain Classified Information the other Party has received from any Third Party.

Article 3

Definitions

For the purposes of this Agreement:

a) **"Classified Information"** means the information and materials, regardless of their form or nature, determined to require protection against unauthorised disclosure, which has been so designated by security classification;

b) **"Competent Security Authority"** means the National Security Authority/ Designated Security Authority designated by a Party as being responsible for the implementation and supervision of this Agreement;

c) **"Originating Party"** means the Party, which releases Classified Information to the other Party;

d) **"Receiving Party"** means the Party which Classified Information is released to by the other Party;

e) **"Third Party"** means any international organisation or state that is not Party to this Agreement;

f) **"Classified Contract"** means an agreement between two or more Contractors creating and defining enforceable rights and obligations between them, which contains or involves Classified Information;

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

h) **"Personnel Security Clearance"** means a certification provided by the Competent Security Authority that an individual is eligible to have access to Classified Information, in accordance with the respective national legislation;

i) **"Facility Security Clearance"** means a certification provided by the Competent Security Authority that, from a security point of view, a facility has the physical and organisational capability to use and store Classified Information, in accordance with the respective national legislation;

j) **"Need-to-know"** means that access to Classified Information may only be granted to a person who has a verified requirement for knowledge of, or possession of it in order to perform his/her official and professional duties, within the framework of which it was released to the Receiving Party.

Article 4

Competent Security Authorities

1. The Competent Security Authorities for the application of this Agreement are:

For the Slovak Republic:
National Security Authority

For the Kingdom of Spain:
Secretary of State, Director of the National Intelligence Centre
National Security Office

2. The Parties shall inform each other, through diplomatic channels, of any modification concerning their Competent Security Authorities.

Article 5

Security Principles

1. The protection and use of the Classified Information exchanged between the Parties is ruled by the following principles:

a) The Receiving Party shall assign to the received Classified Information the level of protection equivalent to the marking expressly given to the Classified Information by the Originating Party;

b) The access to Classified Information is restricted to persons who, in order to perform their duties, need to have access to the Classified Information, on a "Need-to-know" basis, have a Personnel Security Clearance appropriate to the level of security classification of the Classified Information to be accessed or above, and were authorized by the Competent Security Authorities;

c) The Receiving Party shall not transmit the Classified Information to any Third Party, any individual or legal entity, of any Third State, without prior written approval from the Originating Party;

d) The transmitted Classified Information may not be used for any purpose other than the one that it was transmitted for, in accordance with this Agreement;

2. In order to achieve and maintain comparable security standards, the Competent Security Authorities shall, on request, provide each other with information about their security standards, procedures and practices in the field of protection of Classified Information.

3. Parties shall inform of the existence of this Agreement whenever Classified Information is involved.

4. Parties shall ensure that everyone receiving Classified Information duly complies with the obligations of this Agreement.

Article 6

Security Classifications and Equivalences

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in their national legislations:

Slovak Republic	Kingdom of Spain	Equivalent in English
PRÍSNE TAJNÉ	SECRETO	TOP SECRET
TAJNÉ	RESERVADO	SECRET
DÔVERNÉ	CONFIDENCIAL	CONFIDENTIAL
VYHRADENÉ	DIFUSIÓN LIMITADA	RESTRICTED

Article 7

Assistance in Vetting Procedures

1. On request, the Competent Security Authorities of the Parties, taking into account their national legislation, shall assist each other during the vetting procedures of their citizens living or facilities located in the territory of the other Party, preceding the issue of the Personnel Security Clearance or Facility Security Clearance.

2. The Parties shall recognise the Personnel and Facility Security Clearances in accordance with the national legislation of the other Party. The equivalence of the security clearances shall be in compliance with Article 6.
3. The Competent Security Authorities shall communicate to each other any information related to changes of the Personnel and Facility Security Clearances, particularly concerning cases of withdrawal or downgrading of their security classification level.

Article 8

Classification, Reception and Alterations

1. The Receiving Party shall mark the received, produced or developed Classified Information with its own security classification, equivalent in accordance with Article 6.
2. The Parties shall mutually inform each other about all subsequent security classification alterations of the transmitted Classified Information.
3. The Receiving Party and/or its legal entities shall neither downgrade nor declassify the received Classified Information without the prior written approval of the Originating Party.

Article 9

Translation, Reproduction and Destruction

1. Classified Information marked PRÍSNE TAJNÉ/SECRETO/ TOP SECRET shall be translated or reproduced only upon the written approval of the Competent Security Authority of the Originating Party.

2. Translations and reproductions of Classified Information shall be made in accordance with the following principles:
    a) The individuals shall hold a Personnel Security Clearance enabling them access to Classified Information of relevant security classification level;
    b) The translations and the reproductions shall be marked and placed under the same protection as the original;
    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 into which they are translated indicating that they contain Classified Information received from the Originating Party.

3. Classified Information marked PRÍSNE TAJNÉ/ SECRETO/ TOP SECRET shall not be destroyed but shall be returned to the Competent Security Authority of the Originating Party.

4. Classified Information marked TAJNÉ/ RESERVADO/ SECRET shall be destroyed with prior written approval of the Originating Party.

5. Classified Information marked up to DÔVERNÉ/ CONFIDENCIAL/ CONFIDENTIAL shall be destroyed in accordance with the national legislation.

