

No. 47642

**Slovakia
and
France**

Agreement between the Government of the Slovak Republic and the Government of the French Republic concerning the exchange and mutual protection of classified information (with annexes). Bratislava, 26 January 2010

Entry into force: *1 June 2010 by notification, in accordance with article 16*

Authentic texts: *French and Slovak*

Registration with the Secretariat of the United Nations: *Slovakia, 19 July 2010*

**Slovaquie
et
France**

Accord entre le Gouvernement de la République slovaque et le Gouvernement de la République française relatif à l'échange et à la protection réciproque des informations classifiées (avec annexes). Bratislava, 26 janvier 2010

Entrée en vigueur : *1^{er} juin 2010 par notification, conformément à l'article 16*

Textes authentiques : *français et slovaque*

Enregistrement auprès du Secrétariat des Nations Unies : *Slovaquie, 19 juillet 2010*

[FRENCH TEXT – TEXTE FRANÇAIS]

Accord

entre

le Gouvernement de

la République slovaque

et

le Gouvernement de

la République française

relatif à l'échange

et à la protection réciproque des

informations classifiées

**Le Gouvernement de la République slovaque
et
le Gouvernement de la République française,**

ci-après dénommés « les Parties »,

Désireux de garantir la protection des informations et matériels classifiés échangés entre les États des Parties ou des organismes publics ou privés soumis à leurs lois et réglementations nationales respectives, ou produits conjointement par eux,

Sont convenus des dispositions suivantes :

Article premier : Définitions

Aux fins du présent Accord :

- 1.1. « **Informations classifiées** » désigne les informations, documents et matériels, quels qu'en soient la forme, la nature ou le mode de transmission, existants ou en cours d'élaboration, auxquels a été attribué un niveau de classification de sécurité et qui, dans l'intérêt de la sécurité nationale et conformément aux lois et réglementations nationales des États des Parties, requièrent une protection contre toute manipulation non autorisée ou tout autre type d'atteinte à la sécurité.
- 1.2. « **Contrat classifié** » désigne un contrat, un contrat de sous-traitance ou un projet dont l'élaboration et l'exécution nécessitent l'accès à des informations classifiées ou l'utilisation et la production d'informations classifiées.
- 1.3. « **Contractant** » désigne toute personne physique ou morale ayant la capacité juridique de négocier et de conclure des contrats classifiés.
- 1.4. « **Autorité de sécurité compétente** » désigne l'Autorité nationale de sécurité ou l'Autorité de sécurité désignée chargée par l'État de la Partie concernée de la mise en œuvre et de la supervision du présent Accord, en fonction du domaine concerné.
- 1.5. « **Partie d'origine** » désigne l'État de la Partie, y compris toute personne morale relevant de sa juridiction en vertu de ses lois et réglementations nationales, qui transmet des informations classifiées.
- 1.6. « **Partie destinataire** » désigne l'État de la Partie, y compris toute personne morale relevant de sa juridiction en vertu de ses lois et réglementations nationales, à qui des informations classifiées sont transmises.
- 1.7. « **Partie d'accueil** » désigne l'État de la Partie sur le territoire duquel une visite a lieu.
- 1.8. « **Besoin d'en connaître** » désigne le besoin d'avoir accès à des informations classifiées dans le cadre d'une fonction officielle donnée et en vue d'exécuter une tâche spécifique.

- 1.9. « **Tierce partie** » désigne les organisations internationales et les gouvernements des États non parties au présent Accord, de même que leurs personnes morales et leurs ressortissants.

Article 2 : Champ d'application

Le présent Accord constitue les règles communes de sécurité applicables à toutes informations classifiées échangées entre les États des Parties, y compris toute personne morale placée sous leur juridiction en vertu de leurs lois et réglementations nationales, ou produites conjointement par eux.

Article 3 : Autorités nationales de sécurité

- 3.1. Les Autorités nationales de sécurité sont :

Pour la République slovaque :

Národný bezpečnostný úrad,
Butadínska 30,
850 07 Bratislava ;

Pour la République française :

Secrétariat général de la Défense nationale,
51, bd de La Tour-Maubourg,
75700 Paris 07 SP.

- 3.2. Les Parties s'informent mutuellement par la voie diplomatique, sauf autres dispositions convenues, des Autorités de sécurité compétentes appropriées et de leurs points de contact, ainsi que de tout changement y afférent.

Article 4 : Principes de sécurité

- 4.1. Conformément à leurs lois et réglementations nationales, les États des Parties prennent les mesures propres à assurer la protection des informations classifiées transmises ou produites conjointement en vertu du présent Accord et leur accordent un niveau de classification de sécurité équivalent à celui qui est appliqué à leurs propres informations classifiées conformément aux dispositions de l'article 5 paragraphe 5.1.
- 4.2. Dès réception d'informations classifiées, la Partie destinataire leur appose sa propre classification nationale conformément aux équivalences définies à l'article 5 paragraphe 5.1.
- 4.3. L'accès aux informations classifiées est strictement réservé aux personnes habilitées au niveau requis et dont les fonctions nécessitent l'accès aux dites informations classifiées sur la base du besoin d'en connaître.
- 4.4. La Partie destinataire ne déclassifie ni ne déclassifie d'informations classifiées transmises sans l'accord écrit préalable de la Partie d'origine.

- 4.5. Les États des Parties se tiennent mutuellement informés, sans retard injustifié, de tout changement affectant la protection des informations classifiées échangées ou produites conjointement en vertu du présent Accord.
- 4.6. Les informations classifiées transmises ne sont pas utilisées à des fins autres que celles qui sont convenues entre les Autorités de sécurité compétentes.

Article 5 : Classifications de sécurité et équivalences

- 5.1. Les Parties s'engagent à assurer la protection des informations classifiées échangées et adoptent les équivalences de niveaux de classification de sécurité définies dans le tableau ci-dessous :

République slovaque	République française
PRÍSNE TAJNÉ	TRES SECRET DEFENSE
TAJNÉ	SECRET DEFENSE
DÓVERNÉ	CONFIDENTIEL DEFENSE
VYHRADENÉ	(Voir les paragraphes 2 et 3 ci-après)

- 5.2. La République française traite et protège les informations classifiées portant la mention « VYHRADENÉ », transmises par la République slovaque, conformément à ses lois et réglementations en vigueur relatives aux informations protégées portant la mention « DIFFUSION RESTREINTE ».
- 5.3. La République slovaque traite et protège les informations portant la mention « DIFFUSION RESTREINTE », transmises par la République française, conformément à ses lois et réglementations en vigueur relatives à la protection des informations classifiées portant la mention « VYHRADENÉ ».
- 5.4. Afin de maintenir des normes de sécurité comparables, chaque Partie, à la demande de l'autre, fournit toutes les informations requises relatives aux lois, réglementations et procédures de sécurité nationales appliquées pour assurer la sécurité des informations classifiées. Les Parties conviennent de faciliter les contacts entre leurs Autorités de sécurité compétentes respectives.

Article 6 : Procédure d'habilitation de sécurité

- 6.1. Pour l'accès aux informations classifiées, l'État de chaque Partie mène, conformément à ses lois et réglementations nationales, une procédure d'habilitation de sécurité.
- 6.2. Dans le cadre de la procédure d'habilitation de sécurité d'un ressortissant de l'État d'une des Parties qui a séjourné ou se trouve encore sur le territoire de l'État de l'autre Partie, les Autorités de sécurité compétentes se prêtent mutuellement assistance conformément à leurs lois et réglementations nationales.

- 6.3. Les Autorités de sécurité compétentes reconnaissent mutuellement les habilitations de sécurité délivrées conformément à leurs lois et règlements nationaux à leurs ressortissants et à leurs personnes morales dans le cadre de l'accès à des informations classifiées.
- 6.4. Les Autorités de sécurité compétentes se tiennent mutuellement informées des changements qui affectent les habilitations de sécurité de leurs ressortissants ou des personnes morales relevant du présent Accord, en particulier en cas de retrait d'une habilitation ou d'abaissement de son niveau.

