No. 47151

Slovakia
and
Spain

Agreement on the mutual protection of classified information between the Slovak Republic and the Kingdom of Spain. Bratislava, 20 January 2009

Entry into force: *1 January 2010 by notification, in accordance with article 18*

Authentic texts: *English, Slovak and Spanish*

Registration with the Secretariat of the United Nations: *Slovakia, 9 February 2010*

Slovaquie
et
Espagne

Accord entre la République slovaque et le Royaume d'Espagne relatif à la protection mutuelle des informations classifiées. Bratislava, 20 janvier 2009

Entrée en vigueur : *1er janvier 2010 par notification, conformément à l'article 18*

Textes authentiques : *anglais, slovaque et espagnol*

Enregistrement auprès du Secrétariat des Nations Unies : *Slovaquie, 9 février 2010*

[ENGLISH TEXT – TEXTE ANGLAIS]

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.

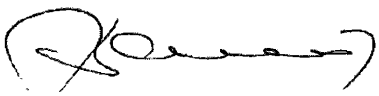
Article 18
Entry into Force

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.

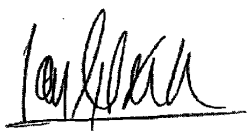
Done at Bratislava, on January 20, 2009 in two originals, each one in Slovak, Spanish and English language, each text being equally authentic.

For the Slovak Republic



František Blanárik
Director
of the National Security Authority
Slovak Republic

For the Kingdom of Spain



José Ángel López Jorrin
Ambassador
of the Kingdom of Spain
to the Slovak Republic

[SLOVAK TEXT – TEXTE SLOVAQUE]

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

František Blanárik
riaditeľ Národného bezpečnostného úradu
Slovenská republika

Za Španielske kráľovstvo

José Ángel López Jorrin
veľvyslanec Španielskeho kráľovstva
v Slovenskej republike

[SPANISH TEXT – TEXTE ESPAGNOL]

Acuerdo

entre

la República Eslovaca

y

el Reino de España

para la protección mutua

de Información Clasificada

La República Eslovaca
y
el Reino de España

(en adelante denominados las "Partes"),

Reconociendo la necesidad de ambas Partes de que se garantice la protección de la Información Clasificada intercambiada entre las mismas en el marco de las negociaciones y los acuerdos de cooperación ya celebrados o que vayan a celebrarse, así como de otros instrumentos contractuales de organizaciones, tanto públicas como privadas, de las Partes;

Deseosas de establecer un conjunto de normas para la protección mutua de la Información Clasificada intercambiada entre las Partes,

Han convenido en lo siguiente:

Artículo 1
Objeto

Por el presente Acuerdo se establecen las normas de seguridad aplicables a todos los instrumentos contractuales en los que se prevea la transmisión de Información Clasificada que se hayan firmado o vayan a firmarse entre las Autoridades de Seguridad Competentes de ambas Partes o por compañías u otras entidades jurídicas debidamente autorizadas para ello.

Artículo 2
Ámbito de aplicación

(1) Por el presente Acuerdo se establecen los procedimientos para la protección de la Información Clasificada que se intercambie entre las Partes.

(2) Ninguna de las Partes podrá invocar el presente Acuerdo con el fin de obtener Información Clasificada que la otra Parte haya recibido de terceros.

Artículo 3
Definiciones

A los efectos del presente Acuerdo:

a) Por **"Información Clasificada"** se entenderá la información o el material, sea cual fuere su forma o naturaleza, que requiera protección contra su divulgación no autorizada y que haya sido designada como tal mediante una clasificación de seguridad;

b) Por **"Autoridad de Seguridad Competente"** se entenderá la Autoridad Nacional de Seguridad / Autoridad de Seguridad Designada que cada Parte designe como responsable de la aplicación y supervisión del presente Acuerdo;

c) Por **"Parte de Origen"** se entenderá la Parte que ceda Información Clasificada a la otra Parte;

d) Por **"Parte Receptora"** se entenderá la Parte a la que se ceda la Información Clasificada por la otra Parte;

e) Por **"Tercero"** se entenderá cualquier Estado u organización internacional que no sea Parte en el presente Acuerdo;

f) Por **"Contrato Clasificado"** se entenderá todo acuerdo entre dos o más Contratistas por el que se creen y definan derechos y obligaciones vinculantes entre los mismos y que contenga o implique Información Clasificada.

g) Por **"Contratista"** se entenderá toda persona física o jurídica que tenga la capacidad jurídica para celebrar Contratos Clasificados;

h) Por **"Habilitación Personal de Seguridad"** se entenderá la certificación expedida por la Autoridad de Seguridad Competente por la que se acredite que una persona cumple los requisitos para acceder a Información Clasificada, de conformidad con las respectivas legislaciones nacionales;

i) Por **"Habilitación de Seguridad para Establecimiento"** se entenderá la certificación expedida por la Autoridad de Seguridad Competente por la que se acredite que, desde el punto de vista de la seguridad, una instalación dispone de la capacidad física y organizativa para utilizar y almacenar Información Clasificada, de conformidad con las respectivas legislaciones nacionales;

j) Por **"Necesidad de Conocer"** se entenderá que el acceso a la Información Clasificada puede otorgarse únicamente a una persona que tenga una necesidad comprobada de conocer o poseer dicha información a los efectos del desempeño de sus funciones oficiales y profesionales, en relación con las cuales se cedió la información a la Parte Receptora.

