

DOHODA

MEDZI

SLOVENSKOU REPUBLIKOU

A

PORTUGALSKOU REPUBLIKOU

O VÝMENE A VZÁJOMNEJ

OCHRANE

UTAJOVANÝCH SKUTOČNOSTÍ

Slovenská republika
a
Portugalská republika

(ďalej len "zmluvné strany"),

uznávajúc potrebu oboch zmluvných strán zabezpečiť ochranu utajovaných skutočností vymieňaných medzi oboma zmluvnými stranami, fyzickými osobami alebo právnickými osobami v ich jurisdikcii v rámci dohôd o spolupráci alebo kontraktov už uzavretých alebo takých, ktoré sa uzavrú v budúcnosti,

želajúc si vytvoriť sústavu pravidiel vzájomnej ochrany utajovaných skutočností vymieňaných medzi zmluvnými stranami,

sa dohodli takto:

Článok 1
Predmet

Táto dohoda ustanovuje pravidlá bezpečnosti týkajúce sa všetkých dohôd o spolupráci alebo kontraktov, či už podpísaných alebo plánovaných na podpis v budúcnosti, ktoré predpokladajú výmenu utajovaných skutočností, medzi príslušnými národnými orgánmi oboch zmluvných strán alebo fyzickými osobami alebo právnickými osobami na to riadne oprávnenými.

Článok 2
Rozsah uplatnenia

- (1) Táto dohoda ustanovuje postupy pre ochranu utajovaných skutočností vymieňaných medzi zmluvnými stranami, alebo fyzickými osobami alebo právnickými osobami v ich jurisdikcii.
- (2) Žiadna zmluvná strana sa nesmie dovolávať tejto dohody, aby získala utajovanú skutočnosť, ktorú prijala druhá zmluvná strana od strany tretej.

Článok 3
Vymedzenie pojmov

Pre účely tejto dohody:

- a) utajovaná skutočnosť je informácia, bez ohľadu na svoju formu, povahu a spôsob prenosu, ktorá podľa príslušného platného práva vyžaduje ochranu pred neoprávneným poskytnutím, a ktorá je označená príslušným stupňom utajenia,

- b) porušenie bezpečnosti je konanie alebo opomenutie konania, úmyselné alebo náhodné, v rozpore s príslušným platným právom, ktorého výsledkom je skutočné alebo možné ohrozenie utajovanej skutočnosti,
- c) ohrozenie utajovanej skutočnosti je situácia, keď v dôsledku porušenia bezpečnosti stratila utajovaná skutočnosť svoju dôvernosť, integritu alebo dostupnosť,
- d) národný bezpečnostný orgán je orgán určený zmluvnou stranou ako zodpovedný za dozor a vykonávanie tejto dohody,
- e) poskytujúca strana je zmluvná strana, ktorá odovzdáva utajovanú skutočnosť druhej zmluvnej strane,
- f) prijímajúca strana je zmluvná strana, ktorá prijíma utajovanú skutočnosť od druhej zmluvnej strany,
- g) tretia strana je akákoľvek medzinárodná organizácia alebo štát, ktorý nie je zmluvnou stranou tejto dohody,
- h) kontrahent je fyzická osoba alebo právnická osoba s právnou spôsobilosťou uzatvoriť kontrakt,
- i) utajovaný kontrakt je dohoda medzi dvoma alebo viacerými kontrahentmi, vytvárajúca a definujúca vymáhateľné práva a záväzky medzi nimi, ktorá obsahuje alebo zahŕňa prístup k utajovaným skutočnostiam,
- j) previerka personálnej bezpečnosti je zistenie národného bezpečnostného orgánu, že fyzická osoba je spôsobilá mať prístup k utajovaným skutočnostiam v súlade s príslušným platným právom,
- k) previerka priemyselnej bezpečnosti je zistenie národného bezpečnostného orgánu, že z bezpečnostného hľadiska je právnická osoba fyzicky a organizačne schopná skladovať a zaobchádzať s utajovanými skutočnosťami v súlade s príslušným platným právom,
- l) need-to-know znamená, že prístup k utajovaným skutočnostiam možno udeliť len osobe, ktorá má odôvodnenú potrebu poznať alebo mať ich pre plnenie svojich povinností,
- m) bezpečnostné pokyny pre projekt sú súhrnom bezpečnostných požiadaviek, ktoré sú použité na konkrétny projekt.

