No. 48637

France
and
Slovenia

Agreement between the Government of the French Republic and the Government of Republic Slovenia concerning the reciprocal protection and exchange of classified information. Ljubljana, 16 November 2009

Entry into force: *1 October 2010 by notification, in accordance with article 15*

Authentic texts: *French and Slovene*

Registration with the Secretariat of the United Nations: *France, 24 June 2011*

France
et
Slovénie

Accord entre le Gouvernement de la République française et le Gouvernement de la République de Slovénie concernant la protection réciproque et l'échange d'informations classifiées. Ljubljana, 16 novembre 2009

Entrée en vigueur : *1er octobre 2010 par notification, conformément à l'article 15*

Textes authentiques : *français et slovène*

Enregistrement auprès du Secrétariat des Nations Unies : *France, 24 juin 2011*

[FRENCH TEXT – TEXTE FRANÇAIS]

ACCORD

ENTRE

LE GOUVERNEMENT DE LA RÉPUBLIQUE FRANÇAISE

ET

LE GOUVERNEMENT DE LA RÉPUBLIQUE DE SLOVÉNIE

CONCERNANT

LA PROTECTION RÉCIPROQUE ET L'ÉCHANGE

D'INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République Française, et le Gouvernement de la République de Slovénie d'autre part, ci-après dénommés « les Parties », souhaitant garantir la protection des Informations classifiées échangées ou produites entre les deux Etats ou entre des organismes publics ou privés placés sous leur juridiction, dans le respect mutuel de leurs intérêts nationaux et de leur sécurité nationale, sont convenus de ce qui suit :

ARTICLE 1
DÉFINITIONS

Aux fins du présent Accord, on entend par :

1. **« Information classifiée » :** les Informations, documents et supports, quelle qu'en soit la forme, y compris ceux en cours d'élaboration, nécessitant une protection contre toute violation, destruction, détournement, divulgation, perte, accès non autorisé ou toute autre forme de compromission et ayant été désignés en tant que tels conformément aux lois et réglementations nationales de l'une ou l'autre des Parties.

2. **« Contrat classé » :** un contrat, contrat de sous-traitance ou projet dont l'élaboration et l'exécution nécessitent l'accès à des Informations classifiées ou l'utilisation et la production d'Informations classifiées.

3. **« Partie à un contrat classé » :** toute personne physique ou morale possédant la capacité juridique de négocier et de conclure des Contrats classés.

4. **« Autorité nationale de sécurité » (ANS) :** l'autorité nationale responsable du contrôle général et de la mise en application du présent Accord pour chacune des Parties.

5. **« Autorités de sécurité compétentes » :** toute autorité de sécurité désignée ou toute autre entité compétente autorisée conformément aux lois et réglementations nationales des Parties, qui est responsable de la mise en application du présent Accord selon les domaines concernés.

6. **« Partie d'origine » :** la Partie, y compris tout organisme public ou privé placé sous sa juridiction, qui transmet une Information classifiée à l'autre Partie.

7. **« Partie destinataire » :** la Partie, y compris tout organisme public ou privé placé sous sa juridiction, qui reçoit une Information classifiée transmise par la Partie d'origine.

8. **« Tierce Partie » :** un Etat, y compris tout organisme public ou privé ou tout individu placé sous la juridiction de celui-ci, ou une organisation internationale n'étant pas partie au présent Accord.

9. **« Partie hôte » :** la Partie sur le territoire de laquelle une visite a lieu.

10. **« Besoin d'en connaître » :** la nécessité d'avoir accès à des Informations classifiées dans le cadre d'une fonction officielle déterminée et pour l'exécution d'une mission spécifique.

ARTICLE 2
ÉQUIVALENCES DES CLASSIFICATIONS DE SÉCURITÉ

1. Les Informations classifiées transmises en vertu du présent Accord sont identifiées par le marquage correspondant aux niveaux de classification de sécurité appropriés conformément aux lois et réglementations nationales des Parties.

2. Les équivalences entre les marquages correspondant aux classifications de sécurité de chacune des Parties sont établies comme suit :

FRANCE	SLOVÉNIE
TRES SECRET DEFENSE	STROGO TAJNO
SECRET DEFENSE	TAJNO
CONFIDENTIEL DEFENSE	ZAUPNO
(NB)	INTERNO

NB : La partie française traite et protège les informations portant la mention « INTERNO » transmises par la partie slovène, conformément à ses lois et réglementations nationales en vigueur relatives aux informations protégées mais non classifiées, telles que celles portant la mention « DIFFUSION RESTREINTE ».
La partie slovène traite et protège les informations non classifiées portant la mention « DIFFUSION RESTREINTE » transmises par la partie française conformément à ses lois et réglementations nationales en vigueur relatives à la protection des Informations portant la mention « INTERNO ».

3. Les Autorités nationales de sécurité se tiennent mutuellement informées de tout marquage supplémentaire qui pourrait être utilisé dans le cadre du présent Accord.

4. Dans certains cas et pour des raisons de sécurité particulières, lorsque la Partie d'origine exige que l'accès à des Informations classifiées de niveau « CONFIDENTIEL DEFENSE / ZAUPNO » et au dessus soit limité aux personnes ayant exclusivement la nationalité[1] des Parties, ces Informations portent un avertissement supplémentaire « SPÉCIAL FRANCE – SLOVÉNIE ».

[1] La nationalité française est l'équivalent de la citoyenneté slovène au regard des lois et réglementations.

ARTICLE 3
AUTORITÉS NATIONALES DE SÉCURITÉ

1. L'Autorité Nationale de Sécurité de chacune des Parties est :

Pour la République Française :
Secrétariat général de la défense nationale (S.G.D.N.)

Pour la République de Slovénie :
Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. Les Autorités nationales de sécurité se tiennent mutuellement informées de toutes autres Autorités de sécurité compétentes responsables de la mise en application du présent Accord.

3. Les Parties s'informent immédiatement de tout changement affectant leurs Autorités nationales de sécurité de même que leurs Autorités de Sécurité Compétentes et affectant la mise en application du présent Accord.

ARTICLE 4
ACCÈS AUX INFORMATIONS CLASSIFIÉES

1. L'accès aux informations portant la mention « DIFFUSION RESTREINTE / INTERNO» est limité aux personnes qui ont le besoin d'en connaître et qui ont été informées en conséquence.

2. L'accès aux Informations classifiées de niveau « CONFIDENTIEL DEFENSE / ZAUPNO» et de niveau supérieur est limité aux personnes qui disposent d'une habilitation de sécurité conformément aux lois et réglementations nationales et qui ont été autorisées à accéder à ces Informations en fonction du besoin d'en connaître.

3. Conformément à l'application des règles procédurales prescrites par leurs lois et réglementations nationales respectives, les Parties reconnaissent mutuellement leurs habilitations de sécurité du personnel concernant l'accès aux Informations classifiées. Les dispositions du deuxième paragraphe de l'article 2 du présent Accord s'appliquent en conséquence.

ARTICLE 5
PROTECTION DES INFORMATIONS CLASSIFIÉES

1. Conformément à leurs lois et réglementations nationales respectives, les Parties accordent aux Informations classifiées mentionnées dans le présent Accord la même protection qu'elles apportent à leurs propres Informations pour un niveau de classification de sécurité équivalent.

2. La Partie d'origine :
   a) s'assure que les Informations classifiées portent le marquage correspondant au niveau de classification approprié conformément à ses lois et réglementations nationales ;
   b) informe la Partie destinataire :
      - de toutes conditions liées à leur transmission ou de toute limitation de leur utilisation,
      - de tout changement de classification éventuel.

3. La Partie destinataire :
   a) appose aux Informations classifiées transmises par la Partie d'origine, dès réception de celles-ci, son propre niveau de classification nationale conformément aux dispositions de l'article 2, paragraphe 2 du présent Accord.
   b) ne déclasse ni ne déclassifie une Information classifiée sans l'accord écrit préalable de la Partie d'origine.

4. Les Parties se tiennent mutuellement informées dans les meilleurs délais de tout changement affectant la protection des Informations classifiées échangées ou produites en vertu du présent Accord.

5. Les Parties veillent à ce que soit satisfaite toute exigence découlant de leurs lois et réglementations de sécurité nationales s'appliquant à la sécurité des agences, bureaux et installations placés sous leur juridiction.

ARTICLE 6
UTILISATION DES INFORMATIONS CLASSIFIÉES

1. Les Informations classifiées transmises ne sont utilisées à aucune autre fin que celle faisant l'objet de leur transmission, conformément aux dispositions du présent Accord ou des instruments contractuels conclus par les Parties.