Article 7 : Utilisation des informations classifiées

- 7.1. Les informations classifiées transmises ou produites conjointement en vertu du présent Accord ne sauraient être déclassées, déclassifiées ni divulguées à une tierce partie sans l'accord écrit préalable de l'Autorité de sécurité compétente de l'État de l'autre Partie.
- 7.2. Avant de transmettre aux contractants des informations classifiées reçues de la Partie d'origine, l'Autorité de sécurité compétente de la Partie destinataire doit :
- a) s'assurer que les contractants et leurs locaux sont en mesure de protéger comme il convient les informations classifiées ;
 - b) s'assurer que le contractant considéré et ses installations détiennent une habilitation de sécurité au niveau requis ;
 - c) s'assurer que les personnes qui ont accès à des informations classifiées détiennent une habilitation de sécurité au niveau requis et ont besoin d'en connaître, et qu'elles ont été informées des responsabilités qui découlent pour elles des lois et règlements nationaux respectifs ;
 - d) procéder à des inspections de sécurité des installations appropriées.

Article 8 : Traduction, reproduction et destruction

- 8.1. Les reproductions et traductions d'informations classifiées sont marquées et protégées de la même manière que les originaux.
- 8.2. Les informations classifiées PRÍSNE TAJNÉ / TRES SECRET DEFENSE ne sont pas reproduites. Des originaux supplémentaires peuvent être fournis sur demande écrite adressée à l'Autorité de sécurité compétente de la Partie d'origine. Des traductions d'informations classifiées PRÍSNE TAJNÉ / TRES SECRET DEFENSE ne peuvent être effectuées que sur la base de l'accord écrit préalable de l'Autorité de sécurité compétente de la partie d'origine.
- 8.3. Les informations classifiées PRÍSNE TAJNÉ / TRES SECRET DEFENSE ne doivent pas être détruites, sauf autorisation expresse de la Partie d'origine. Elles sont restituées à la Partie d'origine conformément aux dispositions de l'article 9 lorsqu'il a

été reconnu qu'elle ne sont plus nécessaires ou après la venue à expiration de leur classification.

- 8.4. La traduction et la reproduction d'informations classifiées TAJNÉ / SECRET DEFENSE sont autorisées uniquement avec l'accord écrit préalable de l'Autorité de sécurité compétente de la Partie d'origine.
- 8.5. Les informations classifiées sont détruites de telle manière que leur reconstruction totale ou partielle soit impossible.

Article 9 : Transmission des informations classifiées

- 9.1. Les informations classifiées sont transmises par la voie diplomatique, sauf autres modalités convenues entre les Autorités de sécurité compétentes.
- 9.2. La transmission doit satisfaire aux conditions suivantes :
 - a) le convoyeur est habilité à un niveau au moins égal à celui des informations classifiées à transmettre ;
 - b) le convoyeur est un employé permanent de l'organisme expéditeur ou destinataire ou de l'administration de l'une ou l'autre des Parties et détient une lettre de courrier délivrée conformément aux lois et règlements appropriés ;
 - c) la Partie d'origine tient un registre des informations classifiées transmises et en fournit sur demande un extrait à la Partie destinataire ;
 - d) les informations classifiées sont dûment empaquetées et scellées conformément aux lois et règlements nationaux de la Partie d'origine ;
 - e) la réception d'informations classifiées est confirmée par écrit sans retard injustifié.
- 9.3. La transmission électronique d'informations classifiées s'effectue sous forme cryptée au moyen des méthodes et dispositifs cryptographiques approuvés par les Autorités de sécurité compétentes.

Article 10 : Contrats classifiés

- 10.1. L'Autorité de sécurité compétente de la Partie d'origine informe de tout contrat classifié l'Autorité de sécurité compétente de la Partie destinataire avant l'échange d'informations classifiées, conformément à ses lois et réglementations nationales. Cette notification précise le niveau de classification le plus élevé des informations classifiées mises en œuvre.
- 10.2. L'État de la Partie qui souhaite conclure, ou autoriser un contractant relevant de sa juridiction à conclure, un contrat classifié avec un contractant relevant de la juridiction de l'État de l'autre Partie doit s'assurer auprès de l'Autorité de sécurité compétente appropriée que ledit contractant est habilité au niveau requis en vue d'exécuter le contrat classifié. À défaut, l'Autorité de sécurité compétente de la Partie

destinataire engage sur demande de l'Autorité de sécurité compétente de l'autre Partie, conformément à ses lois et réglementations nationales, la procédure d'habilitation requise.

- 10.3. Avant toute conclusion d'un contrat classifié, l'Autorité de sécurité compétente doit avoir reçu de son homologue l'assurance écrite que le contractant prévu est habilité au niveau requis et a pris toutes les mesures de sécurité requises afin d'assurer la protection des informations classifiées. Les Autorités de sécurité compétentes s'informent également sans retard injustifié de tout cas de refus d'habilitation.
- 10.4. Tout contrat classifié doit comprendre une annexe de sécurité établie conformément à l'Annexe 1.
- 10.5. L'Autorité de sécurité compétente de la Partie d'origine transmet une copie de l'annexe de sécurité à l'Autorité de sécurité compétente de la Partie destinataire.
- 10.6. Les Autorités de sécurité compétentes font en sorte que soit appliqué et maintenu, dans le cadre de l'exécution des contrats classifiés, un niveau de sécurité équivalent au niveau requis pour assurer la protection de leurs propres contrats classifiés.
- 10.7. L'exécution de tout contrat classifié de sous-traitance est subordonnée à l'accord de l'Autorité de sécurité compétente et tout sous-traitant doit se conformer aux mêmes obligations de sécurité que le contractant, conformément aux dispositions du présent Accord.

Article 11 : Visites

- 11.1. Les visites qui impliquent l'accès à des informations classifiées en vertu du présent Accord sont soumises à l'autorisation écrite préalable de l'Autorité de sécurité compétente de la Partie d'accueil.
- 11.2. Les visites, par des ressortissants d'un État tiers, de locaux situés sur le territoire de l'État d'une Partie impliquant l'accès à des informations classifiées en vertu du présent Accord sont soumises à l'autorisation écrite préalable de l'Autorité de sécurité compétente de l'État de l'autre Partie.
- 11.3. Les visites mentionnées aux paragraphes 11.1 et 11.2 nécessitent que tous les visiteurs justifient du niveau d'habilitation approprié et du besoin d'en connaître.
- 11.4. Les demandes de visites nécessitant un accès à des informations classifiées de niveau PRÍSNE TAJNÉ / TRES SECRET DEFENSE sont transmises par la voie diplomatique à l'Autorité nationale de sécurité de la Partie d'accueil. Les demandes de visites nécessitant l'accès à des informations classifiées de niveau inférieur sont traitées directement entre les Autorités de sécurité compétentes. Les demandes sont adressées au moins trois (3) semaines à l'avance. Les demandes de visite doivent contenir les renseignements mentionnés à l'Annexe 2.
- 11.5. La validité d'une autorisation de visite ne peut excéder une durée de douze (12) mois. Si une visite ne peut être effectuée dans les délais prévus ou si une prorogation de la validité d'une autorisation est nécessaire, une nouvelle autorisation de visite peut être demandée trois (3) semaines au moins avant la venue à expiration de

l'autorisation en cours, sauf autres dispositions établies d'un commun accord par les Autorités de sécurité compétentes.

11.6. Tous les visiteurs doivent respecter les règles et instructions de sécurité de la Partie d'accueil.

Article 12 : Visites multiples

12.1. Les Parties peuvent établir une liste des personnels autorisés à effectuer plusieurs visites en rapport avec une activité, conformément aux modalités convenues par les Autorités de sécurité compétentes. Cette liste est valable pour une durée initiale de douze (12) mois qui, par accord entre les Autorités de sécurité compétentes, peut être prorogée pour des périodes supplémentaires n'excédant pas douze (12) mois.