Článok 4

Národné bezpečnostné orgány

(1) Národné bezpečnostné orgány zodpovedné za vykonávanie tejto dohody sú:

za Slovenskú republiku
Národný bezpečnostný úrad

za Portugalskú republiku
Národný bezpečnostný úrad
Prezídium výboru ministrov

- (2) Národné bezpečnostné orgány si navzájom poskytnú oficiálne kontaktné údaje.
- (3) Národné bezpečnostné orgány sa navzájom informujú o príslušnom platnom práve upravujúcom ochranu utajovaných skutočností.
- (4) Národné bezpečnostné orgány si, s cieľom zabezpečiť úzku spoluprácu pri implementácii tejto dohody, navzájom môžu poskytnúť konzultácie na žiadosť jedného z nich.

Článok 5 Pravidlá bezpečnosti

Ochrana a použitie utajovaných skutočností vymieňaných medzi zmluvnými stranami sa riadi nasledujúcimi pravidlami:

- a) prijímajúca strana prizná prijatej utajovanej skutočnosti úroveň ochrany ekvivalentnú stupňu utajenia výslovne určenému utajovanej skutočnosti poskytujúcou stranou,
- b) prijímajúca strana nezníži ani nezruší stupeň utajenia prijatej utajovanej skutočnosti bez predchádzajúceho písomného súhlasu poskytujúcej strany,
- c) prístup k utajovaným skutočnostiam je obmedzený na osoby, ktoré ho potrebujú na výkon svojich povinností, majú prístup k utajovaným skutočnostiam na princípe need-to-know a majú previerku personálnej bezpečnosti v súlade s príslušným platným právom.

Článok 6 Ekvivalencia stupňov utajenia a stupňov bezpečnostných previerok

Zmluvné strany sa dohodli, že nasledujúce stupne utajenia a stupne bezpečnostných previerok sú ekvivalentné a zodpovedajú stupňom utajenia a stupňom bezpečnostných previerok uvedeným v príslušnom platnom práve:

Pre Slovenskú republiku	Pre Portugalskú republiku	Ekvivalent v angličtine
PRÍSNE TAJNÉ	MUITO SECRETO	TOP SECRET
TAJNÉ	SECRETO	SECRET
DÔVERNÉ	CONFIDENCIAL	CONFIDENTIAL
VYHRADENÉ	RESERVADO	RESTRICTED

Článok 7

Postup pri bezpečnostných previerkach

- (1) Národné bezpečnostné orgány zmluvných strán si na žiadosť a s ohľadom na príslušné platné právo navzájom pomôžu počas vykonávania previerok svojich občanov žijúcich alebo právnických osôb majúcich sídlo na území druhej zmluvnej strany pred vydaním previerky personálnej bezpečnosti a previerky priemyselnej bezpečnosti.
- (2) Zmluvné strany si navzájom uznajú previerky personálnej bezpečnosti a previerky priemyselnej bezpečnosti vydané v súlade s príslušným platným právom druhej zmluvnej strany.
- (3) Národné bezpečnostné orgány si navzájom oznámia každú zmenu súvisiacu s previerkami personálnej bezpečnosti a previerkami priemyselnej bezpečnosti.

Článok 8

Označovanie

- (1) Prijímajúca strana označí prijatú utajovanú skutočnosť vlastným označením stupňa utajenia v súlade s ekvivalentmi podľa článku 6.
- (2) Zmluvné strany sa navzájom informujú o všetkých následných zmenách stupňa utajenia odovzdaných utajovaných skutočností.