2. La Partie destinataire ne divulgue les Informations classifiées échangées ou produites au titre du présent Accord à aucune Tierce Partie sans l'accord écrit préalable de l'Autorité nationale de sécurité ou des Autorités de sécurité compétentes de la Partie d'origine.

3. Les Informations classifiées élaborées conjointement par les Parties dans le cadre d'accords, de contrats ou de toute autre activité commune ne sont ni déclassées ni déclassifiées ou transmises à une Tierce Partie sans le consentement écrit préalable des deux Parties.

4. Avant de transmettre à une Partie à un contrat classé toute Information classifiée reçue de la Partie d'origine, les Autorités de sécurité compétentes de la Partie destinataire :

   a) s'assurent que la Partie à un contrat classé et ses installations sont capables de fournir une protection appropriée aux Informations classifiées ;

   b) attribuent le niveau d'habilitation requis aux installations de la Partie à un contrat classé concernée ;

c) attribuent le niveau d'habilitation requis aux personnes ayant le besoin d'en connaître ;

d) s'assurent que toutes les personnes qui ont accès aux Informations classifiées sont informées de leurs responsabilités qui découlent des lois et réglementations nationales en vigueur ;

e) effectuent des contrôles de sécurité dans les installations concernées.

5. Si l'Autorité nationale de sécurité nationale ou les Autorités de sécurité compétentes de l'une des Parties considère qu'une société enregistrée sur son territoire national est la propriété ou est sous l'influence d'un Etat tiers dont les objectifs ne sont pas compatibles avec ses intérêts, ladite société ne se verra pas délivrer de certificat d'habilitation. L'Autorité nationale de sécurité de la Partie ayant formulé la demande d'habilitation de sécurité est avisée par écrit en conséquence dans les meilleurs délais.

ARTICLE 7
TRANSMISSION DES INFORMATIONS CLASSIFIÉES

1. Les Informations classifiées sont échangées entre les Parties par la voie diplomatique conformément aux lois et réglementations nationales de la Partie d'origine.

2. Les Autorités nationales de sécurité ou les Autorités de sécurité compétentes peuvent, d'un commun accord et conformément aux lois et réglementations nationales des Parties, convenir de ce que les Informations classifiées soient transmises par un autre moyen que la voie diplomatique, dans la mesure où ce mode de transmission s'avère inadapté.

3. La transmission d'Informations classifiées répond aux exigences suivantes :

a. le convoyeur est un employé permanent de l'expéditeur ou du destinataire, ou relève de l'administration publique, et est en possession d'une habilitation de sécurité correspondant au moins au niveau de classification des Informations à convoyer ;

b. le convoyeur est muni d'un certificat de courrier délivré par les autorités compétentes de l'envoyeur ou du bénéficiaire ;

c. la Partie d'origine tient un registre des Informations classifiées transmises ; un extrait de ce registre est fourni sur demande à la Partie destinataire ;

d. les Informations classifiées sont dûment emballées et scellées conformément aux lois et réglementations nationales de la Partie d'origine ;

e. la réception des Informations classifiées est confirmée par écrit dans les meilleurs délais.

4. La transmission d'une importante quantité d'Informations classifiées est organisée entre les Autorités nationales de sécurité ou les Autorités de sécurité compétentes respectives des Parties au cas par cas.

5. Les Informations classifiées sont transmises électroniquement sous forme cryptée, en utilisant des méthodes et dispositifs cryptographiques mutuellement acceptés par les Autorités nationales de sécurité ou les Autorités de sécurité compétentes respectives des Parties, en accord avec leurs lois et réglementations nationales.

ARTICLE 8

REPRODUCTION, TRADUCTION ET DESTRUCTION

1. Toutes les traductions et reproductions d'Informations classifiées sont identifiées par le marquage de classification de sécurité approprié et bénéficient de la même protection que les originaux. Les traductions et le nombre de reproductions sont limités aux quantités nécessaires à un usage officiel.

2. Toute traduction comporte une annotation appropriée, rédigée dans la langue de la traduction, indiquant que le document contient des Informations classifiées transmises par la Partie d'origine.

3. Les Informations classifiées de niveau « TRES SECRET DEFENSE / STROGO TAJNO» ne sont ni traduites ni reproduites. Des exemplaires supplémentaires peuvent être fournis sur demande écrite auprès de la Partie d'origine. Les Informations classifiées de niveau « TRES SECRET DEFENSE / STROGO TAJNO» ne sont pas détruites, sauf autorisation expresse de la Partie d'origine et conformément aux dispositions du paragraphe 5 de l'article 8 du présent accord. Elles sont restituées à la Partie d'origine conformément à l'article 7 du présent Accord, après avoir été reconnues comme n'étant plus nécessaires ou à l'expiration de leur validité.

4. La traduction et la reproduction d'Informations classifiées de niveau « TAJNO / SECRET DEFENSE» sont autorisées uniquement avec l'accord écrit de l'Autorité nationale de sécurité ou des Autorités de sécurité compétentes de la Partie d'origine.

5. Les Informations classifiées sont détruites de telle manière que leur reconstruction totale ou partielle soit impossible.

ARTICLE 9
VISITES

1. Les visites aux installations de l'une des Parties où un représentant de l'autre Partie a accès à des Informations classifiées, ou à des sites où l'accès à de telles Informations est directement possible requièrent l'autorisation écrite préalable de l'Autorité nationale de sécurité ou des Autorités de sécurité compétentes de la Partie hôte conformément à ses lois et réglementations nationales.

2. Les visites aux installations de l'une des Parties par des ressortissants d'une Tierce Partie impliquant l'accès à des Informations classifiées échangées ou produites par les Parties, ou à des sites où l'accès à de telles informations est directement possible requièrent l'autorisation préalable écrite de l'Autorité nationale de sécurité ou des Autorités de sécurité compétentes de l'autre Partie.

3. Les demandes pour des visites nécessitant un accès à des Informations classifiées de niveau « STROGO TAJNO / TRES SECRET DEFENSE » sont transmises par la voie diplomatique à l'Autorité nationale de sécurité de la Partie hôte. Les demandes concernant des visites impliquant un accès à des Informations classifiées de niveau inférieur sont traitées directement entre les Autorités nationales de sécurité ou les Autorités de sécurité compétentes respectives de chacune des Parties, conformément à leurs lois et réglementations nationales. Les demandes sont adressées au moins vingt (20) jours avant la date requise pour la visite.

4. Les demandes de visite contiennent les renseignements suivants :

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

   b) la fonction du visiteur ainsi que des précisions sur l'établissement qu'il représente, ou le titre et les détails du Contrat classé auquel il est partie ;

   c) le niveau d'habilitation de sécurité du visiteur, authentifié par un certificat de sécurité devant être délivré par l'Autorité nationale de sécurité ou les Autorités de sécurité compétentes de la Partie requérante conformément à ses lois et réglementations nationales ;

   d) le nom, l'adresse, le numéro de téléphone / de télécopie, le courriel et le point de contact des établissements, installations et locaux objets de la visite, ainsi que les noms et prénoms des personnes qui doivent recevoir le visiteur ;

   e) l'objet de la visite et toutes les indications nécessaires précisant les sujets à traiter impliquant des informations classifiées et leurs niveaux de classification ;

   f) la date proposée de la visite et la durée prévue. En cas de visites multiples, la durée totale de l'ensemble des visites est précisée ;

   g) la date, la signature et l'apposition du timbre officiel de l'autorité compétente de la Partie requérante.

5. En cas d'urgence, les demandes de visite sont transmises au moins cinq (5) jours ouvrés avant le début de la visite.

6. Les Parties peuvent dresser une liste des personnels autorisés à effectuer plusieurs visites dans le cadre de tout projet, programme ou contrat spécifique, conformément aux conditions générales convenues par les Autorités nationales de sécurité ou les Autorités de sécurité compétentes des Parties. Initialement, ces listes sont valables pour une durée de douze (12) mois et, par accord entre les Autorités nationales de sécurité ou les Autorités de sécurité compétentes des Parties, cette durée peut être prolongée pour d'autres périodes

n'excédant pas douze (12) mois au total. Lesdites listes sont établies conformément aux lois et réglementations nationales de la Partie hôte. Une fois ces listes approuvées, les conditions générales de toute visite particulière peuvent être déterminées directement par les établissements que les personnes mentionnées sur ces listes vont visiter.

7. Toute Information classifiée dont un visiteur prend connaissance est considérée en tant qu'Information classifiée transmise au titre du présent Accord.