Artículo 4

Autoridades de Seguridad Competentes

(1) Las Autoridades de Seguridad Competentes para la aplicación del presente Acuerdo son:

Para la República Eslovaca:
Autoridad Nacional de Seguridad

Para el Reino de España:

Secretario de Estado
Director del Centro Nacional de Inteligencia
Oficina Nacional de Seguridad

(2) Las Partes se informarán mutuamente, por conducto diplomático, sobre cualquier modificación relativa a las Autoridades de Seguridad Competentes.

Artículo 5
Principios relativos a la Seguridad

(1) La protección y utilización de la Información Clasificada intercambiada entre las Partes se regirá por los siguientes principios:

a) La Parte Receptora asignará a la Información Clasificada recibida el grado de protección equivalente a la marca que se haya asignado expresamente a dicha información por la Parte de Origen;

b) El acceso a la Información Clasificada estará restringido a las personas que, para el desempeño de sus funciones, deban tener acceso a la Información Clasificada, con arreglo al criterio de "necesidad de conocer", sean titulares de una Habilitación Personal de Seguridad adecuada al nivel de clasificación de seguridad de la Información Clasificada a la que vaya a accederse, o superior, y hayan sido autorizados por las Autoridades de Seguridad Competentes;

c) La Parte Receptora no transmitirá la Información Clasificada a terceros, ya sean personas físicas o jurídicas, ni a un tercer Estado sin el consentimiento previo por escrito de la Parte de Origen;

d) La Información Clasificada transmitida no podrá utilizarse para fines distintos de aquéllos para los que fue proporcionada, de conformidad con el presente Acuerdo;

(2) Con el fin de alcanzar y mantener normas de seguridad similares, las Autoridades de Seguridad Competentes se informarán mutuamente, si así se les solicita, sobre sus normas, procedimientos y prácticas de seguridad en el ámbito de la protección de la Información Clasificada.

(3) Las Partes informarán sobre la existencia del presente Acuerdo siempre que se trate de Información Clasificada.

(4) Las Partes velarán por que toda persona que reciba Información Clasificada cumpla debidamente las obligaciones del presente Acuerdo.

Artículo 6

Clasificaciones de Seguridad y Equivalencias

Las Partes convienen en que los grados de clasificación de seguridad que se indican a continuación son equivalentes y corresponden a los grados de clasificación de seguridad especificados en sus legislaciones nacionales:

República Eslovaca	Reino de España	Equivalente en inglés
PRÍSNE TAJNÉ	SECRETO	TOP SECRET
TAJNÉ	RESERVADO	SECRET
DÔVERNÉ	CONFIDENCIAL	CONFIDENTIAL
VYHRADENÉ	DIFUSIÓN LIMITADA	RESTRICTED

Artículo 7

Asistencia en los Procedimientos de Habilitación

(1) Las Autoridades de Seguridad Competentes de las Partes, previa solicitud y teniendo en cuenta su legislación nacional, se prestarán asistencia mutua durante los procedimientos de habilitación de sus nacionales que residan en el territorio de la otra Parte o de sus instalaciones situadas en el mismo, con carácter previo a la expedición de la Habilitación Personal de Seguridad o de la Habilitación de Seguridad para Establecimiento.

(2) Las Partes reconocerán las Habilitaciones Personales de Seguridad y las Habilitaciones de Seguridad para Establecimiento de conformidad con la legislación nacional de la otra Parte. La equivalencia de las habilitaciones de seguridad se hará con arreglo al artículo 6.

(3) Las Autoridades de Seguridad Competentes se comunicarán cualquier información sobre modificaciones en las Habilitaciones de Seguridad Personales y para Establecimiento, en particular cuando se trate de la retirada o la reducción de su grado de clasificación de seguridad.

Artículo 8

Clasificación, recepción y modificaciones

(1) La Parte Receptora marcará con su propia clasificación de seguridad la Información Clasificada recibida, producida o desarrollada, con arreglo a las equivalencias indicadas en el artículo 6.

(2) Las Partes se informarán mutuamente de toda modificación posterior de la clasificación de seguridad de la Información Clasificada transmitida.

(3) La Parte Receptora y/o sus entidades jurídicas no rebajarán de grado ni desclasificarán la Información Clasificada recibida sin el consentimiento previo por escrito de la Parte de Origen.

Artículo 9

Traducción, reproducción y destrucción

(1) La Información Clasificada con el grado de PRÍSNE TAJNÉ/ SECRETO/ TOP SECRET sólo podrá traducirse o reproducirse con el consentimiento previo por escrito de la Autoridad de Seguridad Competente de la Parte de Origen.