Článok 9

Preklad, rozmnožovanie a zničenie

- (1) Preklady a kópie utajovaných skutočností sa uskutočnia v súlade s nasledujúcimi postupmi:
 - a) fyzické osoby budú náležite bezpečnostne preverené,
 - b) preklady a kópie sa označia a ochraňujú rovnako ako originál,
 - c) preklady a počet kópií sú obmedzené úradnou potrebou,

- d) preklady majú príslušnú poznámku v jazyku prekladu označujúcu, že obsahujú utajovanú skutočnosť prijatú od poskytovajúcej strany.
- (2) Utajované skutočnosti označené ako TAJNÉ /SECRETO a vyššie sa prekladajú alebo rozmnožujú iba s písomným súhlasom národného bezpečnostného orgánu poskytovajúcej strany v súlade s príslušným platným právom.
- (3) Utajované skutočnosti označené ako TAJNÉ /SECRETO a vyššie sa nezničia, ale vrátia sa národnému bezpečnostnému orgánu poskytovajúcej strany.
- (4) Utajované skutočnosti s označením až po DÔVERNÉ /CONFIDENCIAL sa zničia v súlade s príslušným platným právom.
- (5) Ak by bolo nemožné chrániť a vrátiť utajované skutočnosti vyrobené alebo odovzdané podľa tejto dohody, utajované skutočnosti sa bezodkladne zničia. Prijímajúca strana upovedomí národný bezpečnostný orgán poskytovajúcej strany o zničení čo možno najskôr.

Článok 10

Odobzdanie utajovaných skutočností

- (1) Utajované skutočnosti sa odovzdávajú medzi zmluvnými stranami spravidla diplomatickou cestou.
- (2) Ak by bolo použitie diplomatickej cesty nepraktické alebo zbytočne oddialilo prijatie utajovaných skutočností, odovzdanie môže uskutočniť príslušne bezpečnostne preverený personál, náležite oprávnený poskytujúcou stranou.
- (3) Zmluvné strany môžu utajované skutočnosti odovzdať chránenými elektronickými prostriedkami, na ktorých sa dohodnú národné bezpečnostné orgány v súlade s príslušným platným právom.
- (4) Na odovzdaní utajovaných skutočností veľkých rozmerov alebo množstva sa od prípadu k prípadu dohodnú oba národné bezpečnostné orgány.
- (5) Národný bezpečnostný orgán prijímajúcej strany písomne potvrdí prijatie utajovanej skutočnosti.

Článok 11

Použitie utajovaných skutočností

- (1) Utajovaná skutočnosť sa použije výlučne na účel, na ktorý bola odovzdaná.
- (2) Každá zmluvná strana zabezpečí, že všetky fyzické osoby a právnické osoby, ktoré prijímajú utajované skutočnosti, konajú v súlade so záväzkami ustanovenými v tejto dohode.

- (3) Prijímajúca strana neodovzdá utajované skutočnosti tretej strane alebo akejkoľvek fyzickej osobe alebo právnickej osobe pod jurisdikciou tretieho štátu bez predchádzajúceho písomného súhlasu poskytovajúcej strany.

Článok 12

Utajované kontrakty

- (1) Národný bezpečnostný orgán jednej zmluvnej strany písomne potvrdí, že navrhovaný kontrahent je držiteľom príslušného potvrdenia o previerke priemyselnej bezpečnosti predtým, ako sa uzavrie alebo vykoná utajovaný kontrakt na území druhej zmluvnej strany.
- (2) Každý subkontrahent musí spĺňať tie isté bezpečnostné podmienky ako kontrahent.
- (3) Národný bezpečnostný orgán je zodpovedný za dozor a kontrolu kontrahenta v súlade so záväzkami podľa odseku 2.
- (4) Každý utajovaný kontrakt podpísaný medzi kontrahentmi zmluvných strán podľa ustanovení tejto dohody obsahuje príslušné bezpečnostné pokyny pre projekt s nasledujúcimi časťami:
- a) záväzok kontrahenta zabezpečiť, že osoby, ktoré potrebujú na vykonávanie svojich povinností prístup k utajovaným skutočnostiam, boli náležite bezpečnostne preverené,
 - b) záväzok kontrahenta zabezpečiť, aby všetky osoby s prístupom k utajovaným skutočnostiam boli informované o svojej zodpovednosti vo vzťahu k ochrane utajovaných skutočností v súlade s platným právom,
 - c) záväzok kontrahenta umožniť bezpečnostné inšpekcie svojich priestorov,
 - d) zoznam utajovaných skutočností a ich stupne utajenia,
 - e) postup pri oznámení zmien v stupňoch utajenia,
 - f) komunikačné kanály a prostriedky elektronického prenosu,
 - g) postup pri preprave utajovanej skutočnosti,
 - h) orgány zodpovedné za koordináciu ochrany utajovaných skutočností vo vzťahu k utajovanému kontraktu,
 - i) záväzok oznámiť každé skutočné alebo možné ohrozenie utajovanej skutočnosti.
- (5) Kópia bezpečnostných pokynov pre projekt každého utajovaného kontraktu sa postúpi národnému bezpečnostnému orgánu zmluvnej strany, kde sa