12.2. La liste mentionnée au paragraphe 12.1 est arrêtée conformément aux lois et règlements nationaux de la Partie d'accueil. Après son approbation, les modalités de visites particulières peuvent être définies directement par les organismes concernés. Les demandes de visite doivent renfermer les renseignements mentionnés à l'Annexe 2.

Article 13 : Infractions aux lois et règlements

13.1. Si une infraction aux lois et règlements nationaux relatifs à la protection des informations classifiées en vertu du présent Accord est présumée ou découverte, l'Autorité de sécurité compétente de l'État de l'autre Partie en est informée par écrit sans retard injustifié.

13.2. La notification doit être suffisamment détaillée pour que la Partie d'origine puisse pleinement évaluer les conséquences.

13.3. L'État de la Partie qui a découvert ou suspecté les faits mentionnés à l'article 13 paragraphe 13.1 diligente aussitôt une enquête conformément à ses lois et règlements nationaux. L'État de l'autre Partie coopère à l'enquête sur demande. L'Autorité de sécurité compétente de l'autre Partie est informée sans retard injustifié des résultats de l'enquête, des mesures décidées et des actions correctives engagées.

Article 14 : Frais

Chaque Partie prend en charge les frais encourus par elle dans le cadre de l'application du présent Accord.

Article 15 : Règlement des différends

15.1. Tout différend relatif à l'interprétation ou à l'application du présent Accord est réglé exclusivement par voie de consultations.

15.2. Pendant la durée du différend, les Parties s'engagent à respecter les obligations énoncées par le présent Accord.

Article 16 : Dispositions finales

- 16.1. A la date de son entrée en vigueur, le présent Accord abroge et remplace l'Accord général de sécurité entre le Gouvernement de la République slovaque et le Gouvernement de la République française signé à Paris le 20 mars 1997. A la suite de la cessation d'effet de l'Accord général de sécurité entre le Gouvernement de la République française et le Gouvernement de la République de Slovaquie, les Informations classifiées échangées et produites en vertu dudit Accord demeurent classifiées et sont protégées en vertu du présent Accord.
- 16.2. Le présent Accord est conclu pour une durée indéterminée et entrera en vigueur le premier jour du deuxième mois suivant la réception de la dernière des notifications par lesquelles les Parties auront attesté par la voie diplomatique l'accomplissement des procédures légales requises pour son entrée en vigueur.
- 16.3. Les Autorités de sécurité compétentes se consultent en tant que de besoin sur les aspects techniques particuliers relatifs à l'application du présent Accord et peuvent conclure en tant que de besoin tout arrangement approprié ou protocole spécifique de sécurité complétant le présent Accord.
- 16.4. Chaque Partie informe l'autre de toute modification de ses lois et règlements nationaux appropriés. Dans ce cas, les Parties se consultent afin d'étudier les modifications éventuelles à apporter au présent Accord. Dans l'intervalle, les informations classifiées continuent d'être protégées conformément aux dispositions de celui-ci.
- 16.5. Le présent Accord peut être modifié avec l'accord écrit des deux Parties. Les modifications entrent en vigueur conformément au paragraphe 16.2, sauf dispositions contraires arrêtées d'un commun accord.
- 16.6. Le présent Accord peut être dénoncé soit d'un commun accord soit unilatéralement. Sa dénonciation prend effet six (6) mois après réception de sa notification par écrit. Ladite notification n'a pas d'effet sur les droits et obligations des Parties relatifs aux informations classifiées relevant du présent Accord.

En foi de quoi les représentants des deux Parties, dûment autorisés à cet effet, ont signé le présent Accord et y ont apposé leur sceau.

Fait à Bratislava, le 26 janvier 2010 en double exemplaire en langues slovaque et française, les deux textes faisant également foi.

**Pour le Gouvernement de
la République slovaque**



.....
František Blanárik
Directeur de
l'Autorité nationale de sécurité

**Pour le Gouvernement de
la République française**



.....
Henry Cuny
Ambassadeur de France
en Slovaquie

ANNEXE 1

Tout contrat classifié conclu en vertu des dispositions du présent Accord doit comprendre un guide de classification ainsi que des informations relatives aux instructions de sécurité. Lesdites instructions doivent être conformes à celles qui émanent de l'Autorité de sécurité compétente de la Partie d'origine.

L'annexe de sécurité porte sur les aspects suivants :

- a) l'engagement pris par le contractant de s'assurer que les personnes qui ont besoin d'avoir accès à des informations classifiées dans l'exercice de leurs fonctions ont fait l'objet de l'habilitation de sécurité appropriée ;
- b) l'engagement pris par le contractant de s'assurer que toutes les personnes qui ont accès à des informations classifiées sont informées de leur responsabilité en matière de protection desdites informations en vertu des lois et règlements appropriés ;
- c) la désignation des locaux où le contrat classifié doit être exécuté ;
- d) l'engagement pris par le contractant de permettre des inspections de sécurité de ses locaux ;
- e) la liste des informations classifiées et de leurs niveaux respectifs de classification ;
- f) la procédure de communication des changements de niveau de classification ;
- g) les modes de communication et les moyens de transmission électronique ;
- h) la procédure de transmission des informations classifiées ;
- i) la désignation des autorités compétentes chargées de coordonner la protection des informations classifiées en rapport avec le contrat classifié ;
- j) l'engagement de signaler toute infraction effective ou supposée aux lois et règlements afférents à la protection des informations classifiées relevant du contrat classifié.

ANNEXE 2

Toute demande de visite doit comporter les renseignements suivants :

- a) le nom, le prénom, la date et le lieu de naissance, la nationalité et le numéro de passeport ou de carte d'identité du visiteur ;
- b) l'emploi et la fonction du visiteur et le nom de l'organisme qu'il représente ou dont il relève ;
- c) la confirmation du niveau d'habilitation de sécurité du visiteur et de sa validité ;
- d) la date envisagée pour la visite et sa durée prévue ;
- e) l'objet de la visite et tous renseignements nécessaires précisant les sujets à traiter mettant en jeu des informations classifiées et le niveau de classification de celles-ci ;
- f) les noms des organismes et les locaux qui font l'objet de la visite ;
- g) les nom et prénom des personnes qui doivent être en rapport avec le visiteur ;
- h) la date, la signature et le timbre officiel de l'autorité de sécurité compétente du visiteur.

[SLOVAK TEXT – TEXTE SLOVAQUE]

Dohoda

medzi

vládou Slovenskej republiky

a

vládou Francúzskej republiky

o výmene a

vzájomnej ochrane

utajovaných skutočností

**Vláda Slovenskej republiky
a
vláda Francúzskej republiky**

(ďalej len „zmluvné strany“),

žejajúc si zabezpečiť ochranu utajovaných skutočností a materiálov vymenených alebo spoločne vytvorených štátmi zmluvných strán alebo verejnými alebo súkromnými inštitúciami, ktoré podliehajú ich vnútroštátnym právnym poriadkom,

sa dohodli takto:

**Článok 1
Vymedzenie pojmov**

Pre účely tejto dohody:

- 1.1 **„Utajovaná skutočnosť“** je informácia, dokument alebo materiál, bez ohľadu na svoju podobu, povahu alebo spôsob prenosu, či už hotová alebo v procese prípravy, ktorej bol pridelený stupeň utajenia, a ktorá podlieha v záujme národnej bezpečnosti a v súlade s vnútroštátnymi právnymi poriadkami štátov zmluvných strán ochrane pred neoprávnenou manipuláciou alebo akýmkoľvek iným druhom porušenia bezpečnosti.
- 1.2 **„Utajovaný kontrakt“** je kontrakt, subkontrakt alebo projekt, ktorého príprava alebo uskutočnenie si vyžaduje prístup k utajovaným skutočnostiam, ich použitie alebo výrobu utajovaných skutočností.
- 1.3 **„Kontrahent“** je akákoľvek fyzická osoba alebo právnická osoba majúca spôsobilosť rokovať o a uzatvárať utajované kontrakty.
- 1.4 **„Príslušný bezpečnostný orgán“** je národný bezpečnostný orgán alebo poverený bezpečnostný orgán určený štátom príslušnej zmluvnej strany ako zodpovedný za vykonávanie a dohľad nad vykonávaním tejto dohody v jednotlivých oblastiach.
- 1.5 **„Odvodzávajúca strana“** je štát zmluvnej strany, vrátane právnických osôb vo svojej jurisdikcii v súlade so svojim vnútroštátnym právnym poriadkom, ktorý odovzdáva utajovanú skutočnosť.
- 1.6 **„Priíjajúca strana“** je štát zmluvnej strany, vrátane právnických osôb vo svojej jurisdikcii v súlade so svojim vnútroštátnym právnym poriadkom, ktorému je utajovaná skutočnosť odovzdaná.
- 1.7 **„Hostiteľská strana“** je štát zmluvnej strany, na území ktorého sa uskutočňuje návšteva.
- 1.8 **„Need-to-know“** je potreba mať prístup k utajovaným skutočnostiam v rozsahu danej úradnej funkcie a pre uskutočnenie konkrétnej úlohy.
- 1.9 **„Tretia strana“** sú akékoľvek medzinárodné organizácie, vlády štátov, ktoré nie sú zmluvnými stranami tejto dohody, ako aj ich fyzické osoby a právnické osoby.

Článok 2 Rozsah uplatnenia

Táto dohoda ustanovuje spoločné bezpečnostné opatrenia týkajúce sa akýchkoľvek utajovaných skutočností vymenených medzi alebo spoločne vytvorených štátmi zmluvných strán vrátane právnických osôb v ich jurisdikcii v súlade s ich vnútroštátnymi právnymi poriadkami.

Článok 3 Národné bezpečnostné orgány

3.1 Národné bezpečnostné orgány sú:

pre Slovenskú republiku:
Národný bezpečnostný úrad
Budatínska 30
850 07 Bratislava

pre Francúzsku republiku:
Secrétariat général de la Défense nationale
51, bd de La Tour-Maubourg
75700 Paris 07 SP

3.2 Zmluvné strany sa diplomatickou cestou navzájom informujú o príslušných bezpečnostných orgánoch a ich kontaktných údajoch ako i o akejkoľvek súvisiacej zmene, ak nie je dohodnuté inak.

Článok 4 Pravidlá bezpečnosti

4.1 Štáty zmluvných strán podniknú v súlade so svojimi vnútroštátnymi právnymi poriadkami príslušné opatrenia na ochranu utajovaných skutočností odovzdaných alebo spoločne vytvorených podľa tejto dohody a pridelia utajovanej skutočnosti stupeň utajenia zodpovedajúci pridelenému národnej utajovanej skutočnosti v súlade s ustanovením 5.1.

4.2 Pri prijatí označí prijímajúca strana utajovanú skutočnosť vlastným národným stupňom utajenia v súlade s ekvivalenciou v ustanovení 5.1.

4.3 Prístup k utajovaným skutočnostiam sa prísne obmedzuje na fyzické osoby, ktoré sú riadne preverené a povinnosti ktorých si vyžadujú prístup k uvedeným utajovaným skutočnostiam na základe need-to-know.

4.4 Prijímajúca strana neznižuje stupeň utajenia ani neodtajní utajovanú skutočnosť bez predchádzajúceho písomného súhlasu odovzdávajúcej strany.

4.5 Štáty zmluvných strán sa bez zbytočného odkladu informujú o akejkoľvek zmene týkajúcej sa ochrany utajovaných skutočností vymenených alebo spoločne vytvorených podľa tejto dohody.

- 4.6 Odovzdané utajované skutočnosti sa nepoužijú na iný účel ako na ten, na ktorom sa dohodli príslušné bezpečnostné orgány.

Článok 5 **Stupne utajenia a ekvivalencia**

- 5.1 Zmluvné strany sa zaväzujú chrániť vymenené utajované skutočnosti a prijmú ekvivalenciu stupňov utajenia uvedené v nasledujúcej tabuľke:

Slovenská republika	Francúzska republika
PRÍSNE TAJNÉ	TRES SECRET DEFENSE
TAJNÉ	SECRET DEFENSE
DÓVERNÉ	CONFIDENTIEL DEFENSE
VYHRADENÉ	(vid' ustanovenia 5.2 a 5.3)

- 5.2 Francúzska republika bude spracovávať a ochraňovať utajované skutočnosti označené „VYHRADENÉ“ odovzdané Slovenskou republikou v súlade s platným vnútroštátnym právnym poriadkom vzťahujúcim sa na informácie označené „DIFFUSION RESTREINTE“.
- 5.3 Slovenská republika bude spracovávať a ochraňovať informácie označené „DIFFUSION RESTREINTE“ odovzdané Francúzskou republikou v súlade s platným vnútroštátnym právnym poriadkom vzťahujúcim sa na ochranu utajovaných skutočností označených „VYHRADENÉ“.
- 5.4 Na žiadosť jednej zmluvnej strany a s cieľom udržať ekvivalentné bezpečnostné štandardy poskytne druhá zmluvná strana všetky požadované informácie v súvislosti s vnútroštátnym právnym poriadkom a bezpečnostnými postupmi používanými na zabezpečenie ochrany utajovaných skutočností. Zmluvné strany súhlasia, že umožnia kontakty medzi svojimi príslušnými bezpečnostnými orgánmi.

Článok 6 **Postup pri bezpečnostných previerkach**

- 6.1 Pre prístup k utajovaným skutočnostiam vykoná každý štát zmluvnej strany v súlade s vlastným vnútroštátnym právnym poriadkom bezpečnostnú previerku.
- 6.2 Počas vykonávania bezpečnostnej previerky občana štátu jednej zo zmluvných strán, ktorý sa zdržiaval alebo sa zdržiava na území štátu druhej zmluvnej strany, si príslušné bezpečnostné orgány navzájom poskytnú pomoc v súlade s vnútroštátnymi právnymi poriadkami.
- 6.3 Príslušné bezpečnostné orgány si navzájom uznávajú bezpečnostné previerky priznané svojím občanom a právnickým osobám vo vzťahu k prístupu k utajovaným skutočnostiam v súlade s vlastným vnútroštátnym právnym poriadkom.

- 6.4 Príslušné bezpečnostné orgány sa navzájom informujú o zmenách týkajúcich sa bezpečnostných previerok ich občanov alebo právnických osôb podľa tejto dohody, najmä v prípade ich odňatia alebo zníženia stupňa oprávnenia.

Článok 7

Použitie utajovaných skutočností

- 7.1 Utajovaným skutočnostiam odovzdaným alebo spoločne vytvoreným podľa tejto dohody sa neznižuje stupeň utajenia, neodtajnia sa ani sa nesprístupnia tretej strane bez predchádzajúceho písomného súhlasu príslušného bezpečnostného orgánu štátu druhej zmluvnej strany.
- 7.2 Príslušný bezpečnostný orgán prijímajúcej strany pred odovzdaním akejkoľvek utajovanej skutočnosti prijatej od odovzdávajúcej strany kontrahentom:
- a) sa uistí, že kontrahenti a ich priestory sú spôsobilé poskytnúť náležitú ochranu utajovaným skutočnostiam,
 - b) sa uistí, že príslušný kontrahent a jeho priestory majú potrebný stupeň bezpečnostnej previerky,
 - c) uistí sa, že fyzické osoby majúce prístup k utajovaným skutočnostiam majú potrebný stupeň bezpečnostnej previerky a need-to-know a boli oboznámené so svojimi povinnosťami vyplývajúcimi z vnútroštátneho právneho poriadku,
 - d) vykoná bezpečnostné inšpekcie príslušných priestorov.