(2) Las traducciones y reproducciones de Información Clasificada se realizarán con arreglo a los siguientes principios:

a) Las personas deberán tener la Habilitación Personal de Seguridad que les permita acceder a Información Clasificada del grado de clasificación de seguridad correspondiente;

b) Las traducciones y las reproducciones deberán marcarse y someterse a la misma protección que el original;

c) Las traducciones y el número de copias se limitarán a las requeridas para fines oficiales;

d) Las traducciones deberán llevar una anotación adecuada en la lengua de destino en la que se indique que contienen Información Clasificada recibida de la Parte de Origen.

(3) No podrá destruirse la Información Clasificada con el grado de PRÍSNE TAJNÉ / SECRETO/ TOP SECRET, sino que deberá devolverse a la Autoridad de Seguridad Competente de la Parte de Origen.

(4) La Información Clasificada con el grado de TAJNÉ / RESERVADO/ SECRET podrá destruirse con el consentimiento previo por escrito de la Parte de Origen.

(5) La Información Clasificada hasta el grado de DÔVERNÉ/ CONFIDENCIAL/ CONFIDENTIAL se destruirá de conformidad con la legislación nacional.

Artículo 10

Transmisión entre las partes

(1) Como regla general, la Información Clasificada se transmitirá entre las Partes por conducto diplomático.

(2) Si el uso de este conducto no fuera posible o retrasara excesivamente la recepción de la Información Clasificada, las transmisiones podrán llevarse a cabo por personal con la habilitación de seguridad adecuada y con acreditación de correo expedida por la Parte que transmita la Información Clasificada.

(3) Las Partes podrán transmitir Información Clasificada por medios electrónicos con arreglo a los procedimientos de seguridad mutuamente aprobados por las Autoridades de Seguridad Competentes.

(4) Las Autoridades de Seguridad Competentes de ambas Partes aprobarán, caso por caso, la transmisión de grandes volúmenes o cantidades de Información Clasificada.

(5) La Parte Receptora deberá confirmar la recepción de la Información Clasificada y la difundirá entre sus usuarios.

Artículo 11
Medidas de Seguridad

(1) La Parte que desee celebrar un Contrato Clasificado con un Contratista de la otra Parte o que desee autorizar a uno de sus propios Contratistas a celebrar un Contrato Clasificado en el territorio de la otra Parte como parte de un proyecto clasificado deberá obtener, a través de su Autoridad de Seguridad Competente, una garantía previa por escrito de la Autoridad de Seguridad Competente de la otra Parte de que el Contratista propuesto dispone de una Habilitación de Seguridad para Establecimiento que le permite el acceso a Información Clasificada del grado de clasificación de seguridad que corresponda.

(2) Los subcontratistas deberán cumplir las mismas obligaciones relativas a la seguridad que el Contratista.

(3) Cuando se inicien negociaciones precontractuales entre una entidad jurídica situada en el territorio de una Parte y otra entidad jurídica situada en el territorio de la otra Parte que tengan por objeto la firma de instrumentos contractuales, las Partes se informarán mutuamente a través de sus Autoridades de Seguridad Competentes sobre la clasificación de seguridad de la Información Clasificada utilizada en las negociaciones precontractuales.

(4) Todo Contrato Clasificado celebrado de conformidad con el presente Acuerdo deberá contener una cláusula apropiada sobre seguridad en la que se especifique:

a) el compromiso por parte del Contratista de que garantizará que sus instalaciones cuentan con las condiciones necesarias para el manejo y utilización de Información Clasificada del nivel de clasificación de seguridad adecuado;

b) el compromiso por parte del Contratista de que garantizará que se conceda la Habilitación Personal de Seguridad del nivel adecuado a las personas que desempeñen funciones que impliquen acceso a Información Clasificada;

c) el compromiso por parte del Contratista de que garantizará que se informe a todas las personas con acceso a Información Clasificada sobre su responsabilidad en relación con la protección de la Información Clasificada de conformidad con la legislación nacional;

d) el compromiso por parte del Contratista de que llevará a cabo inspecciones periódicas de seguridad en sus instalaciones;

e) la guía de la Clasificación y el listado de la Información Clasificada;

f) el procedimiento para la comunicación de cambios en el nivel de clasificación de seguridad de la Información Clasificada;

g) los conductos de comunicación y medios electrónicos de transmisión;

h) el procedimiento para el transporte de Información Clasificada;

i) las personas o entidades jurídicas autorizadas responsables de coordinar la custodia de la Información Clasificada relacionada con un Contrato Clasificado;

j) la obligación de notificar cualquier pérdida, filtración o exposición a riesgo, efectivos o presuntos, de Información Clasificada.

(5) Con objeto de que puedan realizarse una supervisión y control adecuados de la seguridad, deberá enviarse una copia de la cláusula relativa a la seguridad de todo Contrato Clasificado a la Autoridad de Seguridad Competente de la Parte en que hayan de desarrollarse los trabajos.