utajovaný kontrakt má vykonať, aby sa tak zabezpečil adekvátny dozor a kontrola.

- (6) Predstavitelia národných bezpečnostných orgánov sa môžu navštevovať s cieľom analýzy efektívnosti opatrení prijatých kontrahentom pri ochrane utajovaných skutočností, ktoré zahŕňajú utajovaný kontrakt.

Článok 13 **Návštevy**

- (1) Návštevy zahŕňajúce prístup štátnych príslušníkov jednej zmluvnej strany k utajovaným skutočnostiam druhej zmluvnej strany, sú predmetom predchádzajúceho písomného súhlasu národných bezpečnostných orgánov v súlade s príslušným platným právom.
- (2) Žiadosť o návštevu sa predkladá prostredníctvom národného bezpečnostného orgánu hostiteľskej zmluvnej strany a doručí sa najmenej 30 dní pred konaním návštevy alebo návštev.
- (3) V súrnych prípadoch sa žiadosť o návštevu predloží najmenej sedem dní vopred.
- (4) Návštevy, zahŕňajúce prístup k utajovaným skutočnostiam, povolí jedna zmluvná strana návštevníkom druhej zmluvnej strany len ak:
 - a) boli príslušne bezpečnostne preverení národným bezpečnostným orgánom žiadajúcej zmluvnej strany a
 - b) boli oprávnení prijať alebo mať prístup k utajovaným skutočnostiam na základe princípu need-to-know a v súlade s príslušným platným právom.
- (5) Národný bezpečnostný orgán zmluvnej strany, ktorá prijme žiadosť o návštevu, informuje národný bezpečnostný orgán žiadajúcej zmluvnej strany v čo najkratšom čase o svojom rozhodnutí.
- (6) Návštevy fyzických osôb z tretieho štátu zahŕňajúce prístup k utajovaným skutočnostiam poskytovajúcej strany povolí písomne národný bezpečnostný orgán poskytovajúcej strany.
- (7) Po schválení návštevy národný bezpečnostný orgán hostiteľskej zmluvnej strany poskytne kópiu žiadosti o návštevu bezpečnostným zamestnancom právnickej osoby, ktorá má byť navštívená.
- (8) Platnosť povolenia na návštevu neprekročí dvanásť mesiacov.
- (9) Zmluvné strany sa môžu dohodnúť na vytvorení zoznamov oprávnených osôb pre opakované návštevy. Takéto zoznamy sú platné dvanásť mesiacov.

(10) Po schválení zoznamov národnými bezpečnostnými orgánmi zmluvných strán sa dohodnú priamo podmienky konkrétnych návštev s právnickými osobami, ktoré majú byť navštívené.