8. Tous les visiteurs respectent les réglementations et instructions de sécurité de la Partie hôte.

ARTICLE 10
CONTRATS CLASSÉS

1. Conformément à l'application des règles procédurales prescrites par leurs lois et réglementations nationales respectives, les Parties reconnaissent mutuellement leurs habilitations de sécurité d'établissement. Les dispositions du deuxième paragraphe de l'article 2 du présent Accord s'appliquent en conséquence.

2. Avant de conclure un Contrat classé avec une Partie à un contrat classé placée sous la juridiction de l'autre Partie, ou d'autoriser l'une de ses propres Parties à un contrat classé à conclure un Contrat classé sur le territoire de l'autre Partie, une Partie reçoit au préalable l'assurance écrite de l'Autorité nationale de sécurité ou des Autorités de sécurité compétentes de l'autre Partie, conformément aux lois et réglementations nationales de celle-ci, que la Partie à un contrat classé proposée a reçu une habilitation de niveau approprié et qu'elle a pris toutes les mesures de sécurité appropriées nécessaires à la protection des Informations classifiées.

3. Les Autorités de sécurité compétentes de chacune des Parties peuvent demander qu'une inspection de sécurité soit effectuée auprès d'une installation donnée afin d'assurer le respect des normes de sécurité conformément aux lois et réglementations nationales.

4. Tout Contrat classé contient des informations relatives aux instructions de sécurité ainsi qu'un guide de classification. Ces instructions sont conformes à celles dispensées par les Autorités de sécurité compétentes de la Partie d'origine.

5. Une annexe de sécurité est ajoutée à tout instrument contractuel contenant des Informations classifiées. Dans cette annexe, l'Autorité nationale de sécurité ou les Autorités de sécurité compétentes de la Partie d'origine précise ce qui doit être protégé par la Partie destinataire, ainsi que le niveau de classification applicable correspondant. Seule la Partie d'origine peut modifier le niveau de classification d'une Information définie dans une annexe de sécurité.

6. L'Autorité nationale de sécurité ou les Autorités de sécurité compétentes de la Partie d'origine transmet une copie de l'annexe de sécurité à l'Autorité nationale de sécurité ou aux Autorités de sécurité compétentes de l'autre Partie.

7. La Partie ayant l'intention de conclure ou d'autoriser l'une de ses Parties à un contrat classé à conclure un Contrat classé avec une Partie à un contrat classé de l'autre Partie s'assure

auprès de l'Autorité nationale de sécurité ou des Autorités de sécurité compétentes de l'autre Partie que la Partie à un contrat classé concernée détient le niveau d'habilitation approprié nécessaire à l'exécution dudit contrat. Dans la négative, l'Autorité nationale de sécurité ou les Autorités de sécurité compétentes de la Partie destinataire entame une procédure d'habilitation au niveau requis.

8. Les Autorités de sécurité compétentes de la Partie d'origine notifient aux Autorités de sécurité compétentes de la Partie destinataire tout Contrat classé avant tout échange d'Informations classifiées. Cette notification doit préciser le plus haut niveau de classification des Informations impliquées dans le contrat concerné.

9. Les Autorités de sécurité compétentes de la Partie sur le territoire de laquelle le travail doit être exécuté sont tenues de veiller à ce que, dans le cadre de l'exécution de Contrat classé, soit appliqué et maintenu un niveau de sécurité équivalent à celui requis pour la protection de leurs propres Contrats.

10. Avant de passer un Contrat classé avec un sous-traitant, la Partie à un contrat classé reçoit l'autorisation de ses Autorités de sécurité compétentes. Les sous-traitants se conforment aux mêmes conditions de sécurité que celles établies pour la Partie à un contrat classé.

ARTICLE 11
COOPÉRATION DE SÉCURITÉ

1. Afin d'atteindre et de maintenir des normes de sécurité comparables, l'Autorité nationale de sécurité ou les Autorités de sécurité compétentes de chacune des Parties fournit à l'autre, sur demande, des informations concernant ses lois, réglementations, normes, procédures et pratiques de sécurité nationales relatives à la protection des Informations classifiées. À cette fin, les Parties consentent à faciliter les contacts entre leurs Autorités nationales de sécurité et leurs Autorités de sécurité compétentes respectives qui peuvent organiser des visites mutuelles.

2. Les Autorités nationales de sécurité ou les Autorités de sécurité compétentes de chacune des Parties se tiennent mutuellement informées des risques de sécurité pouvant compromettre les Informations classifiées transmises.

3. S'agissant de l'habilitation de sécurité d'un ressortissant de l'une des Parties qui séjourne ou a séjourné plus de trois mois sur le territoire de l'autre Partie, les Autorités nationales de sécurité ou les Autorités de sécurité compétentes de chacune des Parties se prêtent assistance conformément à leurs lois et réglementations nationales respectives.

4. Conformément à leurs lois et réglementations nationales, les Autorités nationales de sécurité ou les Autorités de sécurité compétentes se tiennent mutuellement informées des changements relatifs aux habilitations de sécurité de leurs ressortissants en vertu du présent Accord, en particulier en cas de retrait ou de déclassement du niveau d'accès d'une habilitation.

ARTICLE 12
VIOLATION DES LOIS ET DES RÉGLEMENTATIONS RELATIVES À LA PROTECTION DES INFORMATIONS CLASSIFIÉES

1. Chacune des Parties notifie sans délai à l'autre Partie toute infraction ou compromission présumée ou avérée affectant la sécurité des Informations classifiées échangées ou produites au titre du présent Accord. La notification doit être suffisamment détaillée pour que la Partie d'origine puisse procéder à une évaluation complète des conséquences.

2. La partie ayant découvert ou suspectant les faits mène immédiatement une enquête (avec l'aide de l'autre Partie, si nécessaire), conformément aux lois et réglementations nationales en vigueur dans l'État concerné. La Partie qui mène l'enquête informe dans les meilleurs délais l'Autorité nationale de sécurité ou les Autorités de sécurité compétentes de l'autre Partie des résultats de l'enquête, des mesures adoptées et des actions correctrices engagées.

ARTICLE 13
FRAIS

1. Il n'est pas prévu que cet Accord génère de frais spécifiques.

2. Tout frais éventuel encouru par une Partie du fait de l'application du présent Accord est supporté par cette seule Partie.

ARTICLE 14
INTERPRÉTATION ET RÈGLEMENT DES LITIGES

1. Tout litige quant à l'interprétation ou l'application du présent Accord est exclusivement résolu dans le cadre de consultations entre les Parties.

2. Pendant la durée du litige, les Parties continuent à respecter les obligations découlant du présent Accord.

ARTICLE 15
DISPOSITIONS FINALES

1. Le présent Accord est conclu pour une durée indéterminée. Il est soumis à l'approbation des Parties, conformément à leurs procédures juridiques nationales, et entre en vigueur le premier jour du second mois suivant la date de la dernière des notifications échangées entre les Parties confirmant l'accomplissement des exigences nécessaires à l'entrée en vigueur du présent Accord.

2. Le présent Accord peut être modifié à tout moment d'un commun accord par écrit entre les Parties. Les modifications prennent effet selon les modalités prévues au premier paragraphe de cet article.

3. En tant que de besoin, les Autorités nationales de sécurité ou les Autorités de sécurité compétentes des Parties se consultent au sujet des aspects techniques spécifiques concernant l'application du présent Accord et peuvent conclure, au cas par cas, tout instrument juridique approprié ou protocole de sécurité spécifique en vue de compléter le présent Accord.

4. Dans le cas où une modification des lois et réglementations nationales des Parties est susceptible d'avoir un effet sur la protection des Informations classifiées en vertu du présent Accord, les Parties se concertent afin d'examiner toute modification éventuelle du présent Accord.

5. Chacune des Parties peut dénoncer le présent Accord à tout moment par écrit. Le cas échéant, la validité du présent Accord prend fin six (6) mois à compter de la réception par l'autre Partie de la notification de la dénonciation.

6. Nonobstant la dénonciation du présent Accord, toute Information classifiée transmise en vertu du présent Accord continue d'être protégée conformément aux dispositions énoncées dans le présent Accord jusqu'à ce que la Partie d'origine dispense la Partie destinataire de cette obligation.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé le présent Accord.

Fait à Ljubljana, le 16 novembre 2009 en double exemplaire, en langues française et slovène, les deux textes faisant également foi.