(6) Los Representantes de las Autoridades de Seguridad Competentes podrán visitarse mutuamente a fin de analizar la eficacia de las medidas adoptadas por un Contratista para la protección de la Información Clasificada contenida en un Contrato Clasificado. Dichas visitas deberán notificarse con, al menos, veinte días de antelación.

Artículo 12
Visitas

(1) Las visitas de nacionales de una Parte a la otra Parte que supongan acceso a Información Clasificada estarán sujetas a la previa autorización por escrito de la Autoridad de Seguridad Competente de la Parte anfitriona.

(2) Una Parte sólo permitirá las visitas de visitantes de la otra Parte que supongan acceso a Información Clasificada cuando:

a) los mismos hayan obtenido la Habilitación Personal de Seguridad correspondiente de la Autoridad de Seguridad Competente de la Parte de Origen; y

b) hayan sido autorizados a recibir Información Clasificada o acceder a la misma de conformidad con su legislación nacional.

(3) La Autoridad de Seguridad Competente de la Parte que reciba la solicitud de visita estudiará la solicitud, decidirá al respecto y comunicará su decisión a la Autoridad de Seguridad Competente de la Parte requirente.

(4) Las visitas que impliquen acceso a Información Clasificada por nacionales de un tercer Estado podrán autorizarse únicamente de común acuerdo entre las Partes.

(5) La Autoridad de Seguridad Competente de la Parte de Origen informará sobre la visita programada a la Autoridad de Seguridad Competente de la Parte anfitriona mediante una solicitud de visita que deberá recibirse, al menos, treinta días antes de su inicio.

(6) En casos urgentes, la solicitud de visita se enviará con, al menos, siete días de antelación.

(7) La solicitud de visita deberá contener la siguiente información:

a) nombre completo del visitante, fecha y lugar de nacimiento, nacionalidad, número de pasaporte o tarjeta de identidad;

b) nombre de la sociedad u otra entidad jurídica a la que pertenezca o represente el visitante;

c) nombre y dirección de la sociedad u otra entidad jurídica objeto de la visita;

d) confirmación de la Habilitación Personal de Seguridad del visitante y su validez;

e) objeto y fin de la visita o visitas;

f) fecha prevista y duración de la visita o visitas que se solicita. En caso de visitas recurrentes deberá indicarse el periodo total cubierto por las mismas.

g) nombre y número de teléfono del punto de contacto en la compañía u otra entidad jurídica objeto de la visita, contactos previos y cualquier otra información que sirva para determinar la justificación de la visita o visitas;

h) fecha, firma y sello oficial de la Autoridad de Seguridad Competente.

(8) Una vez que se haya aprobado la visita, la Autoridad de Seguridad Competente de la Parte anfitriona entregará una copia de la solicitud de visita a los responsables de seguridad de la sociedad u otra entidad jurídica objeto de la visita.

(9) La validez de las autorizaciones de visita no excederá de un año.

(10) Las Partes podrán acordar, respecto de cualquier proyecto, programa o contrato, la elaboración de listados de personas autorizadas a realizar visitas recurrentes. Dichos listados serán válidos durante un periodo inicial de un año.

(11) Una vez que las Partes hayan aprobado estos listados, las condiciones de cada visita se acordarán directamente con los puntos de contacto correspondientes de la

sociedad u otra entidad jurídica que vayan a ser visitadas por dichas personas, con arreglo a los términos y condiciones que se convengan.

Artículo 13
Infracción de la Seguridad y exposición a riesgo

(1) En caso de que tenga lugar una infracción o comprometimiento de la seguridad que dé lugar a una exposición a riesgo real o presunta de la Información Clasificada originada o cedida por la otra Parte, o cuando se sospeche que se ha divulgado Información Clasificada a personas no autorizadas, la Autoridad de Seguridad Competente de la Parte en la que se haya producido la infracción o exposición a riesgo informará a la Autoridad de Seguridad Competente de la otra Parte tan pronto como sea posible y llevará a cabo la investigación pertinente.

(2) Si la infracción de la seguridad o exposición a riesgo se produce en un Estado distinto de las Partes, la Autoridad de Seguridad Competente de la Parte de Origen tomará las medidas previstas en el apartado 1.

(3) La otra Parte colaborará en la investigación si así se le solicita.

(4) En todo caso, la otra Parte será informada de los resultados de la investigación y recibirá un informe final sobre las causas y el alcance de los daños.

Artículo 14
Gastos

Cada Parte correrá con sus propios gastos derivados de la aplicación y supervisión de todos los aspectos del presente Acuerdo.

Artículo 15
Solución de controversias

Toda controversia relativa a la interpretación o aplicación del presente Acuerdo se resolverá por conducto diplomático, a menos que pueda alcanzarse una solución por las Autoridades de Seguridad Competentes.

Artículo 16
Enmiendas

(1) El presente Acuerdo podrá ser enmendado o completado en cualquier momento con el consentimiento mutuo por escrito de las Partes.

(2) Las enmiendas y sus suplementos entrarán en vigor de conformidad con el artículo 18.