(11) Žiadosť o návštevu obsahuje tieto údaje:

- a) meno a priezvisko, miesto a dátum narodenia, štátnu príslušnosť, číslo pasu alebo identifikačnej karty návštevníka,
- b) názov právnickej osoby, ktorú návštevník zastupuje alebo ku ktorej patrí,
- c) názov a adresa právnickej osoby, ktorá má byť navštívená,
- 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 a v prípade opakovaných návštev aj obdobie pokrývajúce všetky návštevy,
- g) meno a telefónne číslo kontaktnej osoby v právnickej osobe, ktorá má byť navštívená, predchádzajúce kontakty a každú inú informáciu užitočnú pri odôvodnení návštevy alebo návštev,
- h) dátum, podpis a odtlačok úradnej pečiatky príslušného národného bezpečnostného orgánu.

Článok 14

Porušenie bezpečnosti

- (1) V prípade porušenia bezpečnosti, súvisiaceho s utajovanými skutočnosťami pochádzajúcimi alebo prijatými od druhej zmluvnej strany, národný bezpečnostný orgán zmluvnej strany, kde k porušeniu došlo, informuje v čo najkratšom čase národný bezpečnostný orgán druhej zmluvnej strany a zabezpečí príslušné vyšetrovanie.
- (2) Ak k porušeniu dôjde počas odovzdávania v štáte, ktorý nie je zmluvnou stranou, národný bezpečnostný orgán odosielajúcej zmluvnej strany vykoná úkony podľa odseku 1.
- (3) Druhá zmluvná strana na základe žiadosti spolupracuje pri vyšetrovaní.
- (4) Druhá zmluvná strana je vždy písomne informovaná o výsledkoch vyšetrovania, vrátane príčin porušenia bezpečnosti, rozsahu škody a záveroch vyšetrovania.

Článok 15

Náklady

Každá zmluvná strana znáša vlastné náklady vzniknuté v súvislosti s vykonávaním a dohľadom nad všetkými aspektmi tejto dohody.

Článok 16

Urovnávanie sporov

Akýkoľvek spor ohľadom výkladu alebo vykonávania tejto dohody sa rieši rokovaniami.

Článok 17

Platnosť

Táto dohoda nadobudne platnosť tridsiatym (30) dňom odo dňa doručenia posledného písomného oznámenia zmluvných strán diplomatickou cestou, že boli splnené všetky vnútroštátne podmienky pre nadobudnutie platnosti tejto dohody.

Článok 18

Zmeny

- (1) Obe zmluvné strany môžu kedykoľvek túto dohodu zmeniť na základe vzájomného písomného súhlasu.
- (2) Zmeny nadobudnú platnosť podľa článku 17.

Článok 19

Platnosť a skončenie platnosti

- (1) Táto dohoda sa uzaviera na neurčitý čas.
- (2) Každá zmluvná strana môže kedykoľvek vypovedať dohodu písomným oznámením druhej zmluvnej strane diplomatickou cestou, pričom platnosť dohody skončí uplynutím šiestich mesiacov odo dňa prijatia oznámenia o výpovedi.
- (3) Napriek ukončeniu platnosti sa utajované skutočnosti odovzdané podľa tejto dohody naďalej ochraňujú v súlade s jej ustanoveniami, kým poskytujúca strana nezbaví prijímajúcu stranu tohto záväzku.

Článok 20 Registrácia

Zmluvná strana, na území ktorej je táto dohoda podpísaná, ju postúpi na registráciu na Sekretariát Organizácie Spojených národov v súlade s článkom 102 Charty Organizácie Spojených národov a upovedomí druhú zmluvnú stranu o ukončení tohto procesu, oznámiaac príslušné registračné číslo.

Riadne poverení zástupcovia zmluvných strán, dosvedčujúc uvedené, podpísali túto dohodu.

Dané v Bratislave, dňa 25. októbra 2007, v dvoch pôvodných vyhotoveniach, každé v slovenskom, portugalskom a anglickom jazykom, pričom všetky znenia sú autentické. V prípade rozdielnosti výkladu je rozhodujúce znenie v anglickom jazyku.