Článok 8

Preklad, rozmnožovanie a zničenie

- 8.1 Kópie a preklady utajovaných skutočností sa označia a chránia rovnako ako originály.
- 8.2 Utajované skutočnosti označené PRÍSNE TAJNÉ /TRES SECRET DEFENSE sa nerozmnožujú. Ďalšie pôvodné vyhotovenia môžu byť poskytnuté na základe písomnej žiadosti príslušnému bezpečnostnému orgánu odovzdávajúcej strany. Preklady utajovaných skutočností označených PRÍSNE TAJNÉ/ TRES SECRET DEFENSE možno vyhotoviť iba na základe predchádzajúceho písomného súhlasu príslušného bezpečnostného orgánu odovzdávajúcej strany.
- 8.3 Utajované skutočnosti označené PRÍSNE TAJNÉ/ TRES SECRET DEFENSE sa nezničia, ak ich zničenie nebolo vyslovene povolené odovzdávajúcou stranou. Keď už nie sú potrebné alebo keď uplynie ich lehota utajenia, vráti sa odovzdávajúcej strane v súlade s článkom 9.
- 8.4 Preklady a kópie utajovaných skutočností označených TAJNÉ /SECRET DEFENSE sa povolia iba na základe predchádzajúceho písomného súhlasu príslušného bezpečnostného orgánu odovzdávajúcej strany.

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

Článok 9 **Odozdávanie utajovaných skutočností**

9.1 Utajované skutočnosti sa odovzdávajú diplomatickou cestou, ak sa príslušné bezpečnostné orgány nedohodnú na inom spôsobe.

9.2 Odozdávanie sa vykonáva v súlade s týmito požiadavkami:

a) stupeň bezpečnostnej previerky kuriéra je aspoň na úrovni stupňa utajenia prenášaných utajovaných skutočností,

b) kuriér je stálym zamestnancom prijímajúcej alebo odosielajúcej právnickej osoby alebo patrí do správy jednej zo zmluvných strán a má osvedčenie kuriéra vydané v súlade s vnútroštátnym právnym poriadkom,

c) odovzdávajúca strana vedie register odovzdaných utajovaných skutočností a na žiadosť sa poskytne z neho výťah prijímajúcej strane,

d) utajované skutočnosti sa zabalia a zapečatia v súlade s vnútroštátnym právnym poriadkom odovzdávajúcej strany,

e) prijatie utajovaných skutočností sa potvrdí písomne bez zbytočného odkladu.

9.3 Utajované skutočnosti sa odovzdávajú elektronicky v zašifrovanej podobe, s použitím šifrovacích metód a prístrojov, na ktorých sa dohodnú príslušné bezpečnostné orgány.

Článok 10 **Utajované kontrakty**

10.1 Príslušný bezpečnostný orgán odovzdávajúcej strany upovedomí príslušný bezpečnostný orgán prijímajúcej strany o akýchkoľvek utajovaných kontraktoch pred výmenou utajovaných skutočností v súlade s vnútroštátnym právnym poriadkom. V uvedenom oznámení sa uvedie najvyšší stupeň utajenia zahrnutých utajovaných skutočností.

10.2 Štát zmluvnej strany, ktorý zamýšľa uzavrieť alebo poveriť kontrahenta vo svojej jurisdikcii, aby uzavrel utajovaný kontrakt s kontrahentom v jurisdikcii štátu druhej zmluvnej strany, si overí prostredníctvom príslušného bezpečnostného orgánu, že uvedený kontrahent má príslušný stupeň bezpečnostnej previerky pre vykonanie utajovaného kontraktu. V prípade neexistencie potrebnej bezpečnostnej previerky dá príslušný bezpečnostný orgán prijímajúcej strany na žiadosť príslušného bezpečnostného orgánu druhej zmluvnej strany a v súlade s vlastným vnútroštátnym právnym poriadkom podnet na jej začatie.

10.3 Pred uzavretím utajovaného kontraktu si príslušné bezpečnostné orgány poskytnú písomné uistenie, že navrhovaný kontrahent má príslušný stupeň bezpečnostnej

previerky a že podnikol všetky potrebné bezpečnostné opatrenia na ochranu utajovaných skutočností. Príslušné bezpečnostné orgány si tiež navzájom bez zbytočného odkladu oznámia, ak bola bezpečnostná previerka danej právnickej osobe zamietnutá.

- 10.4 Každý utajovaný kontrakt obsahuje list o bezpečnostných aspektoch, bližšie upravený v Prílohe 1.
- 10.5 Príslušný bezpečnostný orgán odovzdávajúcej strany zašle kópiu listu o bezpečnostných aspektoch príslušnému bezpečnostnému orgánu prijímajúcej strany.
- 10.6 Príslušné bezpečnostné orgány sa uistia, že v rámci výkonu utajovaných kontraktov, je použitá a udržiavaná úroveň bezpečnosti zodpovedajúca tej, ktorá je potrebná pre ochranu vlastných utajovaných kontraktov.
- 10.7 Utajované subkontrakty sa vykonávajú so súhlasom príslušného bezpečnostného orgánu a každý subkontrahent splní rovnaké bezpečnostné záväzky ako kontrahent v súlade s touto dohodou.

Článok 11

Návštevy

- 11.1 Návštevy zahŕňajúce prístup k utajovaným skutočnostiam podľa tejto dohody podliehajú predchádzajúcemu písomnému povoleniu príslušného bezpečnostného orgánu hostiteľskej strany.
- 11.2 Návštevy priestorov na území štátu jednej zmluvnej strany občanmi tretieho štátu, ktoré zahŕňajú prístup k utajovaným skutočnostiam podľa tejto dohody, podliehajú predchádzajúcemu písomnému povoleniu príslušného bezpečnostného orgánu štátu druhej zmluvnej strany.
- 11.3 Pri návštevách podľa ustanovení 11.1 a 11.2 majú všetci návštevníci príslušný stupeň bezpečnostnej previerky a need-to-know.
- 11.4 Žiadosti o vykonanie návštevy zahŕňajúce prístup k utajovaným skutočnostiam stupňa utajenia PRÍSNE TAJNÉ/ TRES SECRET DEFENSE sa zašlú národnému bezpečnostnému orgánu hostiteľskej strany diplomatickou cestou. Žiadosti o vykonanie návštevy zahŕňajúce prístup k utajovaným skutočnostiam nižšieho stupňa utajenia sa vybavujú priamo medzi príslušnými bezpečnostnými orgánmi. Žiadosti sa zašlú aspoň tri (3) týždne vopred. Žiadosti o vykonanie návštevy obsahujú informácie uvedené v Prílohe 2.
- 11.5 Platnosť povolenia na vykonanie návštevy neprekročí dvanásť (12) mesiacov. Ak by návšteva nebola vykonaná v danej lehote alebo ak by bolo potrebné predĺženie platnosti povolenia, možno požiadať o nové povolenie o vykonanie návštevy aspoň tri (3) týždne pred uplynutím platnosti predchádzajúceho povolenia, ak sa príslušné bezpečnostné orgány nedohodnú inak.
- 11.6 Všetci návštevníci sa podriaďujú bezpečnostným pravidlám a inštrukciám hostiteľskej strany.