Artículo 17
Duración y terminación

(1) El presente Acuerdo se celebra por un periodo indefinido.

(2) Cualquiera de las Partes podrá denunciar el presente Acuerdo en cualquier momento mediante notificación por escrito a la otra Parte por conducto diplomático.

(3) La denuncia surtirá efecto seis meses después de la fecha de recepción de la correspondiente notificación.

(4) No obstante la denuncia, toda la Información Clasificada transmitida, producida o desarrollada en virtud del presente Acuerdo se mantendrá protegida de conformidad con lo dispuesto en el mismo, hasta que la Parte de Origen dispense a la Parte Receptora de sus obligaciones.

Artículo 18
Entrada en vigor

El presente Acuerdo entrará en vigor el primer día del segundo mes a partir de la recepción de la última notificación escrita de las Partes por conducto diplomático confirmando el cumplimiento de todos los procedimientos nacionales para su entrada en vigor.

En fe de lo cual, los firmantes, representantes debidamente autorizados de las Partes, firman el presente Acuerdo.

Hecho en Bratislava, el 20 de enero de 2009 en dos originales, cada uno en eslovaco, español e inglés, siendo todos los textos igualmente auténticos.

Por la República Eslovaca

František Blanárik
Director de la Autoridad
Nacional de Seguridad
República Eslovaca

Por el Reino de España

José Ángel López Jorrin
Embajador
del Reino de España
en la República Eslovaca

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LA RÉPUBLIQUE SLOVAQUE ET LE ROYAUME D'ESPAGNE RELATIF À LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

La République slovaque et le Royaume d'Espagne, ci-après dénommés « les Parties »,

Reconnaissant la nécessité pour les deux Parties de protéger les Informations classifiées échangées entre elles dans le cadre des négociations et des accords de coopération conclus ou devant être conclus ainsi que d'autres instruments contractuels d'organisations publiques ou privées des Parties,

Souhaitant créer un ensemble de réglementations ayant trait à la protection mutuelle des Informations classifiées échangées entre les Parties,

Sont convenus de ce qui suit :

Article premier. Objet

Le présent Accord établit les règles de sécurité applicables à tous les instruments contractuels qui prévoient la transmission d'Informations classifiées, signés ou devant être signés entre les Autorités de sécurité compétentes des deux Parties ou par des sociétés ou autres organismes juridiques dûment autorisés à cette fin.

Article 2. Champ d'application

1. Le présent Accord définit les procédures de protection des Informations classifiées échangées entre les Parties.

2. Aucune des Parties ne peut invoquer le présent Accord en vue d'obtenir des Informations classifiées que l'autre Partie a reçues d'une Partie tierce.

Article 3. Définitions

Aux fins du présent Accord :

a) L'expression « Informations classifiées » signifie les informations ou matériels, quels qu'en soient la forme ou la nature, déterminés comme requérant une protection contre la divulgation non autorisée, telle que définie par leur niveau de classification de sécurité;

b) L'expression « Autorité de sécurité compétente » signifie l'Agence nationale de sécurité/l'Autorité de sécurité désignée, déterminée par une Partie comme étant responsable de l'application et de la supervision du présent Accord;

c) L'expression « Partie d'origine » signifie la Partie qui communique les Informations classifiées à l'autre Partie;

d) L'expression « Partie destinataire » signifie la Partie à laquelle l'autre Partie transmet les Informations classifiées;

e) L'expression « Partie tierce » signifie toute organisation internationale ou tout État qui n'est pas partie au présent Accord;

f) L'expression « Contrat classifié » signifie tout accord entre deux ou plusieurs Contractants qui crée ou définit des droits et obligations exécutoires entre eux et qui contient ou implique des Informations classifiées;

g) Le terme « Contractant » signifie une personne physique ou morale dotée de la capacité juridique de conclure des Contrats classifiés;

h) L'expression « Habilitation PSC » désigne un certificat remis par l'Autorité de sécurité compétente selon lequel une personne est habilitée à accéder aux Informations classifiées, conformément aux dispositions de la législation nationale respective;

i) L'expression « Habilitation FSC » désigne un certificat remis par l'Autorité de sécurité compétente selon lequel, du point de vue de la sécurité, un établissement est doté de la capacité physique et organisationnelle d'utiliser et de stocker des Informations classifiées, conformément aux dispositions de la législation nationale respective;

j) L'expression « Besoin d'en connaître » signifie un principe selon lequel l'accès à des Informations classifiées ne peut être accordé à une personne que s'il peut être vérifié que leur connaissance ou possession est requise en rapport avec leurs fonctions officielles et professionnelles, dans le cadre desquelles lesdites Informations classifiées ont été communiquées à la Partie destinataire.

Article 4. Autorités de sécurité compétentes

1. Les Autorités de sécurité compétentes pour l'application du présent Accord sont les suivantes :

Pour la République slovaque :

L'Autorité nationale de sécurité

Pour le Royaume d'Espagne :

Le Secrétaire d'État, Directeur du Centre national de renseignements, Bureau de la sécurité nationale.