Za Slovenskú republiku

Za Portugalskú republiku

FRANTIŠEK BLANÁRIK

JOSÉ ERNST HENZLER VIEIRA BRANCO

**Riaditeľ
Národného bezpečnostného úradu**

**Veľvyslanec Portugalskej republiky
v Slovenskej republike**

AGREEMENT

BETWEEN

THE SLOVAK REPUBLIC

AND

THE PORTUGUESE REPUBLIC

CONCERNING

THE EXCHANGE AND THE MUTUAL

PROTECTION

OF CLASSIFIED INFORMATION

The Slovak Republic
and
the Portuguese Republic

Hereinafter referred to as the “Parties”,

Recognising the need of the Parties to guarantee the protection of the Classified Information exchanged between them, the individuals or legal entities in their jurisdiction, under co-operation arrangements or contracts concluded or to be concluded;

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

Agree as follows:

ARTICLE 1
Object

This Agreement sets out the security rules applicable to all cooperation arrangements or contracts, which envisage an exchange of Classified Information, concluded or to be concluded between the competent national authorities of both Parties or by individuals or legal entities duly authorized to that purpose.

ARTICLE 2
Scope of Application

1. This Agreement sets out procedures for the protection of Classified Information exchanged between the Parties, or the individuals or legal entities under their jurisdiction.
2. Either Party may not invoke this Agreement in order to obtain Classified Information that the other Party has received from a Third Party.

ARTICLE 3
Definitions

For the purposes of this Agreement:

- a) “Classified Information” means an information, regardless of its form, nature, and means of transmission, determined in accordance with the respective Law in force to require protection against unauthorised disclosure and which has been marked by appropriate security classification level;
- b) “Breach of Security” means an act or an omission, deliberate or accidental, contrary to the respective Law in force, which results in the actual or possible Compromise of Classified Information;

- c) "Compromise of Classified Information" means a situation when, due to a Breach of Security, Classified Information has lost its confidentiality, integrity or availability;
- d) "National Security Authority" means the authority designated by the Party as being responsible for the implementation and supervision of this Agreement;
- e) "Originating Party" means the Party which releases Classified Information to the other Party;
- f) "Receiving Party" means the Party which receives the Classified Information from the other Party;
- g) "Third Party" means any international organisation or state that is not a Party to this Agreement;
- h) "Contractor" means an individual or a legal entity possessing the legal capacity to conclude contracts;
- i) "Classified Contract" means an arrangement between two or more Contractors creating and defining enforceable rights and obligations between them, which contains or involves access to Classified Information;
- j) "Personnel Security Clearance" means a determination by the National Security Authority that an individual is eligible to have access to Classified Information, in accordance with the respective Law in force;
- k) "Facility Security Clearance" means a determination by the National Security Authority that, from a security point of view, a facility has the physical and organisational capability to handle and store Classified Information, in accordance with the respective Law in force;
- l) "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 their duties;
- m) "Project Security Instructions" means a compilation of security requirements, which are applied to a specific project.

ARTICLE 4

National Security Authorities

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

For the Slovak Republic:
National Security Authority

For the Portuguese Republic:
National Security Authority
Presidency of the Council of Ministers

2. The National Security Authorities shall provide each other with their official contact data.
3. The National Security Authorities shall inform each other of the respective Law in force regulating the protection of Classified Information.
4. In order to ensure close co-operation in the implementation of this Agreement, National Security Authorities may hold consultations at request of one of them.

ARTICLE 5 Security Rules

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

- a) The Receiving Party shall afford to the received Classified Information a level of protection equivalent to the security classification level given to the Classified Information by the Originating Party;
- b) The Receiving Party shall neither downgrade nor declassify the received Classified Information without the prior written consent of the Originating Party;
- c) The access to Classified Information shall be restricted to persons who, in order to perform their duties, have access to the Classified Information, on a Need-to-know basis and hold a Personnel Security Clearance in accordance with the respective Law in force.

ARTICLE 6 Equivalence of the Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the ones specified in the respective Law in force:

For the Slovak Republic	For the Portuguese Republic	Equivalent in English
PRÍSNE TAJNÉ	MUITO SECRETO	TOP SECRET
TAJNÉ	SECRETO	SECRET
DÔVERNÉ	CONFIDENCIAL	CONFIDENTIAL
VYHRADENÉ	RESERVADO	RESTRICTED

ARTICLE 7 Security Clearance Procedure

1. On request, the National Security Authorities of the Parties, taking into account their respective Law in force, shall assist each other during the clearance procedures of their nationals living or facilities located in the territory of the other Party, preceding the issue of the Personnel Security Clearance and the Facility Security Clearance.