Článok 12

Opakované návštevy

- 12.1 Zmluvné strany môžu zostaviť zoznam osôb oprávnených na viaceré návštevy v súvislosti s akoukoľvek aktivitou v súlade so štandardnými podmienkami, na ktorých sa dohodnú príslušné bezpečnostné orgány. Tento zoznam bude platný najprv dvanásť (12) mesiacov, pričom táto lehota môže byť na základe dohody príslušných bezpečnostných orgánov predĺžená o ďalšie obdobia, ktoré úhromom nepresiahnú dvanásť (12) mesiacov.
- 12.2 Zoznam podľa ustanovenia 12.1 sa zostaví v súlade s vnútroštátnym právnym poriadkom hostiteľskej strany. Po jeho schválení sa na podmienkach konkrétnych návštev môžu dohodnúť priamo právnické osoby, ktorých sa to týka. Žiadosti o vykonanie návštevy obsahujú informácie uvedené v Prílohe 2.

Článok 13

Porušenie vnútroštátneho právneho poriadku

- 13.1 Ak je podozrenie alebo sa zistí porušenie vnútroštátneho právneho poriadku vo vzťahu k ochrane utajovaných skutočností podľa tejto dohody, príslušný bezpečnostný orgán štátu druhej zmluvnej strany sa s uvedeným bez zbytočného odkladu písomne oboznámi.
- 13.2 Oznámenie obsahuje dostatočné množstvo podrobností na to, aby mohla odovzdávajúca strana vyhodnotiť celkové následky.
- 13.3 Štát zmluvnej strany, ktorý mal podozrenie alebo zistil skutočnosti uvedené v ustanovení 13.1, bez zbytočného odkladu vykoná vyšetrovanie v súlade s vnútroštátnym právnym poriadkom. Štát druhej zmluvnej strany na žiadosť pri vyšetrovaní spolupracuje. Príslušný bezpečnostný orgán štátu druhej zmluvnej strany sa oboznámi bez zbytočného odkladu s výsledkami vyšetrovania, podniknutými opatreniami a opatreniami na nápravu.

Článok 14

Náklady

Každá zmluvná strana znáša vlastné náklady vzniknuté počas vykonávania tejto dohody.

Článok 15

Riešenie sporov

- 15.1 Akýkoľvek spor v súvislosti s výkladom alebo vykonávaním tejto dohody sa rieši výlučne priamymi konzultáciami.
- 15.2 V čase trvania sporu sa zmluvné strany zaväzujú dodržiavať záväzky uvedené v tejto dohode.

Článok 16 Záverečné ustanovenia

- 16.1 Nadobudnutím platnosti tejto dohody skončí platnosť Všeobecnej bezpečnostnej dohody medzi vládou Slovenskej republiky a vládou Francúzskej republiky, podpísanej v Paríži 20. marca 1997. Aj po zániku platnosti Všeobecnej bezpečnostnej dohody medzi vládou Slovenskej republiky a vládou Francúzskej republiky utajované skutočnosti vymenené a vytvorené podľa nej zostávajú utajovanými skutočnosťami a chránia sa v súlade s ustanoveniami tejto dohody.
- 16.2 Táto dohoda sa uzatvára na neurčitý čas a nadobúda platnosť v prvý deň druhého mesiaca nasledujúceho po prijatí neskoršej notifikácie, ktorou si zmluvné strany diplomatickou cestou oznamujú splnenie všetkých právnych podmienok potrebných pre nadobudnutie jej platnosti.
- 16.3 Príslušné bezpečnostné orgány uskutočňujú konzultácie o konkrétnych technických aspektoch súvisiacich s implementáciou tejto dohody a v prípade potreby môžu uzavrieť vhodné právne nástroje alebo zvláštne bezpečnostné protokoly na doplnenie tejto dohody.
- 16.4 Zmluvné strany sa navzájom informujú o akejkoľvek zmene v príslušnom vnútroštátnom právnom poriadku. V takom prípade uskutočnia zmluvné strany konzultácie s cieľom posúdiť prípadnú potrebu zmeny tejto dohody. Utajované skutočnosti sú zatiaľ chránené v súlade s týmito podmienkami.
- 16.5 Túto dohodu možno meniť na základe písomného súhlasu oboch zmluvných strán. Zmeny nadobudnú platnosť v súlade s ustanovením 16.2, ak nie je dohodnuté inak.
- 16.6 Platnosť tejto dohody možno ukončiť jednostranne alebo na základe vzájomnej dohody. V prípade výpovede platnosť dohody skončí šesť (6) mesiacov odo dňa prijatia písomného oznámenia druhej zmluvnej strane. Oznámenie o skončení platnosti nemá vplyv na práva a povinnosti zmluvných strán vo vzťahu k utajovaným skutočnostiam podľa tejto dohody.

Na tento účel riadne poverení zástupcovia oboch zmluvných strán, dosvedčujúc uvedené, podpísali a zapečatili túto dohodu.

Dané v Bratislave, dňa 26. januára 2010, v dvoch pôvodných vyhotoveniach, každé v slovenskom a francúzskom jazyku, pričom obe znenia majú rovnakú platnosť.

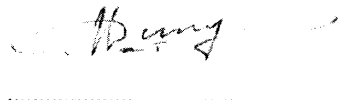
Za vládu Slovenskej republiky



.....
František Blanárik

riaditeľ Národného bezpečnostného úradu

Za vládu Francúzskej republiky



.....
Henry Cuny

vel'vyslanec Francúzska na Slovensku

Príloha I

Každý utajovaný kontrakt uzavretý podľa ustanovení tejto dohody obsahuje klasifikačného sprievodcu a informácie týkajúce sa bezpečnostných pokynov. Uvedené pokyny sú v súlade s tými, ktoré vydá príslušný bezpečnostný orgán odovzdávajúcej strany.

Príslušný list o bezpečnostných aspektoch obsahuje:

- a) záväzok kontrahenta zabezpečiť, aby osoby, ktoré potrebujú na vykonávanie svojich povinností prístup k utajovaným skutočnostiam, boli náležite preverené,
- b) záväzok kontrahenta zabezpečiť, že všetky osoby s prístupom k utajovaným skutočnostiam sú oboznámené so svojimi povinnosťami vo vzťahu k ochrane utajovaných skutočností v súlade s vnútroštátnym právnym poriadkom,
- c) označenie priestorov, kde sa má utajovaný kontrakt uskutočniť,
- d) záväzok kontrahenta povoliť inšpekcie svojich priestorov,
- e) zoznam utajovaných skutočností a ich stupne utajenia,
- f) postup pre oznámenie zmien v stupňoch utajenia,
- g) komunikačné kanály a prostriedky elektronického prenosu,
- h) postup pre odovzdanie utajovaných skutočností,
- i) označenie orgánov príslušných pre koordináciu ochrany utajovaných skutočností v súvislosti s utajovaným kontraktom,
- j) záväzok oznámiť akékoľvek skutočné porušenie vnútroštátneho právneho poriadku alebo podozrenie naň vo vzťahu k ochrane utajovaných skutočností v rámci utajovaného kontraktu.

Príloha 2

Žiadosť o vykonanie návštevy obsahuje:

- a) meno a priezvisko, dátum a miesto narodenia, štátne občianstvo a číslo pasu alebo identifikačnej karty návštevníka,
- b) zamestnanie a pracovné zaradenie návštevníka, názov právnickej osoby, ktorú návštevník reprezentuje alebo ku ktorej patrí,
- c) potvrdenie stupňa bezpečnostnej previerky návštevníka a jej platnosti,
- d) navrhovaný dátum návštevy a jej plánované trvanie,
- e) účel návštevy a potrebné informácie konkretizujúce veci, o ktoré pôjde, vrátane utajovaných skutočností a ich stupňov utajenia,
- f) názvy právnických osôb a ich priestorov, ktorých sa návštevy týkajú,
- g) mená a priezviská fyzických osôb, ktoré sa majú stretnúť s návštevníkmi,
- h) dátum, podpis a odtlačok úradnej pečiatky príslušného bezpečnostného orgánu návštevníka.