2. Les Parties s'informent mutuellement, par la voie diplomatique, de toute modification concernant les Autorités de sécurité compétentes.

Article 5. Principes de sécurité

1. La protection et l'utilisation des Informations classifiées échangées entre les Parties est régie par les principes suivants :

a) La Partie destinataire attribuera aux Informations classifiées reçues le niveau de protection équivalant à celui expressément attribué auxdites Informations classifiées par la Partie d'origine;

b) L'accès aux Informations classifiées est limité aux personnes dont l'accès à celles-ci est requis dans le cadre de l'exercice de leurs fonctions selon le principe du Besoin d'en connaître, qui possèdent la Cote de sécurité du personnel appropriée au niveau de classification de sécurité des Informations classifiées considérées ou plus et qui ont obtenu l'autorisation des Autorités de sécurité compétentes;

c) La Partie destinataire ne transmettra aucune Information classifiée à une quelconque Partie tierce, personne physique ou morale ou à un quelconque État tiers sans l'accord préalable écrit de la Partie d'origine;

d) Les Informations classifiées transmises ne peuvent être utilisées à des fins autres que celles justifiant leur transmission, conformément au présent Accord.

2. Afin de parvenir à des normes de sécurité comparables et de les maintenir, les Autorités de sécurité compétentes se fourniront mutuellement, sur demande, des informations concernant leurs normes, procédures et pratiques de sécurité relatives à la protection des Informations classifiées.

3. Les Parties sont tenues de mentionner l'existence du présent Accord dès que des Informations classifiées sont communiquées.

4. Les Parties veillent à ce que toute personne à laquelle des Informations classifiées sont communiquées réponde dûment aux obligations prévues par le présent Accord.

Article 6. Classification de sécurité et équivalences

Les Parties conviennent que les niveaux de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité spécifiés dans leur législation nationale :

République slovaque	Royaume d'Espagne	Équivalence en anglais
PRÍSNE TAJNÉ	SECRETO	TOP SECRET (SECRET DÉFENSE)
TAJNÉ	RESERVADO	SECRET
DÔVERNÉ	CONFIDENCIAL	CONFIDENTIAL (CONFIDENTIEL)
VYHRADENÉ	DIFUSIÓN LIMITADA	RESTRICTED (RESTREINT)

Article 7. Aide aux enquêtes d'habilitation

1. Les Autorités de sécurité compétentes des Parties se prêtent assistance, sur demande et compte tenu de leur législation nationale, aux fins des enquêtes visant à habiliter leurs citoyens et leurs établissements, vivant ou situés sur le territoire de l'autre Partie, et à leur attribuer une « Cote de sécurité - personnel » (PSC) ou une « Cote de sécurité - établissement » (FSC).

2. Chacune des Parties reconnaît les habilitations PSC et FSC attribuées en conformité avec la législation nationale de l'autre Partie. L'article 6 établit l'équivalence des cotes de sécurité des deux États.

3, Les Autorités de sécurité compétentes se communiquent mutuellement toute information relative à des modifications apportées aux habilitations PSC et FSC, notamment en cas de retrait ou de baisse de leur niveau de classification de sécurité.

Article 8. Classification, réception et modifications

1. La Partie destinataire appose sur les Informations classifiées reçues, produites ou développées ses propres marques de classification de sécurité conformément aux équivalences définies à l'article 6.

2. Les Parties s'informent mutuellement de toute modification ultérieure de la classification de sécurité attribuée aux Informations classifiées transmises.

3. La Partie destinataire et/ou ses organismes juridiques ne peuvent ni abaisser la cote de sécurité ni déclassifier les Informations classifiées qu'elles reçoivent sans le consentement préalable écrit de la Partie d'origine.

Article 9. Traduction, reproduction et destruction

1. Les Informations classifiées PRÍSNE TAJNÉ/SECRET/TOP SECRET ne peuvent être traduites ou reproduites qu'avec le consentement préalable écrit de l'Autorité de sécurité compétente de la Partie d'origine.

2. Les principes suivants s'appliquent à la traduction et à la reproduction d'Informations classifiées :

a) Les personnes physiques doivent posséder une Habilitation PSC leur permettant d'accéder aux Informations classifiées au niveau de classification de sécurité concerné;

b) Les traductions et les reproductions doivent porter la même mention de sécurité et bénéficier de la même protection que les originaux;

c) Le nombre d'exemplaires traduits doit se limiter au nombre requis à des fins officielles;

d) Les traductions doivent contenir une mention appropriée, rédigée dans la langue dans laquelle les documents sont traduits, indiquant qu'elles contiennent des Informations classifiées reçues de la Partie d'origine.

3. Les Informations classifiées PRÍSNE TAJNÉ/SECRET/TOP SECRET ne peuvent pas être détruites. Elles seront renvoyées à l'Autorité de sécurité compétente de la Partie d'origine.

4. Les Informations classifiées TAJNÉ/RESERVADO/SECRET seront détruites sur accord préalable écrit de la Partie d'origine.