Pour le Gouvernement de la République Française

N Michel

Ambassadrice de France en République de Slovénie

Pour le Gouvernement de la République de Slovénie

Secrétaire général du Gouvernement de la République de Slovénie

[SLOVENE TEXT – TEXTE SLOVÈNE]

SPORAZUM

MED

VLADO FRANCOSKE REPUBLIKE

IN

VLADO REPUBLIKE SLOVENIJE

O

IZMENJAVI IN MEDSEBOJNEM VAROVANJU

TAJNIH PODATKOV

Vlada Francoske republike in Vlada Republike Slovenije, v nadaljevanju "pogodbenici", sta se v želji, da bi zagotovili varovanje tajnih podatkov, izmenjanih ali nastalih med njima ali med javnimi in zasebnimi subjekti v njuni pristojnosti, ob vzajemnem upoštevanju državnih interesov in varnosti dogovorili:

1. ČLEN
POMEN IZRAZOV

V tem sporazumu izrazi pomenijo:

1. **"tajni podatek":** podatek, dokument in gradivo, ki ne glede na obliko tudi med nastajanjem zahtevajo varovanje pred kršitvijo, uničenjem, odtujitvijo, razkritjem, izgubo ali nepooblaščenim dostopom ali kakršno koli drugo vrsto ogrožanja in so kot taki določeni po notranjih zakonih in drugih predpisih pogodbenice;

2. **"pogodba s tajnimi podatki":** pogodba, podizvajalska pogodba ali projekt, za pripravo in izvedbo katerega se zahtevata dostop do tajnih podatkov ali njihova uporaba in ustvarjanje tajnih podatkov;

3. **"stranka pogodbe s tajnimi podatki":** fizična ali pravna oseba, ki ima pravno sposobnost za pogajanje in sklepanje pogodb s tajnimi podatki;

4. **"nacionalni varnostni organ" (NVO):** državni organ, ki je za vsako pogodbenico odgovoren za splošni nadzor nad sporazumom in njegovo izvajanje;

5. **"pristojni varnostni organi":** kateri koli imenovani varnostni organ ali pristojni pravni subjekt, ki je pooblaščen v skladu z notranjimi zakoni in drugimi predpisi pogodbenic ter odgovoren za izvajanje sporazuma glede na zadevna področja;

6. **"pogodbenica izvora":** pogodbenica, vključno z javnimi ali zasebnimi subjekti v njeni pristojnosti, ki da tajne podatke drugi pogodbenici;

7. **"pogodbenica prejemnica":** pogodbenica, vključno z javnimi ali zasebnimi subjekti v njeni pristojnosti, ki prejme tajne podatke od pogodbenice izvora;

8. **"tretja stran":** država, vključno z javnimi ali zasebnimi subjekti ali posamezniKom v njeni pristojnosti, ali mednarodna organizacija, ki ni pogodbenica sporazuma;

9. **"gostiteljica":** pogodbenica, na ozemlju katere poteka obisk;

10. **"potreba po seznanitvi":** potreba po dostopu do tajnih podatkov v okviru določenega službenega položaja in za izvedbo določene naloge.

2. ČLEN
ENAKOVREDNOST STOPENJ TAJNOSTI

1. Tajni podatki, dani na podlagi sporazuma, se označijo z ustreznimi stopnjami tajnosti po zakonih in drugih predpisih pogodbenic.

2. Enakovredne oznake stopenj tajnosti so:

FRANCIJA	SLOVENIJA
TRES SECRET DEFENSE	STROGO TAJNO
SECRET DEFENSE	TAJNO
CONFIDENTIEL DEFENSE	ZAUPNO
(Opomba)	INTERNO

(Opomba) Francoska stran podatke z oznako "INTERNO", ki jih da slovenska stran, obravnava in varuje po svojih veljavnih zakonih in drugih predpisih, ki veljajo za varovane, ne pa tajne podatke, in so označeni kot "DIFFUSION RESTREINTE".
Slovenska stran podatke z oznako "DIFFUSION RESTREINTE", ki niso tajni in jih da francoska stran, obravnava in varuje po svojih veljavnih zakonih in drugih predpisih, ki veljajo za varovanje podatkov z oznako "INTERNO".

3. Nacionalna varnostna organa se obveščata o vseh dodatnih oznakah tajnosti, ki bi se lahko uporabljale po tem sporazumu.

4. Kadar pogodbenica izvora v posebnih primerih in iz posebnih varnostnih razlogov zahteva, da je dostop do tajnih podatkov stopnje tajnosti CONFIDENTIEL DEFENSE/ZAUPNO ali višje omejen na osebe, ki imajo izključno državljanstvo[1] pogodbenic, je pri takih podatkih dodano še opozorilo "SPECIAL FRANCE – SLOVENIA".

3. ČLEN
NACIONALNA VARNOSTNA ORGANA

1. Nacionalna varnostna organa pogodbenic sta:

v Francoski republiki:
Secrétariat général de la défense nationale (S. G. D. N.),

[1] Opomba: Izrazu "nationalité française" v Franciji je v Sloveniji po veljavnih zakonih in predpisih enakovreden izraz "slovensko državljanstvo".

v Republiki Sloveniji:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

2. Nacionalna varnostna organa se uradno obvestita o pristojnih varnostnih organih, ki so odgovorni za izvajanje sporazuma.

3. Pogodbenici se takoj obvestita o vsaki spremembi, ki se nanaša na njuna nacionalna varnostna organa in njune pristojne varnostne organe ter vpliva na izvajanje sporazuma.

4. ČLEN
DOSTOP DO TAJNIH PODATKOV

1. Dostop do podatkov z oznako DIFFUSION RESTREINTE/INTERNO je omejen na osebe, za katere velja načelo potrebe po seznanitvi in so bile ustrezno usposobljene.

2. Dostop do podatkov stopnje CONFIDENTIEL DEFENSE/ZAUPNO in višje je omejen na osebe, ki so bile v skladu z notranjimi zakoni in drugimi predpisi varnostno preverjene in pooblaščene za dostop do takih podatkov po načelu potrebe po seznanitvi.

3. Če so izpolnjene postopkovne zahteve, določene v notranjih zakonih in drugih predpisih, pogodbenici medsebojno priznavata dovoljenja za dostop do tajnih podatkov. Skladno s tem se uporablja drugi odstavek 2. člena.

5. ČLEN
VAROVANJE TAJNIH PODATKOV

1. Pogodbenici skladno s svojimi notranjimi zakoni in drugimi predpisi tajnim podatkom iz sporazuma zagotavljata enako varovanje kakor svojim podatkom enake stopnje tajnosti.

2. Pogodbenica izvora:
   a) zagotovi, da imajo tajni podatki ustrezno oznako tajnosti v skladu z njenimi notranjimi zakoni in drugimi predpisi;
   b) obvesti pogodbenico prejemnico o:
      – pogojih dajanja tajnih podatkov ali omejitvah njihove uporabe,
      – vseh morebitnih spremembah stopnje tajnosti.

3. Pogodbenica prejemnica:
   a) tajne podatke pogodbenice izvora takoj ob prejemu opremi s svojo nacionalno oznako stopnje tajnosti skladno z drugim odstavkom 2. člena;
   b) ne zniža ali prekliče stopnje tajnosti danih tajnih podatkov brez predhodnega pisnega soglasja pogodbenice izvora.

4. Pogodbenici se takoj, ko je mogoče, obvestita o vseh spremembah, ki vplivajo na varovanje tajnih podatkov, izmenjanih ali nastalih po tem sporazumu.

5. Pogodbenici zagotavljata ravnanje v skladu z vsemi zahtevami, ki izhajajo iz njunih zakonov in drugih predpisov o nacionalni varnosti ter se nanašajo na varnost državnih organov, uradov in organizacij v njuni pristojnosti.

6. ČLEN
UPORABA TAJNIH PODATKOV

1. Tajni podatki se smejo uporabiti izključno za namene, za katere so bili dani po tem sporazumu ali po pogodbah, sklenjenih med pogodbenicama.

2. Pogodbenica prejemnica tajnih podatkov, izmenjanih ali nastalih po tem sporazumu, ne sme razkriti tretji strani brez predhodnega pisnega soglasja nacionalnega varnostnega organa ali pristojnih varnostnih organov pogodbenice izvora.

3. Tajnim podatkom, ki jih pogodbenici pripravita skupaj po sporazumih, pogodbah ali pri katerem koli drugem skupnem opravilu, ni mogoče znižati ali preklicati stopnje tajnosti ali jih dati tretji strani brez predhodnega pisnega soglasja pogodbenic.