Article 10

Transmission between the Parties

1. The Classified Information shall normally be transmitted between the Parties through diplomatic channels.
2. If the use of such channels would be impractical or unduly delay receipt of the Classified Information, transmissions may be undertaken by appropriately security cleared personnel empowered with a courier certificate issued by the Party transmitting the Classified Information.
3. The Parties may transmit Classified Information by electronic means in accordance with security procedures mutually approved on by the Competent Security Authorities.
4. Delivery of large items or quantities of Classified Information arranged on a case-by-case basis shall be approved on by both Competent Security Authorities.
5. The Receiving Party shall confirm the reception of the Classified Information and shall disseminate it to the users.

Article 11

Security Measures

1. One Party, wishing to place a Classified Contract with a Contractor of the other Party, or wishing to authorise one of its own Contractors to place a Classified Contract in the territory 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 other Party that the proposed Contractor holds a Facility Security Clearance enabling access to Classified Information of relevant security classification level.

2. Any subcontractor must fulfil the same security obligations as the Contractor.
3. When pre-contractual negotiations begin between a legal entity located in the territory of one Party and another legal entity located in the territory of the other Party, aiming at signing of contractual instruments, the Parties shall inform each other through their Competent Security Authorities of the security classification given to the Classified Information involved in the pre-contractual negotiations.
4. Every Classified Contract concluded in accordance with this Agreement shall include an appropriate security section identifying:

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 appropriate level of Personnel Security Clearance is granted to persons who perform duties requiring access to Classified Information;

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) Classification guide and list of Classified Information;

f) Procedure for the communication of changes in the security classification level of Classified Information;

g) Communication channels and electronic means for transmission;

h) Procedure for the transportation of Classified Information;

i) Appropriate authorised individuals or legal entities responsible for the co-ordination of the safeguarding of Classified Information related to the Classified Contract;

j) An obligation to notify any actual or suspected loss, leak or compromise of the Classified Information.

5. Copy of the security section of any Classified Contract shall be forwarded to the Competent Security Authority 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 analyse 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 12
Visits

1. Visits entailing access to Classified Information by nationals from one Party to the other Party are subject to prior written approval given by the Competent Security Authority of the host Party.

2. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they have been:

a) Granted appropriate Personnel Security Clearance by the Competent Security Authority of the sending Party;

b) Authorised to receive or to have access to Classified Information in accordance with their national legislation.

3. The Competent Security Authority of the Party that receives the request for visit, examines and decides on the request and shall inform of its decision the Competent Security Authority of the requesting Party.
4. Visits entailing access to Classified Information by nationals from a third State shall only be authorized by a common agreement of the Parties.
5. The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least thirty days before taking place.
6. In urgent cases, the request for visit shall be sent at least seven days before.
7. The request for visit shall include:
    a) Visitor's first and last name, place and date of birth, nationality, passport or ID card number;
    b) Name of the company or other legal entity the visitor represents or to which the visitor belongs;
    c) Name and address of the company or other legal entity to be visited;
    d) Confirmation of the visitor's Personnel Security Clearance and its validity;
    e) Object and purpose of the visit or visits;
    f) Expected date and duration of the requested visit or visits. In case of recurring visits the total period covered by the visits should be stated;
    g) Name and phone number of the point of contact at the company or other legal entity to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;
    h) The date, signature and stamping of the official seal of the Competent Security Authority.
8. Once the visit has been approved the Competent Security Authority of the host Party shall provide a copy of the request for visit to the security officers of the company or other legal entity to be visited.
9. The validity of visit approval shall not exceed one year.
10. For any project, program or contract the Parties may agree to establish lists of individuals authorized to make recurring visits. The lists are valid for an initial period of one year.
11. Once the lists have been approved by the Parties, the terms of the respective visits shall be directly arranged with the appropriate points of contact in the company or other legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

Article 13

Breach and Compromise of Security

1. In case of breach or compromise of security that results in an actual or suspected compromise of Classified Information originated by or released from the other Party or suspicion that Classified Information has been disclosed to unauthorised

persons, the Competent Security Authority of the Party where the breach or compromise occurs shall inform the Competent Security Authority of the other Party, as soon as possible, and carry out the appropriate investigation.

2. If a breach or compromise of security occurs in a state other than the Parties, the Competent Security Authority of the despatching Party shall take the actions prescribed in Paragraph 1.
3. The other Party shall, upon request, co-operate in the investigation.
4. In any case, the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

Article 14

Expenses

Each Party shall bear its own expenses incurred in connection with the application and supervision of all aspects of this Agreement.

Article 15

Settlement of Disputes

Any dispute concerning 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 16

Amendments

1. This Agreement may be amended or supplemented anytime on the basis of mutual written approval of the Parties.

2. The amendments and supplements shall enter into force according to Article 18.

Article 17

Duration and Termination

1. This Agreement is concluded for an indeterminate period of time.
2. Each Party may, at any time, terminate this Agreement by written notification delivered to the other Party through diplomatic channels.
3. The termination shall take effect six months after the receipt day of the respective notification.
4. Notwithstanding the termination, all Classified Information transmitted, produced or developed pursuant to this Agreement shall continue to be protected in

accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

Article 18
Entry into Force

This Agreement shall enter into force on the first day of the second month after receipt of the last written notification of the Parties through diplomatic channels, confirming the fulfilment of the national procedures for its entering into force.

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

Done at Bratislava, on January 20, 2009 in two originals, each one in Slovak, Spanish and English language, each text being equally authentic.

For the Slovak Republic	For the Kingdom of Spain
František Blanárik Director of the National Security Authority Slovak Republic	**José Ángel López Jorrin** Ambassador of the Kingdom of Spain to the Slovak Republic