5. Les Informations classifiées DÔVERNÉ/CONFIDENCIAL/CONFIDENTIAL seront détruites conformément aux dispositions de la législation nationale.

Article 10. Transmission entre les Parties

1. Les Informations classifiées seront normalement transmises entre les Parties par la voie diplomatique.

2. Si le recours à la voie diplomatique est impossible ou retarde indûment la réception des Informations classifiées, les transmissions peuvent être effectuées par des effectifs dotés de l'habilitation de sécurité adéquate, habilités par un ordre de mission délivré par la Partie qui transmet les Informations classifiées.

3. Les Parties peuvent transmettre des Informations classifiées par la voie électronique conformément aux procédures de sécurité mutuellement approuvées par la Partie qui transmet les Informations classifiées.

4. La transmission de documents classifiés volumineux ou de grandes quantités d'Informations classifiées, organisée au cas par cas, doit être approuvée par les deux Autorités de sécurité compétentes.

5. La Partie destinataire confirmera la réception des Informations classifiées et les distribuera aux utilisateurs.

Article 11. Mesures de sécurité

1. Une Partie qui souhaite adjuger un Contrat classifié à un Contractant de l'autre Partie, ou autoriser un de ses propres Contractants à adjuger un Contrat classifié sur le territoire de l'autre Partie au titre d'un projet classifié, doit obtenir au préalable de l'Autorité de sécurité compétente de l'autre Partie, par écrit, par l'intermédiaire de son Autorité de sécurité compétente, l'assurance que le Contractant possède l'Habilitation FSC permettant l'accès aux Informations classifiées au niveau de classification de sécurité considéré.

2. Tout sous-traitant doit satisfaire, en matière de sécurité, aux mêmes obligations que le Contractant.

3. Lorsque des négociations précontractuelles sont engagées entre un organisme juridique situé sur le territoire d'une Partie et un autre organisme juridique situé sur le territoire de l'autre Partie, dans l'optique de signer des instruments contractuels, les Parties sont tenues de s'informer mutuellement, par l'intermédiaire de leurs Autorités de sécurité compétentes, de la classification de sécurité attribuée aux Informations classifiées visées dans les négociations contractuelles.

4. Tout Contrat classifié conclu conformément au présent Accord doit contenir une section appropriée concernant la sécurité, qui définit :

a) L'engagement du Contractant à veiller à ce que ses locaux réunissent les conditions nécessaires au traitement et au stockage d'Informations classifiées au niveau de classification de sécurité considéré;

b) L'engagement du Contractant à veiller à ce qu'un niveau approprié d'Habilitation PSC soit attribué aux personnes qui nécessitent un accès aux Informations confidentielles dans le cadre de leurs fonctions;

c) L'engagement du Contractant à veiller à ce que toutes les personnes ayant accès aux Informations classifiées soient informées de leur responsabilité en termes de protection des Informations classifiées conformément aux dispositions de la législation nationale;

d) L'engagement du Contractant à effectuer des inspections de sûreté régulières de ses locaux;

e) Un guide de classification et une liste des Informations classifiées;

f) La procédure de communication des changements du niveau de classification de sécurité d'Informations classifiées;

g) Les voies de communication et les moyens de transmission électroniques;

h) La procédure d'acheminement des Informations classifiées;

i) Les personnes physiques ou morales compétentes autorisées, responsables de la coordination de la sauvegarde des Informations classifiées liées au Contrat classifié;

j) Une obligation de notifier toute perte, révélation ou mise en péril réelle ou présumée des Informations classifiées.

5. Un exemplaire de la section « sécurité » de tout Contrat classifié doit être transmis à l'Autorité de sécurité compétente de la Partie sur le territoire de laquelle il est prévu d'effectuer les travaux, afin de permettre une supervision et un contrôle de sécurité appropriés.

6. Des représentants des Autorités de sécurité compétentes peuvent se rendre mutuellement visite afin d'analyser l'efficacité des mesures adoptées par un Contractant pour la protection des Informations classifiées visées dans un Contrat classifié. La visite doit être notifiée au moins vingt jours à l'avance.

Article 12. Visites

1. Les ressortissants d'une Partie autoriseront l'autre Partie à effectuer des visites demandant un accès à des Informations classifiées uniquement sur accord préalable écrit de l'Autorité de sécurité compétente de la Partie d'accueil.

2. Une Partie autorisera des visiteurs de l'autre Partie à effectuer des visites demandant l'accès aux Informations classifiées uniquement si ceux-ci :

a) Ont reçu de l'Autorité de sécurité compétente de la Partie expéditrice l'Habilitation PSC adéquate;

b) Sont habilités à recevoir des Informations classifiées ou à y accéder conformément aux dispositions de leur législation nationale.

3. L'Autorité de sécurité compétente de la Partie qui reçoit la demande de visite examine la demande et prend la décision appropriée à cet égard dont elle informe l'Autorité de sécurité compétente de la Partie requérante.

4. Les visites demandant un accès à des Informations classifiées par des ressortissants de pays tiers seront uniquement autorisées sur accord entre les Parties.