4. Preden se tajni podatki pogodbenice izvora dajo strankam pogodbe s tajnimi podatki, pristojni varnostni organi pogodbenice prejemnice:

   a) zagotovijo, da je stranka pogodbe s tajnimi podatki v svojih objektih sposobna poskrbeti za ustrezno varovanje tajnih podatkov;

   b) ustrezno varnostno preverijo objekte te stranke pogodbe s tajnimi podatki;

   c) ustrezno varnostno preverijo posameznike na podlagi načela potrebe po seznanitvi;

   d) zagotovijo, da so vsi posamezniki, ki imajo dostop do tajnih podatkov, seznanjeni s svojo odgovornostjo, ki izhaja iz veljavnih notranjih zakonov in drugih predpisov;

   e) opravijo varnostni nadzor v zadevnih objektih.

5. Če nacionalni varnostni organ ali pristojni varnostni organi ene pogodbenice menijo, da ima registrirano družbo na njenem državnem ozemlju v lasti ali jo obvladuje tretja država, katere cilji niso združljivi z njenimi interesi, se omenjeni družbi varnostno dovoljenje ne izda. Nacionalni varnostni organ pogodbenice, ki je zaprosil za varnostno dovoljenje organizacije, mora biti o tem čim prej ustrezno pisno obveščen.

7. ČLEN
PRENOS TAJNIH PODATKOV

1. Tajni podatki se med pogodbenicama izmenjavajo po diplomatski poti v skladu z notranjimi zakoni in drugimi predpisi pogodbenice izvora.

2. Nacionalna varnostna organa ali pristojni varnostni organi se lahko z medsebojnim soglasjem ter spoštovanjem notranjih zakonov in drugih predpisov dogovorijo, da prenos tajnih podatkov poteka drugače kakor po diplomatski poti, če se izkaže, da ta način prenosa ni primeren.

3. Prenos mora ustrezati naslednjim zahtevam:

   a) kurir mora biti redno zaposlen pri pošiljatelju ali prejemniku ali biti uslužbenec javne uprave in mora imeti dovoljenje za dostop do tajnih podatkov najmanj enake stopnje, kakor so tajni podatki, ki jih mora prenesti;

   b) kurir mora imeti kurirsko potrdilo, ki ga izda pristojni organ pošiljateljice ali prejemnice;

   c) pogodbenica izvora vodi evidenco o prenosu tajnih podatkov; na zahtevo se izpisek iz te evidence predloži pogodbenici prejemnici;

   d) tajni podatki morajo biti pravilno zapakirani in zapečateni v skladu z notranjimi zakoni in drugimi predpisi pogodbenice izvora;

   e) prejem tajnih podatkov je treba čim hitreje pisno potrditi.

4. Prenos večje količine tajnih podatkov se med nacionalnima varnostnima organoma ali pristojnimi varnostnimi organi organizira za vsak primer posebej.

5. Elektronski prenos tajnih podatkov poteka v šifrirani obliki z uporabo kriptografskih metod in pripomočkov, ki jih skupaj odobrita nacionalna varnostna organa ali pristojni varnostni organi ob upoštevanju notranjih zakonov in drugih predpisov.

8. ČLEN

RAZMNOŽEVANJE, PREVAJANJE IN UNIČEVANJE

1. Vsi izvodi in prevodi tajnih podatkov se označijo z ustrezno stopnjo tajnosti in varujejo kot izvirni tajni podatki. Prevodi in število izvodov se omejijo na količino, potrebno za službene namene.

2. Vsi prevodi morajo v jeziku prevoda imeti ustrezno oznako, da vsebujejo tajne podatke pogodbenice izvora.

3. Tajni podatki z oznako TRES SECRET DEFENSE/STROGO TAJNO se ne smejo prevajati ali razmnoževati. S pisnim zaprosilom, naslovljenim na pogodbenico izvora, se lahko zagotovijo dodatni izvirni dokumenti. Tajni podatki z oznako TRES SECRET DEFENSE/STROGO TAJNO se ne smejo uničiti, razen če pogodbenica izvora izrecno pisno ne dovoli uničenja v skladu z določbami petega odstavka 8. člena sporazuma. Po izteku njihove veljavnosti ali ko niso več potrebni, se v skladu s 7. členom vrnejo pogodbenici izvora.

4. Prevajanje in razmnoževanje tajnih podatkov z oznako SECRET DEFENSE/TAJNO sta dovoljeni samo s pisnim dovoljenjem nacionalnega varnostnega organa/pristojnih varnostnih organov pogodbenice izvora.

5. Tajni podatki se uničijo tako, da jih ni mogoče več delno ali v celoti obnoviti.

9. ČLEN
OBISKI

1. Za obiske objektov ene pogodbenice, pri katerih ima predstavnik druge pogodbenice dostop do tajnih podatkov, ali za obiske krajev, pri katerih je do takih podatkov mogoč neposreden dostop, je treba predhodno pridobiti pisno dovoljenje nacionalnega varnostnega organa ali pristojnih varnostnih organov pogodbenice gostiteljice v skladu z njenimi notranjimi zakoni in drugimi predpisi.

2. Za obiske objektov ene pogodbenice, ki jih opravijo državljani tretje strani in pri katerih je mogoč dostop do tajnih podatkov, izmenjanih ali nastalih med pogodbenicama, ali za obiske krajev, pri katerih je do takih podatkov mogoč neposreden dostop, je treba predhodno pridobiti pisno dovoljenje nacionalnega varnostnega organa ali pristojnih varnostnih organov druge pogodbenice.

3. Zaprosila za obiske, pri katerih se zahteva dostop do tajnih podatkov stopnje TRES SECRET DEFENSE/STROGO TAJNO, se po diplomatski poti pošljejo nacionalnemu varnostnemu organu pogodbenice gostiteljice. Zaprosila za obiske, pri katerih se zahteva dostop do tajnih podatkov nižje stopnje tajnosti, se izmenjajo neposredno med nacionalnima varnostnima organoma ali zadevnimi pristojnimi varnostnimi organi skladno z notranjimi zakoni in drugimi predpisi. Zaprosila je treba poslati najmanj dvajset (20) dni pred dnevom predvidenega obiska.

4. Zaprosilo za obisk mora vključevati naslednje podatke:

   a) ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo in številko osebne izkaznice ali potnega lista;

   b) položaj obiskovalca s podatki o organizaciji, ki jo predstavlja, ali naslov in podrobne podatke o pogodbi s tajnimi podatki, pri kateri obiskovalec sodeluje;

   c) stopnjo dovoljenja za dostop do tajnih podatkov obiskovalca, izkazano z varnostnim potrdilom, ki ga izda nacionalni varnostni organ ali pristojni varnostni organ pogodbenice prosilke skladno z notranjimi zakoni in drugimi predpisi;

   d) ime, naslov, telefonsko številko, številko telefaksa, elektronski naslov in osebo za stike ustanov, organizacij in prostorov, v katerih bo potekal obisk; ime in priimek oseb, ki bodo obiskovalca sprejele;

   e) namen obiska in vse potrebne informacije, ki natančneje določajo teme obravnave, zaradi katerih se zahteva dostop do tajnih podatkov, in stopnje njihove tajnosti;

   f) predlagane datume in trajanje obiska. Pri večkratnih obiskih se navede celotno obdobje, v katerem bodo potekali;

   g) datum, podpis in uradni žig pristojnega organa pogodbenice prosilke.

5. Zaprosilo za obisk se v nujnih primerih predloži najmanj pet (5) delovnih dni pred začetkom obiska.

6. Pogodbenici lahko pripravita seznam pooblaščenega osebja za izvedbo večkratnih obiskov v zvezi s katerim koli projektom, programom ali posebno pogodbo skladno s splošnimi pogoji, dogovorjenimi med nacionalnima varnostnima organoma ali pristojnimi varnostnimi organi pogodbenic. Omenjeni seznami veljajo dvanajst (12) mesecev, s sporazumom med nacionalnima varnostnima organoma ali pristojnimi varnostnimi organi pogodbenic pa se veljavnost lahko podaljša za obdobja, ki skupaj trajajo največ dvanajst (12) mesecev. Ti seznami se sestavijo v skladu z notranjimi zakoni in drugimi predpisi pogodbenice gostiteljice. Po odobritvi seznamov lahko organizacije, ki jih bodo obiskale osebe s seznama, same pripravijo splošne pogoje katerih koli posebnih obiskov.

7. Vsak tajni podatek, s katerim se obiskovalec seznani, se šteje kot tajni podatek, dan po tem sporazumu.

8. Vsi obiskovalci morajo ravnati v skladu s predpisi o varovanju tajnosti in navodili pogodbenice gostiteljice.

10. ČLEN
POGODBA S TAJNIMI PODATKI

1. Pogodbenici ob izpolnjevanju postopkovnih zahtev, ki jih določajo njuni notranji zakoni in drugi predpisi, medsebojno priznavata varnostna dovoljenja organizacij. Skladno s tem se uporablja drugi odstavek 2. člena.