2. The Parties shall recognise the Personnel Security Clearances and Facility Security Clearances issued in accordance with the Law in force of the other Party.
3. The National Security Authorities shall inform each other about any modifications regarding the Personnel Security Clearances and Facility Security Clearances.

ARTICLE 8

Marking

1. The Receiving Party shall mark the received Classified Information with its own security classification marking, in accordance with the equivalence referred to in Article 6.
2. The Parties shall inform each other about all subsequent classification alterations to the released Classified Information.

ARTICLE 9

Translation, Reproduction and Destruction

1. Translations and reproductions of Classified Information shall be made in accordance with the following procedures:
 - a) The individuals shall be appropriately security cleared;
 - 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 reproductions shall be limited to that required for official purposes;
 - d) The translations shall bear an appropriate note in the language of translation indicating that they contain Classified Information received from the Originating Party.
2. Classified Information marked as TAJNÉ /SECRETO and above shall be translated or reproduced only upon written permission of the National Security Authority of the Originating Party in accordance with the respective Law in force.
3. Classified Information marked as TAJNÉ /SECRETO and above shall not be destroyed but shall be returned to the National Security Authority of the Originating Party.
4. Classified Information marked up to DÔVERNÉ /CONFIDENCIAL shall be destroyed in accordance with the respective Law in force.
5. If it is impossible to protect and return Classified Information generated or transferred in accordance with this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

ARTICLE 10

Transmission of Classified Information

1. Classified Information shall normally be transmitted between the Parties through diplomatic channels.
2. If the use of the diplomatic channels would be impractical or unduly delay receipt of the Classified Information, transmission may be carried out by appropriately security cleared personnel, duly authorised by the Originating Party.
3. Classified Information may be transmitted via protected electronic means approved by the National Security Authorities in accordance with the respective Law in force.
4. The transmission of large items or quantities of Classified Information shall be approved on a case-by-case basis by both National Security Authorities.
5. The National Security Authority of the Receiving Party shall confirm in writing the receipt of the Classified Information.

ARTICLE 11

Use of Classified Information

1. The transmitted Classified Information shall be used only for the purpose it has been transmitted for.
2. Either Party shall ensure that all individuals and legal entities that receive Classified Information duly comply with the obligations established in this Agreement.
3. The Receiving Party shall not release the Classified Information to a Third Party or to any individual or legal entity under the jurisdiction of a third state, without prior written permission from the Originating Party.

ARTICLE 12

Classified Contracts

1. The National Security Authority of one Party shall confirm in writing before conclusion of a Classified Contract or its carrying out in the territory of the other Party, that the proposed Contractor holds an appropriate Facility Security Clearance certificate.
2. Any subcontractor must fulfil the same security obligations as the Contractor.
3. The National Security Authority shall be responsible for the supervision and control of the compliance of the Contractor with the commitments set in Paragraph 2.
4. Every Classified Contract concluded between Contractors of the Parties, under the provisions of this Agreement, shall include appropriate Project Security Instructions identifying the following aspects:

- a) Commitment of the Contractor to ensure that persons that require access to Classified Information to perform their duties have been appropriately secured cleared;
 - b) Commitment of the Contractor to ensure that all persons with access to Classified Information are informed of their responsibility related to protection of Classified Information, in accordance with the Law in force;
 - c) Commitment of the Contractor to allow security inspections of its premises;
 - d) List of Classified Information and the respective security classification levels;
 - e) Procedure for communication of alterations in the security classification levels;
 - f) Communication channels and means of electronic transmission;
 - g) Procedure for transportation of Classified Information;
 - h) Authorities competent for the co-ordination of the protection of Classified Information related to the Classified Contract;
 - i) An obligation to notify any actual or suspected Compromise of Classified Information.
5. Copy of the Project Security Instructions of any Classified Contract shall be forwarded to the National Security Authority of the Party where the Classified Contract is to be performed to allow adequate security supervision and control.
 6. Representatives of the National 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.