[TRANSLATION – TRADUCTION]

AGREEMENT BETWEEN THE GOVERNMENT OF THE SLOVAK REPUBLIC AND THE GOVERNMENT OF THE FRENCH REPUBLIC CONCERNING THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Slovak Republic and the Government of the French Republic, hereinafter referred to as “the Parties”,

Desiring to guarantee the protection of classified information and material exchanged between the States of the Parties or between public or private agencies which are subject to their respective national legislation and regulations, or jointly produced by them,

Have agreed as follows:

Article 1. Definitions

For the purposes of this Agreement:

1.1 “Classified information” means information, documents and materials, regardless of their form, nature or manner of transmission, whether they exist or are being developed, which have been assigned a level of classification or protection and which, in the interest of national security and pursuant to the national legislation and regulations of the States of the Parties, require protection against any unauthorized manipulation or any other type of security violation.

1.2 “Classified contract” means a contract, subcontract or project whose development or performance requires access to classified information or the use and production of classified information.

1.3 “Contractor” means any individual or legal entity having the legal capacity to negotiate and conclude classified contracts.

1.4 “Competent security authority” means the national security authority entrusted by the State of the Party concerned with the implementation and monitoring of this Agreement, in relation to the relevant field.

1.5 “Originating Party” means the State of the Party, including any legal entity subject to its jurisdiction by virtue of its national legislation and regulations, which transmits classified information.

1.6 “Recipient Party” means the State of the Party, including any legal entity subject to its jurisdiction by virtue of its national legislation and regulations, to which classified information is transmitted.

1.7 “Host Party” means the State of the Party in whose territory a visit takes place.

1.8 “Need to know” means the need to have access to classified information within the framework of a specific official duty and for carrying out a specific task.

1.9 “Third party” means any international organization or Government of a State that is not a Party to this Agreement and any legal entity or national of such a State.

Article 2. Scope

This Agreement constitutes the common security rules applicable to any classified information exchanged between the States of the Parties, including any legal entity placed under their jurisdiction by virtue of their national legislation and regulations, or jointly produced by them.

Article 3. National security authorities

3.1 The national security authorities are as follows:

For the Slovak Republic:

Národný bezpečnostný úrad

Butadínska 30

850 07 Bratislava;

For the French Republic:

Secrétariat général de la Défense nationale

51, bd de La Tour-Maubourg

75700 Paris 07 SP.

3.2 The Parties shall inform each other through the diplomatic channel, unless different provisions are agreed upon, of the relevant competent security authorities and the contact points thereof, and of any related change.

Article 4. Principles of security

4.1 In accordance with their respective national legislation and regulations, the States of the Parties shall take appropriate measures to ensure the protection of classified information transmitted or jointly produced under this Agreement and shall accord to such information a level of security classification equivalent to that accorded to information of their own that is classified in accordance with the provisions of article 5, paragraph 5.1.

4.2 Upon receiving classified information, the recipient Party shall affix thereto its own national classification in accordance with the equivalent defined in article 5, paragraph 5.1.

4.3 Access to classified information shall be restricted to persons with an appropriate level of clearance, whose duties necessitate access to such information, based on the need to know.

4.4 The recipient Party shall neither downgrade nor declassify any transmitted classified information without the prior written consent of the originating Party.

4.5 The States of the Parties shall mutually inform each other, without undue delay, of any change affecting the protection of classified information exchanged or jointly produced under this Agreement.

4.6 Transmitted classified information shall not be used for purposes other than those agreed upon between the competent security authorities.

Article 5. Security classifications and equivalents

5.1 The Parties undertake to ensure the protection of classified information that is exchanged and adopt the security classification level equivalents defined in the following table:

Slovak Republic	French Republic	English Translation
PRÍSNE TAJNÉ	TRÈS SECRET DÉFENSE	TOP SECRET
TAJNÉ	SECRET DÉFENSE	SECRET
DOVERNÉ	CONFIDENTIEL DÉFENSE	CONFIDENTIAL
VYHRADENÉ	(See paragraphs 2 and 3 below)	

5.2 Information bearing the mark “VYHRADENÉ” that is transmitted by the Slovak Republic shall be handled and protected by the French Republic in accordance with its national legislation and regulations in force concerning classified information bearing the mark “DIFFUSION RESTREINTE” [RESTRICTED DISTRIBUTION].

5.3 Information bearing the mark “DIFFUSION RESTREINTE” that is transmitted by the French Republic shall be handled and protected by the Slovak Republic in accordance with its national legislation and regulations in force concerning classified information bearing the mark “VYHRADENÉ”.

5.4 In order to maintain comparable security norms, each Party, at the request of the other Party, shall furnish all required information concerning the national legislation, regulations and security procedures applied in order to guarantee the security of classified information. The Parties shall facilitate contact between their respective competent security authorities.

Article 6. Security clearance procedure

6.1 For access to classified information, the State of each Party shall implement a security clearance procedure in accordance with its national legislation and regulations.

6.2 In the framework of the procedure of security clearance of a national of the State of one of the Parties who has stayed or is still staying in the territory of the State of the other Party, the competent security authorities shall lend each other mutual assistance in accordance with their national legislation and regulations.

6.3 The competent security authorities shall mutually recognize security clearances issued in accordance with their national legislation and regulations to their nationals and to their legal entities in connection with access to classified information.

6.4 The competent security authorities shall keep each other informed of changes concerning the security clearances of their nationals or of the legal entities concerned by this Agreement, in particular in the case of withdrawal of clearance or lowering of the clearance level.

Article 7. Use of classified information

7.1 Classified information transmitted or jointly produced by the Parties under this Agreement may not be downgraded, declassified or transmitted to a third party without the prior written consent of the competent security authority of the State of the other Party.

7.2 Prior to transmission to contractors of any classified information received from the originating Party, the competent security authorities of the recipient Party shall:

(a) Ensure that the contractors and their premises are able to protect classified information appropriately;

(b) Ensure that the contractor considered and the contractor's facilities have a security clearance of the required level;

(c) Ensure that persons who have access to the classified information have a security clearance of the required level, have a need to know and have been informed of their responsibilities under the relevant the national legislation and regulations;

(d) Proceed with security checks in the facilities concerned.

Article 8. Translation, reproduction and destruction

8.1 Reproductions and translations of classified information shall be marked and protected in the same manner as the originals.

8.2 Information classified as PRÍSNE TAJNÉ / TRÈS SECRET DÉFENSE [TOP SECRET] may not be reproduced. Additional originals may be supplied upon written request addressed to the competent security authority of the originating Party. Translations of information classified as PRÍSNE TAJNÉ / TRÈS SECRET DÉFENSE [TOP SECRET] shall be possible solely on the basis of prior written consent of the originating Party.

8.3 Information classified as PRÍSNE TAJNÉ / TRÈS SECRET DÉFENSE [TOP SECRET] may not be destroyed unless the originating Party expressly authorizes such destruction. Such information shall be returned to the originating Party in accordance with article 9 after being recognized as no longer necessary or upon expiration of its classification.

8.4 Translation and reproduction of information classified as TAJNÉ / SECRET DÉFENSE [SECRET] shall be permitted solely on the basis of prior written consent of the competent security authority of the originating Party.

8.5 Classified information shall be destroyed in a manner precluding its full or partial reconstruction.

Article 9. Transmission of classified information

9.1 Classified information shall be transmitted through the diplomatic channel unless other modalities are agreed upon between the competent security authorities.

9.2 Transmission shall meet the following requirements:

- (a) The courier must have security clearance of a level at least equal to that of the classified information to be transmitted;
- (b) The courier must be a permanent employee of the originating or recipient organization or of the administration of either Party and must hold a courier pass issued in accordance with the relevant legislation and regulations;
- (c) The originating Party must keep a register of the classified information transmitted and provide an extract thereof to the recipient Party upon request;
- (d) The classified information must be duly packaged and sealed in accordance with the national legislation and regulations of the originating Party;
- (e) Receipt of classified information must be confirmed in writing without undue delay.