2. Pred sklenitvijo pogodbe s tajnimi podatki s stranko pogodbe s tajnimi podatki, ki je v pristojnosti druge pogodbenice, ali pooblastitvijo ene od svojih strank pogodbe s tajnimi podatki za sklenitev pogodbe s tajnimi podatki na ozemlju druge pogodbenice mora pogodbenica najprej pridobiti pisno zagotovilo nacionalnega varnostnega organa ali pristojnih varnostnih organov druge pogodbenice, skladno z njenimi notranjimi zakoni in drugimi predpisi, da je predlagani stranki pogodbe s tajnimi podatki priznana ustrezna stopnja varovanja tajnih podatkov in da je sprejela vse ustrezne varnostne ukrepe za njihovo varovanje.

3. Pristojni varnostni organi vsake pogodbenice lahko zahtevajo, da se opravi varnostni inšpekcijski pregled objekta zaradi zagotavljanja spoštovanja varnostnih standardov po notranjih zakonih in drugih predpisih.

4. Vse pogodbe s tajnimi podatki morajo vsebovati podatke o navodilih o varovanju tajnosti in pojasnila o stopnjah tajnosti. Ta navodila morajo biti v skladu s tistimi, ki jih dajo pristojni varnostni organi pogodbenice izvora.

5. Za vsak pogodbeni dokument, ki vsebuje tajne podatke, se pripravi varnostni dodatek. V njem nacionalni varnostni organ ali pristojni varnostni organi pogodbenice izvora podrobno opredelijo, kaj mora pogodbenica prejemnica varovati, in ustrezno stopnjo tajnosti. Stopnjo tajnosti podatkov, določeno v varnostnem dodatku, sme spremeniti samo pogodbenica izvora.

6. Nacionalni varnostni organ ali pristojni varnostni organi pogodbenice izvora pošljejo izvod varnostnega dodatka nacionalnemu varnostnemu organu ali pristojnim varnostnim organom druge pogodbenice.

7. Pogodbenica, ki namerava skleniti pogodbo s tajnimi podatki s stranko pogodbe s tajnimi podatki druge pogodbenice ali želi za to pooblastiti eno od svojih strank pogodbe s tajnimi podatki, mora pri nacionalnem varnostnem organu ali pristojnih varnostnih organih druge pogodbenice preveriti, da ima ta stranka pogodbe s tajnimi podatki ustrezno varnostno dovoljenje za izvajanje navedene pogodbe. Če takega dovoljenja nima, nacionalni varnostni organ ali pristojni varnostni organi pogodbenice prejemnice začnejo postopek varnostnega preverjanja za zahtevano stopnjo tajnosti podatkov.

8. Pred vsako izmenjavo tajnih podatkov morajo pristojni varnostni organi pogodbenice izvora uradno obvestiti pristojne varnostne organe pogodbenice prejemnice o pogodbah s tajnimi podatki. V tem obvestilu morajo podrobno opredeliti najvišjo stopnjo tajnosti podatkov v pogodbi.

9. Pristojni varnostni organi pogodbenice, na ozemlju katere bo delo potekalo, morajo pri izvajanju pogodb s tajnimi podatki zagotoviti, da se uporablja in ohranja enaka stopnja varovanja tajnih podatkov, kakor jo zahtevajo za varovanje svojih pogodb s tajnimi podatki.

10. Stranka pogodbe s tajnimi podatki mora dobiti dovoljenje svojih pristojnih varnostnih organov, preden začne s podizvajalcem izvajati pogodbo s tajnimi podatki. Podizvajalci morajo ravnati v skladu s pogoji varovanja, kakršni so določeni za stranko pogodbe s tajnimi podatki.

11. ČLEN
SODELOVANJE PRI VAROVANJU TAJNOSTI

1. Za doseganje in ohranjanje primerljivih varnostnih standardov si nacionalna varnostna organa ali pristojni varnostni organi na podlagi zaprosila zagotovijo podatke o državnih varnostnih standardih, postopkih in praksah za varovanje tajnih podatkov. Pogodbenici soglašata, da bosta v ta namen olajševali stike med nacionalnima varnostnima organoma in pristojnimi varnostnimi organi, ki lahko organizirajo medsebojne obiske.

2. Nacionalna varnostna organa ali pristojni varnostni organi se obveščajo o varnostnih tveganjih, ki bi lahko ogrozila dane tajne podatke.

3. Pri varnostnem preverjanju državljana ene od pogodbenic, ki je prebival na ozemlju druge pogodbenice ali se še zadržuje na njem, si nacionalni varnostni organ in pristojni varnostni organi pogodbenice pomagajo v skladu z notranjimi zakoni in drugimi predpisi.

4. Nacionalni varnostni organ ali pristojni varnostni organi se v skladu z notranjimi zakoni in drugimi predpisi obveščajo o spremembah, ki vplivajo na varnostna dovoljenja njihovih državljanov po tem sporazumu, zlasti ob odvzemu ali znižanju stopnje varnostnega dovoljenja.

12. ČLEN
KRŠITEV ZAKONOV IN DRUGIH PREDPISOV O VAROVANJU TAJNIH PODATKOV

1. Vsaka pogodbenica takoj uradno obvesti drugo pogodbenico o sumu ali odkritju kršitve ali ogrožanja varovanja tajnih podatkov, izmenjanih ali nastalih po tem sporazumu. Obvestilo mora biti dovolj podrobno, da pogodbenica izvora lahko v celoti oceni posledice.

2. Pogodbenica takoj, ko odkrije dejstva ali se ji vzbudi sum, opravi preiskavo (po potrebi s pomočjo druge pogodbenice) v skladu s svojimi veljavnimi notranjimi zakoni in drugimi predpisi. Pogodbenica, ki vodi preiskavo, čim prej obvesti nacionalni varnostni organ ali pristojne varnostne organe druge pogodbenice o ugotovitvah preiskave, sprejetih ukrepih in odpravi pomanjkljivosti.

13. ČLEN
STROŠKI

1. Posebni stroški po tem sporazumu niso predvideni.

2. Morebitne stroške, ki za pogodbenico nastanejo zaradi izvajanja tega sporazuma, krije ta pogodbenica.

14. ČLEN
RAZLAGA IN REŠEVANJE SPOROV

1. Vsi spori zaradi razlage ali uporabe sporazuma se rešujejo izključno s posvetovanjem med pogodbenicama.

2. Pogodbenici se zavezujeta, da bosta med sporom spoštovali obveznosti iz sporazuma.

15. ČLEN
KONČNE DOLOČBE

1. Sporazum je sklenjen za nedoločen čas. Odobren mora biti v skladu z notranjepravnimi postopki pogodbenic in začne veljati prvi dan drugega meseca po dnevu zadnjega uradnega obvestila med pogodbenicama, da so izpolnjene vse zahteve, potrebne za začetek veljavnosti sporazuma.

2. Sporazum se lahko kadar koli spremeni s pisnim soglasjem pogodbenic. Spremembe začnejo veljati v skladu prvim odstavkom tega člena.

3. Po potrebi in za vsak primer posebej se nacionalna varnostna organa ali pristojni varnostni organi pogodbenic posvetujejo o posebnih tehničnih vidikih v zvezi z izvajanjem tega

sporazuma in za njegovo dopolnitev lahko sklenejo ustrezen pravni dokument ali poseben varnostni protokol.

4. Kadar bi spremembe zakonov in drugih predpisov pogodbenic lahko vplivale na varovanje tajnih podatkov po sporazumu, se pogodbenici posvetujeta in preučita njegove morebitne spremembe.

5. Vsaka pogodbenica lahko sporazum kadar koli pisno odpove. V tem primeru preneha veljati šest mesecev po dnevu, ko druga pogodbenica prejme uradno obvestilo o odpovedi.

6. Ne glede na odpoved sporazuma se vsi tajni podatki, dani na njegovi podlagi, še naprej varujejo v skladu z njegovimi določbami, dokler pogodbenica izvora pogodbenice prejemnice ne razreši te obveznosti.

V potrditev navedenega sta podpisana, ki sta bila za to pravilno pooblaščena, podpisala ta sporazum.

Sestavljeno v Ljubljani dne 16.11.2009 v dveh izvirnikih v francoskem in slovenskem jeziku, pri čemer sta besedili enako verodostojni.