ARTICLE 13

Visits

1. Visits entailing access to Classified Information by nationals from one Party to the other Party are subject to prior written permission of the National Security Authorities in accordance with the respective Law in force.
2. The request for visit shall be submitted through the National Security Authority of the host Party and has to be received at least thirty days before the visit or visits take place.
3. In urgent cases, the request for visit shall be submitted at least seven days in advance.
4. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they have been:
 - a) Appropriately security cleared by the National Security Authority of the requesting Party; and

- b) Authorised to receive or to have access to Classified Information on a Need-to-know basis, in accordance with the respective Law in force.
5. The National Security Authority of the Party that receives the request for visit shall inform, as soon as possible, the National Security Authority of the requesting Party about the decision.
 6. Visits of individuals from a Third Party entailing access to Classified Information of the Originating Party shall be authorized in writing by the National Security Authority of the Originating Party.
 7. Once the visit has been approved, the National Security Authority of the host Party shall provide a copy of the request for visit to the security officers of the entity to be visited.
 8. The validity of the visit permission shall not exceed twelve months.
 9. Parties may agree to set up lists of authorized persons to make recurring visits. Those lists are valid for a period of twelve months.
 10. After the lists have been approved by the National Security Authorities the conditions of the specific visits shall be directly arranged with the entities to be visited.
 11. The request for visit shall entail the following information:
 - a) Visitor's first and last name, place and date of birth, nationality, passport or identification card number;
 - b) Name of the entity the visitor represents or to which the visitor belongs;
 - c) Name and address of the 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, and in case of recurring visits, the total period covered by the visits;
 - g) Name and phone number of the point of contact at the 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 National Security Authority.

ARTICLE 14

Breach of Security

1. In case of Breach of Security related to Classified Information originated by or received from the other Party, the National Security Authority of the Party

where the Breach of Security occurs shall inform the National Security Authority of the other Party, as soon as possible, and ensure the appropriate investigation.

2. If a Breach of Security occurs during transmission, in a State other than the Parties, the National Security Authority of the despatching Party shall take the actions prescribed in Paragraph 1.
3. The other Party shall, if required, co-operate in the investigation.
4. In any case, the other Party shall be informed of the results of the investigation, in writing, including the reasons for the Breach of Security, the extent of the damage and the conclusions of the investigation.

ARTICLE 15

Expenses

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

ARTICLE 16

Settlement of Disputes

Any dispute concerning the interpretation or application of this Agreement shall be settled through negotiations.

ARTICLE 17

Entry into Force

This Agreement shall enter into force on the thirtieth (30) day following the receipt of the last notification, in writing and through diplomatic channels, stating that all necessary internal requirements of both Parties for the entry into force have been fulfilled.

ARTICLE 18

Amendments

1. This Agreement may be amended on the basis of mutual written consent of the Parties.
2. The amendments shall enter into force according to Article 17.

ARTICLE 19

Duration and Termination

1. This Agreement is concluded for an indefinite period of time.

2. Either Party may terminate this Agreement at any time, by written notification through diplomatic channels, producing its effects six months after the date of its receipt by the other Party.
3. Notwithstanding the termination, all Classified Information transmitted according to this Agreement shall continue to be protected in compliance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

Article 20 Registration

The Party in whose territory this Agreement is signed shall transmit it for registration to the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, and shall notify the other Party of the conclusion of the proceeding, indicating the respective registration number.

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

Done at Bratislava on 25th October 2007, in two originals, each one in the Slovak Portuguese, and English languages, all texts being authentic. In case of any difference of interpretation the English text shall prevail.

For the Slovak Republic

For the Portuguese Republic

FRANTISEK BLANARIK

**JOSÉ ERNST HENZLER VIEIRA
BRANCO**

**Director
of the National Security Authority**

**Ambassador of the Portuguese Republic
to the Slovak Republic**