5. L'Autorité de sécurité compétente de la Partie expéditrice est tenue de notifier l'Autorité de sécurité compétente de la Partie d'accueil de la visite prévue au moyen d'une demande de visite qui devra parvenir au moins trente jours au préalable.

6. En cas d'urgence, la demande de visite sera envoyée au moins sept jours à l'avance.

7. La demande de visite doit contenir :

a) Le nom et le prénom du visiteur, sa date et son lieu de naissance, sa nationalité, son numéro de passeport ou de carte d'identité;

b) Le nom de la société ou de tout autre organisme juridique que le visiteur représente ou auquel il appartient;

c) Le nom et l'adresse de la société ou de tout autre organisme juridique à visiter;

d) La confirmation que le visiteur est doté d'une Habilitation PSC, avec mention de sa durée de validité;

e) L'objet et la finalité de la visite ou des visites;

f) La date et la durée prévues de la visite ou des visites requises. En cas de visites récurrentes, la période totale accumulée des visites doit être indiquée;

g) Le nom et le numéro de téléphone du point de contact de la société ou de tout autre organisme juridique à visiter, les contacts précédents et tout autre renseignement permettant de déterminer la pertinence de la visite ou des visites;

h) La date, la signature et le cachet officiel de l'Autorité de sécurité compétente.

8. Une fois la visite approuvée, l'Autorité de sécurité compétente de la Partie d'accueil doit fournir une copie de la demande de visite aux responsables de la sécurité de la société ou de tout autre organisme juridique à visiter.

9. L'approbation de la visite restera valable pendant un an maximum.

10. Pour tout projet, programme ou contrat, les Parties peuvent convenir de dresser des listes des personnes autorisées à procéder à des visites récurrentes. Les listes restent valides pendant une durée initiale d'un an.

11. Une fois les listes approuvées par les Parties, les modalités des visites respectives seront directement définies avec les points de contact concernés de la société ou de tout autre organisme juridique à visiter par lesdites personnes, selon les conditions convenues.

Article 13. Infraction à et compromission de la sécurité

1. Lorsque se produit une infraction ou une compromission qui entrave effectivement ou qui est suspectée d'entraver la sécurité des Informations classifiées provenant ou reçues de l'autre Partie ou lorsqu'il est présumé que des Informations classifiées ont été divulguées à des personnes non autorisées, l'Autorité de sécurité compétente de la Partie sur le territoire de laquelle l'infraction ou la compromission a eu lieu doit en informer au plus tôt l'Autorité de sécurité compétente de l'autre Partie et mener l'enquête appropriée.

2. Si une infraction à la sécurité ou une compromission se produit dans un État autre que les Parties, l'Autorité de sécurité compétente de la Partie expéditrice prend les mesures visées au paragraphe 1.

3. L'autre Partie collabore à l'enquête sur simple demande.

4. L'autre Partie doit en tout cas être tenue au courant des résultats de l'enquête et reçoit un exposé définitif des motifs et l'étendue de l'infraction.

Article 14. Coûts

Chaque Partie assume ses propres coûts inhérents à l'application et à la supervision de tous les aspects du présent Accord.

Article 15. Règlement des litiges

Tout litige relatif à l'application ou à l'interprétation du présent Accord sera résolu par la voie diplomatique, à moins que les Autorités de sécurité compétentes ne parviennent à un accord.

Article 16. Modifications

1. Le présent Accord peut être modifié ou complété à tout moment, sur accord mutuel écrit des Parties.

2. Les modifications et ajouts entreront en vigueur conformément à l'article 18.

Article 17. Durée et résiliation

1. Le présent Accord est conclu pour une durée indéterminée.

2. Chaque Partie peut, à tout moment, mettre fin au présent Accord par notification écrite adressée à l'autre Partie par la voie diplomatique.

3. La résiliation prendra effet six mois après le jour de la réception de la notification respective.

4. Nonobstant la résiliation, toutes les Informations classifiées transmises, produites ou développées dans le cadre du présent Accord continueront à bénéficier d'une protection conformément aux dispositions du présent Accord jusqu'à ce que la Partie d'origine délivre la Partie destinataire de cette obligation.

Article 18. Entrée en vigueur

Les Parties se notifient par la voie diplomatique l'accomplissement des procédures nationales nécessaires à l'entrée en vigueur du présent Accord. Ledit Accord entre en vigueur le premier jour du deuxième mois qui suit la réception de la dernière notification écrite.

EN FOI DE QUOI, les soussignés, représentants dûment autorisés des Parties, ont signé le présent Accord.

FAIT à Bratislava le 20 janvier 2009, en deux exemplaires originaux, chacun rédigé en slovaque, espagnol et anglais, les deux textes faisant également foi.

Pour la République slovaque :

FRANTIŠEK BLANÁRIK
Directeur de l'Autorité nationale de sécurité de la République slovaque

Pour le Royaume d'Espagne :

JOSÉ ÁNGEL LÓPEZ JORRIN
Ambassadeur du Royaume d'Espagne en République slovaque