Za Vlado Francoske republike

Veleposlanica Francije
v Republiki Sloveniji

Za Vlado Republike Slovenije

Generalni sekretar
Vlade Republike Slovenije

[TRANSLATION – TRADUCTION]

AGREEMENT BETWEEN THE GOVERNMENT OF THE FRENCH REPUBLIC AND THE GOVERNMENT OF THE REPUBIC OF SLOVENIA CONCERNING THE RECIPROCAL PROTECTION AND EXCHANGE OF CLASSIFIED INFORMATION

The Government of the French Republic and the Government of the Republic of Slovenia (hereinafter referred to as "the Parties"), wishing to guarantee the protection of classified information exchanged between the two States or between public and private entities under their jurisdiction, in mutual respect of their national interests and national security, have agreed as follows:

Article 1. Definitions

For the purposes of this Agreement:

1. "Classified Information": refers to any item of information, document or material, irrespective of its form, including those in course of preparation, requiring protection against any violation, destruction, misappropriation, disclosure, loss, unauthorized access or compromise of any other kind and having been designated as such in accordance with the laws and regulations of either Party.

2. "Classified Contract": refers to any contract, subcontract or project whose development and execution requires access to classified information or the utilization and production of classified information.

3. "Party to a Classified Contract": refers to any physical or moral person having the legal capacity to negotiate and conclude classified contracts.

4. "National Security Agency" (NSA): refers to the national authority responsible for overall supervision and implementation of this Agreement for each of the Parties.

5. "Competent security authorities": refers to any designated security authority or other competent entity authorized under the national laws and regulations of the Parties and responsible for the implementation of this Agreement according to the fields concerned.

6. "Originating Party": refers to the Party, including any public or private agency subject to its jurisdiction, which transmits classified information to the other Party.

7. "Recipient Party": refers to the Party, including any public or private agency subject to its jurisdiction, which receives classified information transmitted by the originating Party.

8. "Third party": refers to a State, including any public or private agency or any individual subject to its jurisdiction, or any international organization which is not a party to this Agreement.

9. "Host Party": refers to the Party in whose territory a visit takes place.

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

Article 2. Security classification equivalents

1. Classified information transmitted under this Agreement shall be identified by markings of the appropriate security classification levels in conformity with the national laws and regulations of the Parties.

2. The equivalences of the security classifications established by each of the Parties are:

FRANCE	SLOVENIA
TRÈS SECRET DÉFENSE	STROGO TAJNO
SECRET DÉFENSE	TAJNO
DÉFENSE – CONFIDENTIEL	ZAUPNO
(NB)	INTERNO

N.B. The French Party shall handle and protect information bearing the designation “INTERNO” transmitted by the Slovene Party in accordance with its national laws and regulations in force concerning information which is protected but not classified, such as those designated “DIFFUSION RESTREINTE”.

The Slovene Party shall handle and protect information bearing the designation “DIFFUSION RESTREINTE” transmitted by the French Party in accordance with its national laws and regulations in force concerning information which is protected but not classified, such as those designated “INTERNO”.

3. The national security authorities shall keep one another informed of any additional designation which may be used within the framework of this Agreement.

4. In certain cases and for specific security reasons, when the originating Party requires that access to information classified at the “CONFIDENTIEL DÉFENSE/ZAUPNO” or higher level be restricted to persons bearing the nationality of the Parties and no other, that information shall bear the additional designation “SPÉCIAL FRANCE – SLOVÉNIE”.

Article 3. National security authorities

1. The national security authority for each of the Parties is as follows:

For the French Republic:

Secrétariat-Général de la Défense nationale (SGDN)

For the Republic of Slovenia:

Urad Vlade Republike Slovenije za varovanje tajnik podatkov

2. The national security authorities shall keep one another informed of any other competent security authority responsible for implementation of this Agreement.

3. The Parties shall inform one another immediately of any change affecting their national security authorities and competent security authorities and affecting implementation of this Agreement.

Article 4. Access to classified information

1. Access to information bearing the designation DIFFUSION RESTREINTE/ INTERNO shall be restricted to persons who have a need to know and have been briefed accordingly.

2. Access to information classified at CONFIDENTIEL DÉFENSE/ZAUPNO or a higher level shall be restricted to persons with a security clearance in accordance with national laws and regulations and have been authorized to have access to such information on a need-to-know basis.

3. In accordance with the application of the procedural rules laid down in their respective national laws and regulations, the Parties shall recognize one another's personnel security clearances concerning access to classified information. The provisions of article 2, paragraph 2, of this Agreement shall apply accordingly.

Article 5. Protection of classified information

1. In accordance with their respective national laws and regulations, the Parties shall afford to the classified information referred to in this Agreement the same protection as they afford to their own information of the equivalent security classification level.

2. The originating Party shall:

(a) Ensure that the classified information bears the marking corresponding to the appropriate classification level in accordance with its national laws and regulations;

(b) Inform the recipient Party:

- Of any conditions attaching to its transmission or restriction on its use;
- Of any subsequent changes in the classification.

3. The recipient Party shall:

(a) Immediately on receipt of classified information transmitted by the originating Party, designate it within its own national classification level in accordance with the provisions of article 2, paragraph 2, of this Agreement;

(b) Refrain from changing or removing the classification of classified information without the written consent of the originating Party.

4. The Parties shall inform one another as soon as possible of any changes affecting the protection of classified information exchanged or produced under this Agreement.

5. The Parties shall ensure compliance with all requirements deriving from their national security laws and regulations applying to the security of the agencies, offices and facilities under their jurisdiction.

Article 6.Use of classified information

1. In accordance with the provisions of this Agreement and the contractual instruments concluded by the Parties, classified information transmitted shall not be used for any purpose other than that for which it is transmitted.

2. The recipient Party shall not disclose classified information exchanged or produced under this Agreement to any third party without the prior written agreement of the national security authority or the competent security authorities of the originating Party.

3. Classified information developed jointly by the Parties under agreements, contracts or other common activity shall not be downgraded, declassified or transmitted to a third party without the prior written consent of both Parties.

4. Prior to the transmission of any classified information received from the originating Party to a party to a classified contract, the competent security authorities of the recipient Party shall:

(a) Make sure that the party to a classified contract and its facilities are able to provide appropriate protection for the classified information;

(b) Grant the required level of clearance to the party concerned to a classified contract;

(c) Grant the required level of clearance to persons with a need to know;

(d) Make sure that all persons with access to classified information are informed of their responsibilities arising from the national laws and regulations in force;

(e) Perform security checks in the facilities concerned.

5. If the national security authority or the competent security authorities of one of the Parties considers that a company registered in its national territory is owned by or under the influence of a State whose objectives are incompatible with its interests, that company shall not be issued with a clearance certificate. The national security authority of the Party requesting the security clearance shall consequently be advised in writing as soon as possible.

Article 7. Transmission of classified information

1. Classified information shall be exchanged between the Parties through the diplomatic channel in accordance with the national laws and regulations of the originating Party.

2. The national security authorities or the competent security authorities may, by mutual agreement and in accordance with the national laws and regulations of the Parties, agree that classified information may be transmitted by a mode other than that of the diplomatic channel where the latter proves unsuitable.

3. Transmissions of classified information shall meet the following requirements:

(a) The courier shall be a permanent employee of the originator or the recipient or an official of the public administration and hold a security clearance at least matching the classification level of the information to be transmitted;

(b) The courier shall be in possession of a courier's certificate issued by the competent authorities of the originator or the recipient;

(c) The originating Party shall keep a register of the classified information transmitted; an extract from that register shall be supplied to the recipient Party on request;

(d) The classified information shall be duly wrapped and sealed in accordance with the national laws and regulations of the originating Party;

(e) Receipt of classified information shall be confirmed in writing as soon as possible.

4. Transmission of a large quantity of classified information shall be organized between the respective national security authorities or the competent security authorities of the Parties on a case-by-case basis.

5. Classified information transmitted electronically shall be encrypted with the use of cryptographic methods and devices mutually accepted by the competent respective national security agencies of the Parties in accordance with their national laws and regulations.

Article 8. Reproduction, translation and destruction

1. All translations and reproductions of classified information shall be identified by the appropriate security classification markings and enjoy the same protection as the originals. Translations and the number of reproductions shall be restricted to the amounts necessary for official use.

2. Every translation shall bear an appropriate notification in the language of the translation stating that the document contains classified information transmitted by the originating Party.

3. Information classified as TRÈS SECRET DÉFENSE/STROGO TAJNO shall be neither translated nor reproduced. Additional copies may be supplied to the originating Party on written request. Information classified at this level may not be destroyed save with the express authorization of the originating Party and in conformity with the provisions of article 8, paragraph 5, of this Agreement. It shall be returned to the originating Party in conformity with article 7 of this Agreement after being recognized as no longer necessary or on expiry of its validity.