9.3 Electronic transmission of classified information shall take place in encrypted form only, with use of cryptographic methods and devices approved by the competent security authorities.

Article 10. Classified contracts

10.1 Prior to exchange of classified information, the competent security authority of the originating Party shall inform the competent security authority of the recipient Party of any classified contract, in accordance with its national legislation and regulations. Such notification must indicate the highest classification level of the information involved.

10.2 The State of a Party which wishes to conclude, or to authorize a contractor subject to its jurisdiction to conclude, a classified contract with a contractor subject to the jurisdiction of the State of the other Party shall ascertain from the appropriate competent security authority that the said contractor has clearance at the level required for performing the classified contract. Failing that, the competent security authority of the recipient Party shall begin, at the request of the competent security authority of the other Party, in accordance with its national legislation and regulations, the required clearance process.

10.3 Before any conclusion of a classified contract, the competent security authority must have received from its counterpart written assurance that the proposed contractor has clearance at the required level and has taken all required security measures to protect classified information. Moreover, the competent security authorities are informed without undue delay of any refusal to grant clearance.

10.4 Every classified contract must include a security annex drawn up in accordance with annex 1.

10.5 The competent security authority of the originating Party shall transmit a copy of the security annex to the competent security authority of the recipient Party

10.6 The competent security authorities shall see to it that, in connection with the performance of classified contracts, a level of security equivalent to that required for the protection of their own classified contracts is applied and maintained.

10.7 The consent of the competent security authority is required for the performance of any classified subcontracting contract. All subcontractors must fulfil the same security obligations as the contractor, in accordance with the provisions of this Agreement.

Article 11. Visits

11.1 Visits involving access to classified information under this Agreement shall be subject to prior written authorization from the competent security authority of the host Party.

11.2 Such visits by nationals of a third State to facilities located in the territory of the State of one Party as may involve access to classified information under this Agreement shall be subject to prior written authorization from the competent security authority of the State of the other Party.

11.3 For the visits provided for in paragraphs 11.1 and 11.2 above, every visitor must have a security clearance of the appropriate level and a need to know.

11.4 Requests for visits necessitating access to classified information of PRÍSNE TAJNÉ / TRÈS SECRET DÉFENSE [TOP SECRET] level shall be transmitted through the diplomatic channel to the competent security authority of the host Party. Requests for visits necessitating access to a lower level of classified information shall be handled directly between the respective competent national authorities. Requests shall be submitted at least three (3) weeks beforehand. Requests for visits shall contain the information specified in Annex 2.

11.5 The period of validity of an authorization to visit may not exceed twelve (12) months. If it is impossible to carry out a visit within the time limit provided for or if it is necessary to extend the period of validity of an authorization, a new authorization to visit may be requested, at least three (3) weeks before the expiration of the current authorization, unless competent security authorities establish different provisions by common agreement.

11.6 All visitors shall respect the security regulations and instructions of the host Party.

Article 12. Multiple visits

12.1 The Parties may draw up a list of staff authorized to carry out more than one visits in relation to an activity in accordance with the modalities agreed upon by the competent security authorities. That list shall be valid for an initial 12-month period which, by agreement between the competent security authorities, may be extended for additional periods not exceeding twelve (12) months.

12.2 The list referred to in paragraph 12.1 shall be drawn up in conformity with the national legislation and regulations of the host Party. Once that list has been approved, the modalities of specific visits may be defined directly by the agencies concerned. The visit requests must include the information referred to in Annex 2.

Article 13. Violation of legislation and regulations

13.1 Where a violation of national legislation or regulations on the protection of classified information under this Agreement is presumed or discovered, the competent security authority of the State of the other Party shall be notified accordingly in writing without undue delay.

13.2 Such notification must be sufficiently detailed to enable the originating Party to assess the consequences fully.

13.3 The State of the Party having discovered or suspected the acts referred to in article 13, paragraph 13.1, shall immediately conduct an inquiry in accordance with its national legislation and regulations. The State of the other Party shall cooperate in the inquiry upon request. The competent security authority of the other Party shall be informed without undue delay of the findings of the inquiry, the measures decided upon and the corrective action taken.

Article 14. Costs

Each Party shall bear the costs incurred by it in the framework of the implementation of this Agreement.

Article 15. Settlement of disputes

15.1 Any dispute concerning the interpretation or application of this Agreement shall be settled exclusively through consultations.

15.2 The Parties undertake to respect their obligations under this Agreement throughout the duration of the dispute.

Article 16. Final provisions

16.1 On the date of its entry into force, this Agreement shall cancel and replace the General Security Agreement between the Government of the Slovak Republic and the Government of the French Republic, signed in Paris on 20 March 1997. Once that General Security Agreement ceases to have effect, the classified information exchanged or produced under it shall remain classified and be protected under the present Agreement.

16.2 This Agreement is concluded for an indefinite period and shall enter into force on the first day of the second month following the receipt of the last notification by which the Parties certify through the diplomatic channel the completion of the legal procedures necessary for such entry into force.

16.3 The competent security authorities shall consult each other as necessary on particular technical matters connected with the implementation of this Agreement and may conclude as necessary any appropriate arrangement or specific protocol related to security and supplementing this Agreement.

16.4 Each Party shall inform the other of any change to its relevant national legislation or regulations. In such a case, the Parties shall consult each other in order to consider

possible amendments to this Agreement. In the meantime, classified information shall continue to be protected in accordance with the provisions of this Agreement.

16.5 This Agreement may be amended by written accord between the two Parties. Such amendments shall take effect in accordance with paragraph 16.2, unless different provisions are established by mutual agreement.

16.6 This Agreement may be terminated by mutual consent or unilaterally. Such termination shall take effect six (6) months after receipt of the relevant written notification. The said notification shall not affect the Parties' rights and obligations regarding classified information covered by this Agreement.

IN WITNESS WHEREOF, the representatives of the two Parties, duly authorized to that purpose, have signed this Agreement and affixed their seals hereto.

DONE at Bratislava on 26 January 2010, in duplicate, in the Slovak and French languages, both texts being equally authentic.

For the Government of the Slovak Republic:

FRANTIŠEK BLANÁRIK
Director of the National security authority

For the Government of the French Republic:

HENRY CUNY
Ambassador of France in Slovakia

ANNEX 1

Any classified contract concluded under this Agreement must include a classification guide and information related to security instructions. Such instructions must be in line with those issued by the competent security authority of the originating Party.

The security annex shall cover the following elements:

(a) Contractor's commitment to ensuring that the persons who need to have access to classified information in the performance of their duties have been granted appropriate security clearance;

(b) Contractor's commitment to ensuring that all persons who have access to classified information are informed of their responsibility as regards the protection of the said information under the relevant legislation and regulations;

(c) Designation of the premises where the classified contract must be performed;

(d) Contractor's commitment to authorizing security inspections of those premises;

(e) List of classified information and of the respective clearance levels;

(f) Procedure for communicating clearance level changes;

(g) Methods of communication and means of electronic transmission;

(h) Procedure for transmitting classified information;

(i) Designation of the competent authorities entrusted with coordinating the protection of classified information connected with the classified contract;

(j) Commitment to reporting any actual or presumed infringement of the legislation and regulations related to the protection of classified information concerned by the classified contract.

ANNEX 2

Any request for a visit must include the following information:

- (a) Surname, given name, date and place of birth, nationality and passport number or identity card number;
- (b) Post and duties of the visitor and name of the organization that he or she represents or comes under the authority of;
- (c) Confirmation of the visitor's security clearance level and of its validity;
- (d) Planned date and duration of the visit;
- (e) Purpose of the visit and any necessary information, specifying matters to be treated that involve classified information and its level of classification;
- (f) Names of organizations and premises to be visited;
- (g) Surnames and given names of the persons to be in contact with the visitor;
- (h) Date, signature and official stamp of the visitor's competent security authority.