4. Information classified at TAJNO/SECRET DÉFENSE level shall be translated or reproduced solely with the written agreement of the national security agency or the competent security authorities of the originating Party.

5. Classified information shall be destroyed in such a way as to render its partial or total reconstruction impossible.

Article 9. Visits

1. Visits to facilities of one of the Parties where a representative of the other Party has access to classified information or to sites where access to such information is directly possible shall require the prior written authorization of the national security agency or the

competent security authorities of the host Party or in conformity with its national laws and regulations.

2. Visits to facilities of one of the Parties by representatives of a third party involving access to classified information exchanged or produced between the Parties or to sites where access to such information is directly possible shall require the prior written authorization of the national security agency or the competent security authorities of the other Party.

3. Requests for visits where access to classified information of STROGO TAJNO/TRÈS SECRET DÉFENSE level is necessary shall be transmitted by the diplomatic channel to the national security authority of the host Party. Requests concerning visits necessitating access to classified information of a lower level shall be handled directly by the national security authorities or the competent security authorities in the respective Parties in conformity with their national laws and regulations. Requests shall be addressed at least 20 (twenty) days prior to the requested date for the visit.

4. Requests for visits must contain the following:

(a) The visitor's surname and given names, date and place of birth, nationality and passport or identity card number;

(b) The visitor's position, with particulars of the establishment he represents, or the title and details of the classified contract to which he is a party;

(c) The visitor's level of security clearance, authenticated by a security certificate to be issued by the national security authority or the competent security authorities of the requesting Party in conformity with its national laws and regulations;

(d) The name, address, phone/fax number, e-mail and contact point of the establishment, facility or premises to be visited and the surnames and given names of the persons who are to receive the visitor;

(e) The purpose of the visit and all the necessary particulars specifying the subjects to be dealt with involving classified information and their classification levels;

(f) The proposed date and anticipated duration of the visit. Where several visits are envisaged, the total duration of all the visits is to be specified;

(g) The date, signature and affixed official stamp of the competent authority in the requesting Party.

5. In urgent cases, requests for visits may be transmitted not less than five (5) working days before the start of the visit.

6. The Parties may establish lists of personnel authorized to effect recurring visits within the framework of any specific project, programme or contract in conformity with the general conditions agreed on by the national security authorities or the competent security authorities of the Parties. Such lists shall be valid initially for twelve (12) months; by agreement between the national security authorities or the competent security authorities of the Parties, such validity may be extended for further periods not exceeding twelve (12) months in all. Such lists shall be established in conformity with the national laws and regulations of the host Party. Once a list has been approved, the general conditions for any particular visit may be determined directly by the establishments which persons on the list are to visit.

7. Any classified information acquired by a visitor shall be deemed to be classified information transmitted under this Agreement.

8. All visitors shall comply with the security regulations and instructions of the host Party.

Article 10. Classified contracts

1. In accordance with the application of the procedural rules laid down in their respective national laws and regulations, the Parties shall recognize one other's establishment security clearances. The provisions of article 2, paragraph 2, of this Agreement shall accordingly be applicable.

2. Before concluding a classified contract with a party to a classified contract under the jurisdiction of the other Party, or authorizing one of its parties to a classified contract to conclude a classified contract in the territory of the other Party, one Party shall receive prior written assurance from the national security authority or the competent security authorities of the other Party in conformity with the national laws and regulations of the latter, to the effect that the party to a proposed classified contract has received clearance at the appropriate level and has taken all appropriate security measures necessary for the protection of the classified information.

3. To ensure compliance with security standards in conformity with national laws and regulations, the competent security authorities of either of the Parties may request a security inspection in a particular facility.

4. A classified contract shall contain information on security instructions and a classification guide. Such instructions shall be in conformity with those issued by the competent security authorities of the originating Party.

5. A security annex shall be included with any contractual instrument containing classified information. In that annex the competent security authorities shall specify what must be protected by the recipient Party and the corresponding applicable classification level. The originating Party alone may change the classification level of an item of information defined in a security annex.

6. The national security authority or the competent security authorities in the originating Party shall transmit a copy of the security annex to the national security authority or the competent security authorities of the other Party.

7. The Party intending to conclude, or authorize one of its parties to a classified contract to conclude, a classified contract with a party to a classified contract of the other Party shall verify with the national security authority or the competent security authorities of the other Party that the party to a classified contract concerned has the appropriate security clearance level needed for performance of the contract. Otherwise the national security authority or the competent security authorities of the recipient Party shall introduce a clearance procedure at the appropriate level.

8. The competent security authorities of the originating Party shall notify the competent security authorities of the recipient Party of any classified contract prior to any exchange of classified information. Such notification must indicate the highest classification level of any information involved in the contract.

9. The competent security authorities of the Party in whose territory the work is to be done are required to ensure that during performance of the classified contract a level of security equivalent to that required for the protection of their own contracts is applied and maintained.

10. Before concluding a classified contract with a subcontractor, the party to a classified contract shall obtain authorization from its competent security authorities. Subcontractors shall comply with the same security requirements as those laid down for the party to a classified contract.

Article 11. Security cooperation

1. To achieve and maintain comparable security standards, the national security authority or the competent security authorities of each Party shall provide the other on request with information on its national laws, regulations, standards, procedures and practices relating to protection of classified information. For that purpose the Parties agree to facilitate contacts between their respective national security authorities or competent security authorities, which may organize visits to one another.

2. The national security authorities or the competent security authorities of each of the Parties shall keep one another informed of security risks of a nature to compromise classified information transmitted.

3. In matters relating to the security clearance of a national of one Party who is residing or has resided for over three months in the territory of the other Party, the national security authorities or the competent security authorities of each Party shall assist one another in conformity with their respective national laws and regulations.

4. In conformity with their national laws and regulations, the national security authorities or the competent security authorities shall keep one another informed of changes in the security clearances of their nationals under this Agreement, particularly in the event of a withdrawal or a declassification of access to clearance.

Article 12. Breaches of laws and regulations concerning the protection of classified information

1. Each Party shall notify the other without delay of any presumed or confirmed breach or compromise affecting the security of classified information exchanged or produced under the terms of this Agreement. The notification must be detailed enough to enable the originating Party to undertake a complete evaluation of the consequences.

2. The Party establishing or suspecting the facts shall immediately open an inquiry (with the aid of the other Party where necessary) in conformity with the national laws and regulations in force in the State concerned. The Party conducting the inquiry shall inform the national security authority or the competent security authorities of the other Party as soon as possible of the results of the inquiry, the measures adopted and the corrective action taken.

Article 13. Costs

1. It is not anticipated that this Agreement will give rise to specific costs.

2. Any cost incurred by a Party as a result of the application of this Agreement shall be borne solely by that Party.

Article 14. Interpretation and settlement of disputes

1. Any dispute concerning the interpretation or application of this Agreement shall be settled exclusively by way of consultations between the Parties.

2. Throughout the duration of the dispute, the Parties shall continue to respect the obligations deriving from this Agreement.

Article 15. Final provisions

1. This agreement is concluded for an indefinite period. It shall be submitted for approval by the Parties in conformity with their national legal procedures and shall enter into force on the first day of the second month following the date of the last of the notifications exchanged between the Parties confirming completion of the requirements necessary for the entry into force of this Agreement.

2. This Agreement may be amended at any time by written agreement between the Parties. Amendments shall take effect in accordance with the modalities laid down in the first paragraph of this article.

3. As necessary, the national security authorities or competent security authorities of the parties shall consult one another on the subject of specific technical aspects of the application of this Agreement and may conclude, on a case-by-case basis, any appropriate legal instrument or specific security protocol intended to supplement this Agreement.

4. If any change in the national laws and regulations of the Parties is likely to affect the protection of classified information under this Agreement, the Parties shall consult one another to consider all possible amendments to this Agreement.

5. Either Party may denounce this Agreement in writing at any time. In such case the Agreement shall cease to be valid six (6) months after receipt by the other Party of notification of the denunciation.

6. Notwithstanding denunciation of this Agreement, all classified information transmitted under its terms shall remain protected in conformity with the provisions of the Agreement until the originating Party releases the recipient Party from that obligation.

IN WITNESS WHEREOF, the undersigned, duly authorized to that effect, have signed this Agreement.

DONE at Ljubljana on 16 November 2009 in two copies, in the French and Slovene languages, both texts being equally authentic.

For the Government of the French Republic:

NICOLE MICHELANGELI
Ambassador of France to the Republic of Slovenia

For the Government of the Republic of Slovenia:

MILAN MARTIN CVIKL
Secretary-General of the Government of the Republic of Slovenia